O'REILLY

ТОМАС ЛИМОНЧЕЛЛИ
КРИСТИНА ХОГАН
СТРАТА ЧЕЙЛАП

второе издание

СИСТЕМНОЕ И СЕТЕВОЕ АДМИНИСТРИРОВАНИЕ

ПРАКТИЧЕСКОЕ РУКОВОДСТВО

СИМВОЛ®

The Practice of System and Network Administration

Second Edition

Thomas A. Limoncelli,
Christina J. Hogan and Strata R. Chalup

Addison-Wesley

HIGH TECH

Системное и сетевое администрирование

Практическое руководство

Второе издание

Томас Лимончелли,
Кристина Хоган и Страта Чейлап

Санкт-Петербург — Москва
2009

Серия «High tech»

Томас Лимончелли, Кристина Хоган, Страта Чейлап

Системное и сетевое администрирование Практическое руководство, 2-е издание

Перевод Ю. Белозеровой, Р. Багаутдинова

Главный редактор	*А. Галунов*
Зав. редакцией	*Н. Макарова*
Выпускающий редактор	*Л. Пискунова*
Научные редакторы	*А. Бахарев, Р. Багаутдинов*
Редактор	*Е. Тульсанова*
Корректор	*Е. Бекназарова*
Верстка	*Л. Пискунова*

Лимончелли Т., Хоган К., Чейлап С.

Системное и сетевое администрирование. Практическое руководство, 2-е издание. – Пер. с англ. – СПб: Символ-Плюс, 2009. – 944 с., ил.

ISBN: 978-5-93286-130-1

Эта книга совсем не похожа на другие книги по системному администрированию. Вы не узнаете из нее, как управлять той или иной системой, однако она незаменима для тех, кто желает стать профессиональным и эффективным системным администратором. Книга содержит основную информацию о системах, сетях, серверах и вычислительных центрах, базовые и «продвинутые» принципы администрирования и разработки проектов вне зависимости от специфики операционной системы. Обсуждаются задачи, стоящие перед системными администраторами, и наиболее часто встречающиеся проблемы и эффективные способы их решения. Издание призвано стать настоящим наставником для новичков и отличным справочником для продвинутых админов. Нетехническим руководителям, в чьем подчинении находятся IT-отделы, эта книга поможет лучше понять специфику работы их подчиненных. Главы, посвященные менеджменту, помогут руководителям IT-отделов повысить эффективность их работы, а также будут интересны всем, кто желает сделать карьеру в данной сфере. Повествование сопровождается множеством ярких примеров из жизни, а юмор авторов делает его живым и увлекательным.

ISBN: 978–5–93286–130–1
ISBN: 978–0–321–49266–1 (англ)

Издательство «Символ-Плюс». 199034, Санкт-Петербург, 16 линия, 7,
тел. (812) 3245353, www.symbol.ru. Лицензия ЛП N 000054 от 25.12.98.
Подписано в печать 25.05.2009. Формат 70x100 $^{1}/_{16}$. Печать офсетная.
Объем 59 печ. л. Тираж 1500 экз. Заказ N
Отпечатано с готовых диапозитивов в ГУП «Типография «Наука»
199034, Санкт-Петербург, 9 линия, 12.

Краткое содержание

Оглавление

Предисловие

Цель написания этой книги – изложить знания, полученные нами от наших наставников и из личного опыта. Эти знания отличаются от тех, которые обычно даются в руководствах и книгах по системному администрированию.

Эта книга основана на нашем опыте системного администрирования в различных организациях. Мы создавали новые компании. Мы помогали корпоративным сетям развиваться. Мы работали в небольших только что появившихся компаниях и университетах, которые испытывали недостаток финансирования. Мы трудились в средних и крупных транснациональных компаниях, где возникали необычные задачи, связанные с поглощениями и появлением дочерних компаний. Мы также работали в быстро развивающихся интернет-компаниях, где нормой были высочайшие требования к надежности, производительности и масштабируемости. У нас есть опыт работы и в медленно развивающихся компаниях, где представителями высоких технологий были радиотелефоны. На первый взгляд может показаться, что условия работы и задачи во всех этих организациях должны были различаться, но в основе своей они состояли из одних и тех же элементов и к ним применялись одни и те же фундаментальные принципы.

Эта книга даст вам настоящую основу – способы осмысления проблем системного администрирования, а не ограниченные решения отдельных проблем. Имея надежную основу, вы сможете решать любые проблемы по мере их появления независимо от операционной системы (ОС), марки компьютера или типа интерфейса. Уникальность этой книги в том, что в ней рассматривается системное администрирование в целом, тогда как большинство книг по системному администрированию посвящены обслуживанию определенного продукта. По мере накопления опыта все системные администраторы рано или поздно понимают, что в общем и целом все проблемы и решения совершенно не зависят от платформы. Эта книга изменит ваш подход к работе системного администратора.

Принципы, изложенные в этой книге, применимы ко всем интерфейсам. Описанные способы могут изменяться в ту или иную сторону в зависимости от интерфейса, но основные принципы будут применимы всегда. В случаях, когда применение определенных концепций неочевидно, мы привели примеры для организаций различного размера.

В этой книге вы не найдете описаний конфигурирования или отладки конкретной ОС и восстановления общих библиотек или DLL после их случайного удаления или перемещения. Этим темам посвящено много превосходных книг, и на многие из них мы будем ссылаться в тексте. Вместо этого мы обсудим как простые, так и более сложные принципы эффективного системного админист-

рирования, известные нам из нашего опыта. Эти принципы применимы ко всем ОС. Их последовательное применение может значительно упростить вам жизнь. Если вы усовершенствуете способы решения проблем, это принесет вам значительную пользу. Правильно применяйте основные принципы – и все встанет на свои места. При неправильном применении вы потеряете время, многократно исправляя одно и то же, а ваши пользователи[1] будут недовольны, так как они не смогут эффективно работать на неисправных машинах.

Для кого эта книга

Эта книга написана для системных администраторов любого уровня. Начинающим системным администраторам она даст общее представление о работе корпоративных сетей, об их роли в организациях и о личном профессиональном развитии. Администраторы среднего уровня узнают, как решать более сложные проблемы, улучшить функционирование сетей, упростить свою работу и повысить удовлетворенность пользователей. Независимо от вашего уровня книга поможет понять, в чем именно должна заключаться ваша ежедневная работа; вы узнаете, что можно сделать сейчас для экономии времени в будущем, как выработать стратегию; вы научитесь быть архитекторами и дизайнерами, составлять долгосрочные планы, вести переговоры с поставщиками и взаимодействовать с администрацией. Эти темы важны для старших системных администраторов, но ни одной из них нет в руководствах к операционной системе. Даже старшие системные администраторы и системные архитекторы смогут чему-то научиться на нашем опыте и опыте наших коллег, так же как и мы учились друг у друга во время написания книги. Кроме того, мы рассмотрим некоторые вопросы менеджмента для системных администраторов, которые хотят понять особенности работы менеджеров или собираются ими стать либо просто занимаются менеджментом в личных целях.

В книге мы иллюстрируем наши выводы примерами. В основном это примеры средних и крупных корпоративных сетей, масштабность которых создает дополнительные проблемы. Как правило, это общие примеры, не зависящие от ОС. Если приводятся специфические примеры для определенной ОС, то это обычно бывает UNIX или Windows.

Одной из важнейших причин для написания книги стало понимание того, что проблемы, с которыми сталкивается системный администратор, одинаковы для всех ОС. Новая ОС, значительно отличающаяся от того, с чем мы сталкивались раньше, может показаться «черным ящиком», мешающим и даже опасным. Тем не менее, несмотря на непривычный интерфейс, как только мы освоим новую технологию, в конечном итоге мы понимаем, что столкнулись с тем же набором проблем развертывания, масштабирования и обслуживания новой ОС. Признав этот факт, зная проблемы, требующие решения, и понимая, какие способы применить, на основе опыта работы в других ОС вы сумеете быстрее разобраться в новых задачах.

Нам хотелось бы верить, что эта книга изменит вашу жизнь. Надеемся, вы добьетесь такого успеха, что, встретив нас на улице, крепко нас обнимете.

---

[1] В этой книге мы будем называть конечных пользователей ваших систем именно «пользователями», а не «юзерами», как это делают некоторые сисадмины. Подробное объяснение причин вы найдете в разделе 31.1.2.

Основные принципы

Если мы чему-то и научились за многие годы, так это тому, как важны простота, ясность, универсальность, автоматизация, взаимодействие и решение базовых проблем в первую очередь. К этим шести принципам мы будем неоднократно возвращаться в книге.

1. *Простота* означает, что самое лаконичное решение проблемы – это самое лучшее решение. Это помогает сохранить систему простой для понимания и снижает количество сложных межкомпонентных взаимодействий, способных превратить отладку в кошмар.
2. *Ясность* означает, что решение должно быть понятным, чтобы можно было его легко объяснить участникам проекта или даже посторонним. Ясность помогает упростить изменение системы, а также ее обслуживание и отладку. В мире системного администрирования лучше написать пять строк понятного кода, нежели одну строку, непостижимую ни для кого, кроме вас.
3. *Универсальность* означает, что решение не должно быть применимо только в одном отдельном случае. Решения должны использоваться повторно. Использование открытых, стандартных, независимых от поставщика (разработчика) протоколов делает системы более гибкими и позволяет упростить взаимосвязи между программными пакетами, тем самым улучшив обслуживание.
4. *Автоматизация* подразумевает замену человеческого труда программами. Автоматизация критически важна. Она повышает однотипность и расширяемость системы, облегчает нагрузку администратора и избавляет от утомительных повторяющихся задач, предоставляя системному администратору больше времени на улучшение обслуживания.
5. *Взаимодействие* с нужными людьми может решить больше проблем, чем программы или оборудование. Вам надо взаимодействовать с другими системными администраторами и с вашими пользователями. Вы обязаны быть инициатором взаимодействия. Взаимодействие гарантирует, что все работают для достижения одних и тех же целей. Из-за неправильного взаимодействия люди становятся огорченными и раздраженными. Также в понятие взаимодействия входит документация. Документация упрощает поддержку, обслуживание и модернизацию системы. Эффективное взаимодействие и подобающая документация также упрощают передачу проектов и обслуживания преемнику при переходе на другую работу или другую должность.
6. *Первоочередное решение базовых проблем* означает, что вы строите корпоративную сеть на надежном основании, выявляя и решая базовые проблемы прежде, чем начнете бороться с проблемами более высокого уровня. Первоочередное решение базовых проблем позволяет значительно упростить внедрение дополнительной функциональности и делает службы более устойчивыми к сбоям. Полноценная базовая инфраструктура может быть неоднократно усовершенствована для развития корпоративной сети с относительно малыми усилиями. Иногда системному администратору приходится прилагать серьезные усилия для решения проблем, которые не возникали бы или решались бы простым усовершенствованием, если бы в основе корпоративной сети лежала надлежащая базовая инфраструктура. Эта книга поможет вам выявлять базовые проблемы и покажет, как применять остальные пять принципов. В каждой главе будут рассматри-

ваться базовые проблемы в определенной сфере. Научитесь правильно применять основы – и все остальное встанет на свои места.

Эти принципы универсальны. Они применимы на всех уровнях системы. Они применимы к физическим сетям и компьютерному оборудованию. Они применимы ко всем операционным системам в корпоративной сети, всем используемым протоколам, всему программному обеспечению и всем службам. Они применимы в университетах, некоммерческих организациях, правительственных сетях, в компаниях и на сайтах интернет-услуг.

Кто такой системный администратор

Если вы попросите шестерых системных администраторов описать свою работу, вы получите шесть разных ответов. Работу системного администратора сложно как-то определить, поскольку она слишком разнообразна. Системный администратор отвечает за компьютеры, сети и за людей, которые их используют. Системный администратор может отвечать за оборудование, операционные системы, программное обеспечение, конфигурацию, приложения и безопасность. От системного администратора зависит, насколько эффективно другие люди используют свои компьютеры и сети.

Время от времени системному администратору приходится быть консультантом по бизнес-процессам, корпоративным прорицателем, сторожем, разработчиком программ, инженером-электриком, экономистом, психиатром, телепатом и даже барменом.

Поэтому в различных компаниях должность системного администратора может называться по-разному. Иногда их называют администраторами сетей, системными архитекторами, системными инженерами, системными программистами, операторами и т. д.

Эта книга – для всех вышеперечисленных.

У нас есть наиболее универсальное определение системного администратора: это тот, кто управляет компьютерными и сетевыми системами от имени другого лица, например работодателя или пользователя. Системный администратор – это тот, благодаря кому все функционирует.

Чем занимается системный администратор

Трудно дать определение системному администрированию, но еще сложнее объяснить это человеку, далекому от техники, особенно если этот человек – ваша мать. Мать имеет право знать, на какие средства ее ребенок оплачивает счета. У друга Кристины Хоган всегда возникали проблемы с объяснением матери, чем он зарабатывает на жизнь, потому что каждый раз он давал разные ответы на ее вопрос. Она задавала этот вопрос каждые два месяца, требуя ответа, который будет для нее понятным. Как-то он начал работать над WebTV[1]. Когда приставки поступили в продажу, он подарил такую маме. С тех пор он говорил ей, что следит за тем, чтобы ее служба WebTV работала, и работала отлично. Она была очень довольна, что теперь может что-то показать подругам и сказать: «Это сделал мой сын!»

[1] WebTV – приставка для просмотра интернет-телевидения. – *Прим. перев.*

Зачем нужно системное администрирование

Системное администрирование необходимо, поскольку нам нужны компьютеры и сети. Компьютеры играют сейчас в нашей жизни значительно более важную роль, нежели раньше. Что произошло?

Широкое распространение Интернета и внутренних сетей и мировая ориентация на интернет-технологии определили зависимость компаний от компьютеров. Интернет подразумевает работу 24/7 (24 часа в сутки, 7 дней в неделю), и нестабильная работа здесь недопустима.

Обработка заказов может идти ежедневно непрерывным потоком незаметно для пользователей. Однако от интернет-систем ожидают беспрепятственной доступности в любое время из любого места. Ночные перерывы на профилактику стали неслыханной роскошью. Те ненадежные системы энергоснабжения вычислительных центров, которые раньше вызывали периодические, но решаемые проблемы, теперь могут парализовать регистрацию продаж.

Сейчас у менеджеров сложилось более реалистичное представление о компьютерах. До того как персональные компьютеры появились на их рабочих столах, мнение о компьютерах у большинства людей формировалось под влиянием кинематографа: огромные, всезнающие, самодостаточные волшебные машины. Чем больше людей непосредственно взаимодействовали с компьютерами, тем более реалистичными становились представления. Теперь в фильмах показывают даже работу системных администраторов. Классический фильм 1993 года «Парк юрского периода» стал первой популярной кинолентой, в которой была продемонстрирована ключевая роль администратора в больших системах.

В фильме также было показано, что зависимость системы от одного человека грозит катастрофой. Информационные технологии – это «командный вид спорта». Жаль, что Деннис Недри[1] не читал эту книгу.

В бизнесе неважно все, кроме того, что считает важным директор. Директор распределяет финансирование и расставляет приоритеты. Сейчас директора стали понимать важность информационных технологий. Раньше электронная почта была прерогативой особо продвинутых специалистов, теперь директора зависят от электронной почты и замечают малейшие перебои в ее работе. Массовая подготовка к проблеме 2000 года[2] тоже показала директорам компаний, насколько сильно их организации зависят от компьютеров, насколько дорого может обойтись их обслуживание и как быстро чисто техническая сложность может стать серьезной угрозой. Большинство людей не думают, что с решением проблемы 2000 года всем просто повезло, а считают, что неприятностей удалось избежать благодаря огромным усилиям многих людей. Опрос, проведенный телекомпанией CBS, показал следующее: 63% американцев уверены, что время и силы, потраченные на предотвращение потенциальных проблем, того стоили. Новости трех крупнейших телекомпаний в понедельник, 3 января 2000 года отражали то же мнение.

Раньше люди не имели доступа к компьютерам с детства и с осторожностью изучали их и их возможности. Но сейчас все растет число людей, знакомых

---

[1] Деннис Недри (Dennis Nedry) – персонаж фильма «Парк юрского периода», программист, системный администратор центра управления парком. – *Прим. перев.*

[2] Эта проблема была связана с неспособностью некоторых старых компьютеров отображать правильное системное время в новом веке. – *Прим. перев.*

с компьютерами с детства, которые, становясь руководителями, ожидают от компьютеров безграничных возможностей. Исполнительных директоров предприятий, которых изумляла автоматизация расчетов заработной платы, скоро заменит поколение руководителей, которые с детства привыкли к системе мгновенных сообщений и не понимают, почему они не могут вести все свои дела посредством текстовых сообщений.

Компьютеры сейчас важны, как никогда ранее. Если вы хотите, чтобы компьютеры работали, и работали хорошо, необходимо системное администрирование. Необходимы мы.

Структура книги

Эта книга состоит из следующих основных частей:

- Часть I «Введение». Это большая книга, поэтому мы начнем с обзора того, о чем вы здесь узнаете (глава 1), и нескольких советов, которые помогут вам сэкономить время, требуемое на прочтение книги (глава 2).
- Часть II «Основные элементы». Главы 3–14 посвящены основам информационной инфраструктуры, аппаратного и программного обеспечения, от которых зависит все остальное.
- Часть III «Процессы изменений». В главах 15–21 рассматриваются вопросы изменения системы, начиная с устранения мельчайших сбоев и заканчивая массовой реорганизацией.
- Часть IV «Предоставление услуг». В главах 22–29 приводятся советы по построению основных служб, таких как электронная почта, печать, хранение данных и веб-сервисы.
- Часть V «Методы управления». В главах 30–36 рассматриваются вопросы управления – независимо от того, есть ли в названии вашей должности слово «менеджер».
- В двух приложениях содержится обзор позитивных и негативных ролей системного администратора в организации и список сокращений, используемых в книге.

В каждой главе обсуждается отдельная тема. Некоторые темы технические, другие – нет. Если какая-то глава неприменима к вашему случаю, ее можно смело пропустить. Главы связаны ссылками, поэтому есть вероятность, что вы потом вернетесь к главе, которая раньше показалась вам скучной. Мы не обидимся.

В каждой главе есть два основных раздела. В разделе «Основы» обсуждаются темы первостепенной важности, которые вам просто необходимо усвоить. Пренебрегая этими вопросами, вы усложните себе работу в будущем. Относитесь к ним как к вложениям в будущую эффективность. В разделе «Тонкости» описаны секреты, которые помогут вам выполнять свою работу эффектно. Не тратьте на них свое время, пока не разберетесь с основами. Мы старались пояснять изложенное забавными историями и случаями из собственного опыта. Надеемся, это сделает наши советы более весомыми для вас. Никогда не доверяйте торговцам, которые не пользуются тем, что продают.

Изменения во втором издании

После выхода первого издания мы получили большое количество отзывов от читателей. Мы выступали на конференциях и в группах пользователей компьютеров по всему миру. Мы получили много электронных писем. Мы слушали. Делали заметки. Мы сгладили острые углы и заполнили основные пробелы.

Первое издание вызвало много положительных отзывов. Мы стали очень популярны. Тем не менее по прошествии времени некоторые главы устарели.

Первое издание, появившееся в книжных магазинах в августе 2001 года, по большей части писалось в 2000 году. С тех пор многое изменилось. В то время, после спада популярности доменов первого уровня, многое казалось угрожающим. ОС Windows 2000 была еще новинкой, лучшей системой считалась Solaris, а Linux пользовалась популярностью только среди фанатов. Спам был мелкой неприятностью, а не индустрией. Аутсорсинг потерял свою привлекательность и превратился из спасения для корпораций во всеобщее посмешище. Википедия была лишь проектом в умах энтузиастов, а не крупнейшей в мире свободной энциклопедией. Слово Google не было ни общеизвестным именем, ни глаголом[1]. Веб-«фермы» были редкостью, и «крупные сайты» посещались миллионы раз в день, а не в час. На самом деле у нас даже не было отдельной главы, посвященной запуску веб-серверов, так как мы считали, что вся необходимая информация выводится из правильного сочетания глав «Вычислительный центр», «Серверы», «Службы» и «Мониторинг служб». Что еще людям надо?

Как же все изменилось!

Linux перестала быть сомнительным явлением, Google набирает обороты, а «офшоринг» стало новым модным словечком. Расцвет Индии и Китая как экономических сверхдержав изменил наше представление о мире. AJAX и другие технологии Веб 2.0 возродили интерес к веб-приложениям.

Вот список изменений в книге:

- *Обновленные главы:* каждая глава была переработана и дополнена, добавлены новые забавные истории. Мы пояснили многие моменты. Мы многому научились за прошедшие пять лет, и это отразилось на всех главах. Упоминаемые устаревшие технологии были заменены на новые.
- *Новые главы:*
  - глава 9 «Документация»;
  - глава 25 «Хранение данных»;
  - глава 29 «Веб-службы».
- *Дополненные главы:*
  - Приложение B из первого издания, которое пропустили многие читатели, не дочитавшие книгу до конца, стало главой 1 «Что делать, если...».
  - Раздел «С чего начать» из вступительной части первого издания был дополнен и стал главой 2 «Как выбраться из ямы».

[1] В английском языке сейчас имеется глагол to google, да и в русском все чаще говорят «гуглить» вместо «искать в Интернете». – *Прим. перев.*

- *Измененное оглавление:*
  - Часть I «Введение». Вводный обзор содержания книги.
  - Часть II «Основные элементы». Основные составляющие любых ИТ-систем.
  - Часть III «Процессы изменений». Рекомендации по реализации изменений от мельчайших до крупнейших.
  - Часть IV «Предоставление услуг». Справочник по наиболее распространенным службам.
  - Часть V «Методы управления». Организационные проблемы.

Что дальше

Каждая глава посвящена отдельной теме. Вы можете читать их в любом порядке. Тем не менее мы тщательно выверили последовательность глав, так что информация будет более понятна, если читать книгу от начала до конца. В любом случае мы надеемся, что книга вам понравится. Мы многому научились и получили огромное удовольствие, когда ее писали. Итак, приступим.

Томас А. Лимончелли
Корпорация Google
tom@limoncelli.org

Кристина Дж. Хоган
Команда Формулы-1 BMW Sauber
chogan@chogan.com

Страта Р. Чейлап
Корпорация Virtual.Net
strata@virtual.net

P. S. В книгах, как и в программах, встречаются ошибки. Список изменений, а также новости и заметки и даже список рассылок, на которые можно подписаться, вы найдете на нашем сайте *www.EverythingSysAdmin.com*.

Благодарности

Благодарность за первое издание

Вряд ли мы сможем поблагодарить всех, кто так или иначе помогал нам, но все равно попытаемся это сделать. Главными источниками нашего вдохновения послужили книги «*The Practice of Programming*»[1] и «*Programming Pearls*»[2].

Мы благодарны компаниям Global Networking and Computing (GNAC), Synopsys и Eircom за разрешение использовать фотографии их информационных центров, чтобы проиллюстрировать реальные примеры грамотного применения принципов, о которых идет речь в книге.

Мы в долгу перед следующими людьми за их помощь в редактировании книги: Валери Наталь (Valerie Natale), Энн Мари Куинт (Anne Marie Quint), Джошем Саймоном (Josh Simon) и Амарой Уилли (Amara Willey).

Люди, с которыми мы встречались на конференциях USENIX, SAGE и LISA, оказали огромное влияние на нашу жизнь и карьеру. Мы не смогли бы написать эту книгу, если бы не познакомились с этими людьми и не научились у них многому.

Писать эту книгу нам помогали десятки людей. Кто-то просто рассказывал забавные случаи из жизни, кто-то давал советы по написанию книги, а кто-то был нашим наставником в работе. Единственный честный способ отблагодарить их всех – перечислить их имена в алфавитном порядке и заранее извиниться перед всеми, кто в этот список не вошел: Раджив Агравала (Rajeev Agrawala), Эл Ахо (Al Aho), Джефф Аллен (Jeff Allen), Эрик Андерсон (Eric Anderson), Энн Беннингер (Ann Benninger), Эрик Берглунд (Eric Berglund), Мелисса Бинд (Melissa Binde), Стивен Браниган (Steven Branigan), Шейла Браун-Клингер (Sheila Brown-Klinger), Брент Чэпмен (Brent Chapman), Билл Чесвик (Bill Cheswick), Ли Дэймон (Lee Damon), Тина Дарморэй (Tina Darmohray), Бах Туок (Дейзи) Дэвис (Bach Thuoc (Daisy) Davis), Р. Дрю Дэвис (R. Drew Davis), Инго Дин (Ingo Dean), Арнольд де Леон (Arnold de Leon), Джим Деннис (Jim Dennis), Барбара Диджкер (Barbara Dijker), Виктор Духовны (Viktor Dukhovni), Шель-Мари Элерс (Chelle-Marie Ehlers), Майкл Эрлингер (Michael Erlinger), Пол Эванс (Paul Evans), Рэми Эвард (Remy Evard), Лукман Фэйзал (Lookman Fazal), Роберт Фалмер (Robert

---

[1] Брайан У. Керниган, Роб Пайк «Практика программирования». – Пер. с англ. – Вильямс, 2004.

[2] Джон Бентли «Жемчужины программирования. 2-е издание». – Пер. с англ. – СПб.: Питер, 2002.

Fulmer), Карсон Гаспар (Carson Gaspar), Пол Глик (Paul Glick), Дэвид «Zonker» Гаррис (David «Zonker» Harris), Кэтрин «Cappy» Гаррисон (Katherine «Cappy» Harrison), Джим Хикштейн (Jim Hickstein), Сандра Генри-Стокер (Sandra Henry-Stocker), Марк Хортон (Mark Horton), Билл «Whump» Хамфриз (Bill «Whump» Humphries), Тим Хантер (Tim Hunter), Джефф Дженсен (Jeff Jensen), Дженнифер Джой (Jennifer Joy), Алан Джадж (Alan Judge), Кристоф Колт (Christophe Kalt), Скот К. Кеннеди (Scott C. Kennedy), Брайан Керниган (Brian Kernighan), Джим Ламберт (Jim Lambert), Элиот Лир (Eliot Lear), Стивен Левин (Steven Levine), Лес Ллойд (Les Lloyd), Ральф Лоура (Ralph Loura), Брайан Мак-Дональд (Bryan MacDonald), Шерри Мак-Брайд (Sherry McBride), Марк Меллис (Mark Mellis), Клифф Миллер (Cliff Miller), Хэл Миллер (Hal Miller), Рут Милнер (Ruth Milner), Д. Тоби Моррилл (D. Toby Morrill), Джо Моррис (Joe Morris), Тимоти Мерфи (Timothy Murphy), Рави Нарайан (Ravi Narayan), Нильс-Питер Нельсон (Nils-Peter Nelson), Эви Немет (Evi Nemeth), Уильям Нинке (William Ninke), Кэт Окита (Cat Okita), Джим Парадис (Jim Paradis), Пат Парсгиан (Pat Parseghian), Дэвид Партер (David Parter), Роб Пайк (Rob Pike), Хэл Померанц (Hal Pomeranz), Дэвид Пресотто (David Presotto), Даг Раймер (Doug Reimer), Томми Рейнголд (Tommy Reingold), Майк Ричичи (Mike Richichi), Мэттью Ф. Ринджел (Matthew F. Ringel), Деннис Ритчи (Dennis Ritchie), Пол Д. Роригстампер (Paul D. Rohrigstamper), Бен Розенгарт (Ben Rosengart), Дэвид Росс (David Ross), Питер Сэйлус (Peter Salus), Скот Шульц (Scott Schultz), Даррен Шоу (Darren Shaw), Гленн Зиб (Glenn Sieb), Карл Сиил (Karl Siil), Сисили Смит (Cicely Smith), Брайан Стэнселл (Bryan Stansell), Хэл Штерн (Hal Stern), Джей Стайлз (Jay Stiles), Ким Супсинкас (Kim Supsinkas), Кен Томпсон (Ken Thompson), Грег Тусар (Greg Tusar), Ким Уоллес (Kim Wallace), The Rabbit Warren, доктор философии Джери Вайтцман (Geri Weitzman), Глен Уайли (Glen Wiley), Пат Уилсон (Pat Wilson), Джим Уитгофф (Jim Witthoff), Фрэнк Войчик (Frank Wojcik), Джей Йу (Jay Yu) и Элизабет Звики (Elizabeth Zwicky).

Также благодарим корпорацию Lumeta и компанию Lucent Technologies/Bell Labs за поддержку при написании этой книги.

И последние в списке, но не по значению – сотрудники издательства Addison-Wesley, благодаря которым мы получили огромное удовольствие от написания книги. В частности, мы хотели бы поблагодарить Карен Гетман (Karen Gettman), Мэри Харт (Mary Hart) и Эмили Фрей (Emily Frey).

Благодарность за второе издание

Помимо всех тех, кто помогал нам с первым изданием книги, мы хотели бы поблагодарить людей, без помощи и поддержки которых второго издания никогда бы не было: Ли Дэймона (Lee Damon), Натана Дитча (Nathan Dietsch), Бенджамина Фина (Benjamin Feen), Стивена Гарриса (Stephen Harris), Кристину Е. Полк (Christine E. Polk), Гленна Е. Зиба (Glenn E. Sieb), Джухани Тали (Juhani Tali) и многочисленных сотрудников организации League of Professional System Administrators (LOPSA). Отдельный привет и наилучшие пожелания Майку Чейлапу (Mike Chalup) за любовь, верность и поддержку и, самое главное, за горы перестиранного белья и груды перемытой посуды, позволившие Страте заниматься книгой. А также крепко обнимаем и нежно целуем малышку Джоанну Лир (Joanna Lear) и благодарим ее за терпение.

Благодарим корпорацию Lumeta за разрешение на публикацию второго издания.

Спасибо Wingfoot за разрешение использовать их сервер для нашей базы данных отслеживания ошибок.

Благодарим Энн Мари Куинт за ввод данных, корректуру и массу отличных предложений.

И последние в списке, но не по значению – люди, которым мы приносим огромную гору благодарностей в стиле «без вас мы ничего не добились бы»: Марк Тауб (Mark Taub), Кэтрин Нолан (Catherine Nolan), Райна Чробак (Raina Chrobak) и Лара Уайсонг (Lara Wysong) из Addison-Wesley.

Об авторах

Том, Кристина и Страта познакомились друг с другом, посещая конференции USENIX и активно участвуя в деятельности сообщества системных администраторов. Именно на одной из таких конференций Том и Кристина впервые заговорили об этой книге. Страта и Кристина вместе работали в компаниях Synopsys и GNAC и в 1998 году совместно с другими авторами выпустили книгу.

Томас А. Лимончелли

Том – всемирно известный писатель и лектор, специализирующийся на системном администрировании, тайм-менеджменте и методах организации общественных политических движений. Том работал системным администратором с 1988 года. Ему приходилось работать как на небольшие, так и на крупные компании, включая Google, Cibernet Corp, Dean for America, Lumeta, AT&T, Lucent/Bell Labs и Mentor Graphics. В Google он занимался улучшением развертывания IT-инфраструктуры в новых офисах. После разделения AT&T на компании AT&T, Lucent и NCR Том возглавил группу, которая разделила компьютерную и сетевую инфраструктуру Bell Labs на три новые компании. Помимо первого и второго издания этой книги, в список его опубликованных трудов входит книга «Time Management for System Administration»[1], а также работы по безопасности, сетям, управлению проектами и карьерному менеджменту. Том часто посещает конференции и пользовательские группы, читает лекции, выступает на семинарах и презентациях, читает программные речи.

В свободное время Том принимает активное участие в общественной борьбе за гражданские права. Он получил награды и признание как на местном, так и на национальном уровне. Первая опубликованная работа Тома (1997 г.) была посвящена опыту, который системные администраторы могут перенять у активистов. По мнению Тома, нет особой разницы между его профессиональной карьерой и участием в общественных движениях. И здесь, и там он помогает людям.

Том получил степень бакалавра компьютерных наук, закончив университет Дрю. Сейчас он живет в городе Блумфилде (Bloomfield), штат Нью-Джерси, США.

Благодаря своему участию в жизни сообщества Том и Кристина в 2005 году были удостоены награды «Outstanding Achievement Award» (Награда за выдающиеся достижения) от USENIX/SAGE.

---

[1] Томас Лимончелли «Тайм-менеджмент для системных администраторов». – Пер. с англ. – СПб.: Символ-Плюс, 2007.

Кристина Дж. Хоган

Карьера Кристины в области системного администрирования началась на факультете математики в колледже Тринити (г. Дублин), где она проработала почти 5 лет. После этого она переехала на солнечную Сицилию. Там она проработала год в исследовательской компании. После этого 5 лет работы в Калифорнии. Проработав пару лет архитектором систем безопасности в Synopsys, Кристина перешла в компанию GNAC всего через несколько месяцев после ее основания. Там она работала с недавно созданными компаниями, сайтами электронной коммерции, биотехнологическими компаниями, крупными транснациональными компаниями, деятельность которых связана с оборудованием и программным обеспечением. Техническая сторона ее деятельности предполагала работу с системами безопасности и сетями, общение с пользователями и помощь в установке вычислительного центра GNAC и обеспечении подключения к Интернету. Кроме того, Кристина занималась управлением проектами, работой с пользователями и персоналом. Она провела в GNAC почти 3 года, после чего пустилась в свободное плавание, став независимым консультантом по безопасности и работая в основном с сайтами электронной коммерции.

С тех пор Кристина успела стать мамой и сменить карьеру. Теперь она работает специалистом по аэродинамике для команды Формулы-1 BMW Sauber. Кристина получила степень доктора в области авиационного машиностроения, закончив Имперский колледж Лондона; степень бакалавра математических наук и степень магистра компьютерных наук в Тринити-колледже в Дублине; а также диплом юридического факультета в Дублинском институте технологий.

Страта Р. Чейлап

Страта является владельцем и старшим консультантом корпорации Virtual.Net. Это фирма, специализирующаяся в области стратегического и методического IT-консалтинга и оказывающая помощь малым и средним компаниям в масштабировании IT-систем. Во время первого бума доменов первого уровня Страта занималась архитектурой масштабируемых инфраструктур, а также руководила архитекторами, работавшими с такими проектами, как talkway.net, Palm VII и mac.com.

В 1993 году было основано частное предприятие Virtual.Net, которое в 2005 году было зарегистрировано в качестве акционерного общества. Среди пользователей этой корпорации были такие компании, как Apple, Sun, Cimflex Teknowledge, Cisco, McAfee и Micronas USA.

Впервые Страта познакомилась с компьютерами в 1981 году. Она работала в системе TOPS-20 на компьютерах DEC, а в 1983 году полностью перешла на UNIX, работая в Ultrix на VAX 11-780, в Unisys на микросистемах Motorola 68K, а также в Minix на Intel. Страта обладает уникальной способностью смотреть на вещи с позиции человека, который был одновременно пользователем и администратором интернет-служб с 1981 года. Она была свидетелем развития того, что мы сейчас считаем современной сетью. В некоторых случаях она наблюдала за происходящим, как говорится, «из первых рядов». Страта быстро распознала потенциал компьютерных технологий. Она участвовала в первых слушаниях Национальной администрации телекоммуникационной инфраструктуры США (National Telecommunications Infrastructure Administration – NTIA) и в заседаниях по предоставлению грантов в 1993–1995 годах. В 1994 году

Страта продемонстрировала потенциальные возможности Интернета, проведя революционную виртуальную конференцию NTIA. Она является убежденной футуристкой и постоянно следит за новыми технологиями, которые можно применить в сфере информационных технологий и менеджмента.

В душе Страта всегда была предана Новой Англии, но живет она в Калифорнии вместе с супругом, не выносящим снег и морозы. Страта занимается садом, увлекается научной фантастикой и фэнтези, является волонтером-радиооператором служб спасения (позывной KF6NBZ). Кроме того, она сертифицированный аквалангист, хотя предпочитает прыжки в воду и плаванье с маской. Пару лет Страта путешествовала по стране на трейлере, став технокочевником[1], – сначала в 1990, а потом в 2002 году. В этот период она продолжала консультировать пользователей. Еще одним ее хобби стало изучение энергосберегающих методов строительства и дизайна, включая посещение семинаров для владельцев-застройщиков. И наконец, она действительно выросла на козьей ферме.

В отличие от ее знаменитых соавторов, у Страты нет высшего образования. Она ушла из Массачусетского технологического института (МТИ) со второго курса и никогда об этом не жалела. Впоследствии она несколько лет управляла Центром когнитивных наук МТИ, а также была консультантом вычислительной группы факультета компьютерной и электротехники МТИ. Кроме того, Страта год была администратором электронной почты МТИ, после чего отправилась в Кремниевую долину.

[1] Термин «технокочевник» (technomad) был впервые введен Стивеном Робертсом (Steven Roberts) и употребляется для обозначения путешественников, постоянно пользующихся средствами коммуникации, такими как Интернет. – *Прим. перев.*

Часть I
Введение

Глава 1

Что делать, если...

В этой главе мы собрали различные советы из всей книги, чтобы дать вам представление о том, как их можно применять на практике в повседневных ситуациях или находить ответы на распространенные вопросы системных администраторов и менеджеров.

1.1. Необходимо создать новую сеть

- Обдумайте необходимую организационную структуру. Глава 30.
- Согласуйте с руководством приоритеты задач, чтобы определить порядок их реализации.
- Тщательно спланируйте пространства имен. Глава 8.
- Создайте надежный вычислительный центр. Глава 6.
- Создайте надежную сеть с учетом будущего расширения. Глава 7.
- Создайте службы, которые можно будет масштабировать. Глава 5.
- Создайте систему хранения программного обеспечения или, по крайней мере, простой план иерархии каталогов, который впоследствии может послужить основой системы хранения ПО. Глава 28.
- Упорядочьте исходные основные используемые службы:
  - Аутентификация и авторизация. Раздел 3.1.3.
  - Управление жизненным циклом компьютера. Глава 3.
  - Электронная почта. Глава 23.
  - Файловые службы, резервное копирование. Глава 26.
  - Конфигурация сети. Раздел 3.1.3.
  - Печать. Глава 24.
  - Удаленный доступ. Глава 27.

1.2. Необходимо расширить небольшую сеть

- Создайте службу поддержки. Глава 13.
- Составьте списки новых работников, новых настольных компьютеров, ноутбуков и серверов. Раздел 3.1.1.5.
- Оцените возможности центра управления сетью, выделенного для мониторинга и координирования работы сети. Глава 22.

- Продумайте структуру отдела и потребность в новых сотрудниках и подготовьте статистические данные по решенным и нерешенным проблемам. Глава 30.
- Ведите мониторинг пропускной способности и доступности служб, чтобы предсказать, когда их нужно масштабировать. Глава 22.
- Будьте готовы к наплыву новых компьютеров, сотрудников и системных администраторов. Разделы 1.23, 1.24 и 1.25.

1.3. Необходимо выйти на мировой уровень

- Разработайте архитектуру вашей глобальной вычислительной сети (Wide Area Network, WAN). Глава 7.
- Следуйте трем основным правилам: масштабировать, масштабировать и еще раз масштабировать.
- Синхронизируйте время на серверах со временем по Гринвичу (Greenwich Mean Time, GMT), чтобы иметь возможность эффективно анализировать лог-файлы.
- Добейтесь того, чтобы ваша служба поддержки действительно работала круглосуточно и без выходных. Найдите способ повлиять на системных администраторов в других временных зонах. Глава 13.
- Рассчитывайте архитектуру служб с учетом удаленных соединений – как правило, с малой пропускной способностью и менее надежных. Глава 5.
- Настройте приложения для использования на соединениях с большими задержками. Раздел 5.1.2.
- Обеспечьте, чтобы безопасность и разграничение прав доступа соответствовали требованиям глобальной сети.

1.4. Необходимо заменить службы

- Следите за ходом изменений. Глава 18.
- Учитывайте при планировании замены зависимости сети и зависимости служб.
- Измените сроки аренды сетевых адресов по протоколу DHCP (Dynamic Host Configuration Protocol) с учетом перехода. Раздел 3.1.4.1.
- Избегайте жесткого указания имен серверов в конфигурации. Вместо этого жестко указывайте псевдонимы (алиасы), которые будут перемещаться вместе со службой. Раздел 5.1.6.
- Измените значения времени жизни (TTL) в DNS для переключения на новые серверы. Раздел 19.2.1.

1.5. Необходимо переместить вычислительный центр

- Запланируйте перерывы, если система не полностью дублирована и вы не можете сначала перенести одну половину системы, а потом вторую. Глава 20.

- Удостоверьтесь, что новый вычислительный центр рассчитан как на текущую нагрузку, так и на возможное расширение. Глава 6.
- Сделайте резервные копии файловых систем всех машин перед их перемещением.
- Проведите тестирование ваших резервных копий. Раздел 26.2.1.
- Перед перемещением выработайте алгоритмы тестирования и после перемещения тестируйте, тестируйте и еще раз тестируйте все. Глава 18.
- Промаркируйте каждый кабель, прежде чем его отключить. Раздел 6.1.7.
- На новом месте с новой аппаратурой установите минимально необходимые службы на резервное оборудование.
- До начала перемещения протестируйте всю новую аппаратуру – сеть, электропитание, источники бесперебойного питания (UPS), системы отопления, вентиляции и кондиционирования и т. д. Глава 6, особенно раздел 6.1.4.
- Выберите небольшую группу пользователей для рабочего тестирования минимальных служб, затем проведите тесты по стандартным сценариям, прежде чем перемещать что-то еще.
- Запустите охлаждение на 2–3 суток, а затем замените все фильтры, прежде чем начать заполнять помещение.
- Проведите генеральную репетицию. Раздел 18.2.5.

1.6. Необходимо переехать в другое или новое здание

- Заранее, за месяц или более, получите доступ к новому помещению, чтобы создать инфраструктуру.
- Для связи внутри здания пользуйтесь портативными рациями. Глава 6 и раздел 20.1.7.3.
- Используйте карманный компьютер (КПК) или неэлектронный органайзер. Раздел 32.1.2.
- Заранее, за 2–3 месяца, подключитесь к Интернету.
- Сообщите руководству, что подключение к Интернету займет несколько месяцев и должно быть сделано в первую очередь.
- Проложите сетевой кабель во время, а не после строительства офиса. Раздел 7.1.4.
- Сотрудничайте с той компанией по перевозкам, которая поможет вам спланировать переезд.
- Назначьте ответственного за ведение списка всех переезжающих сотрудников, их новых номеров офиса, расположения кабинета и т. д.
- Назначьте дату утверждения окончательной версии списка. Передайте копии списка компании по перевозкам, пользуйтесь списком при печати ярлыков и т. д. Если после этой даты изменится чье-то размещение, не пытайтесь внести изменения во все розданные копии списка. Переместите сотруд-

ника в соответствии с основным списком и запланируйте второе перемещение после окончания переезда.

- Распечатайте и раздайте всем по листу с 12 ярлыками с их именами и новым местом, чтобы пометить коробки, пакеты и персональные компьютеры (PC). Если вам не хочется этим заниматься, хотя бы дайте людям инструкции, как и что написать на каждой коробке, чтобы она была доставлена по назначению.
- Раздайте всем пластиковые пакеты, достаточно большие, чтобы туда поместились все кабели от персонального компьютера. Технически грамотные сотрудники могут самостоятельно отключить и подключить компьютеры по прибытии, а людям, далеким от техники, должны помочь системные администраторы.
- Всегда заказывайте больше коробок, чем требуется для переезда.
- Не используйте картонные коробки. Пользуйтесь пластиковыми ящиками, которые можно использовать повторно.

1.7. Необходимо часто переезжать

- Добейтесь выделения одного дня в неделю для переездов. Составьте расписание работ на каждый день.
- Утвердите методику и форму, в которой вы будете собирать необходимую информацию о персональном оборудовании сотрудников, количестве сетевых и телефонных подключений, а также об особых требованиях. Дайте задание системным администраторам заранее собирать информацию о нестандартном оборудовании и делать заметки.
- Заблаговременно подключите и протестируйте сетевые кабели.
- Скажите пользователям, чтобы перед переездом они отключили питание компьютеров и собрали в помеченные коробки все кабели, мыши, клавиатуры и прочие комплектующие, которые могут потеряться.
- Проведите коллективное обсуждение всех возможностей привлечь сотрудников к работе по переезду. Будьте внимательны при оценке их уровня навыков. Возможно, некоторым людям не стоит доверять делать что-либо самостоятельно.
- Перевозкой оборудования должна заниматься транспортная компания. Для распаковки, подключения и тестирования должна быть выделена команда системных администраторов. Будьте осторожны при выборе компании по перевозкам.
- Обучите службу поддержки уделять особое внимание пользователям, сообщающим о появившихся после переезда проблемах, которых не было до переезда. Такие заявки в первую очередь надо передавать команде, занимающейся переездом, в обход стандартных процедур рассмотрения.
- Формализация процесса, выделение для него одного дня в неделю, проведение подготовительных работ и выделенная команда для переездов сделают процесс более плавным, с меньшими задержками для пользователей и меньшим количеством связанных с переездом проблем у системных администраторов.

1.8. Необходимо провести инспекцию сети

- Используйте главы и разделы этой книги, чтобы составить предварительный список тем для проверки, взяв пункты из разделов «Основы» за приблизительный образец хорошо организованной сети.
- Убедите системных администраторов и менеджеров организации, что ваша задача – не выносить оценку, а выяснить, как работает их сеть, чтобы понять сходство и различие между ней и теми сетями, с которыми вам приходилось работать ранее. Это важно как в работе консультанта, так и в подведении результатов инспекции для потенциального поглощения.
- Ведите документацию вашей команды в личной базе данных (например, wiki). Объемы собираемой информации превысят вашу способность запоминать: документируйте, документируйте и еще раз документируйте.
- Составьте или запросите инвентарный список оборудования – рабочих станций и серверов, – а также схему локальной сети и описание производственной деятельности служб. Это делается с целью выработать разные точки зрения на инфраструктуру.
- Изучите доменную аутентификацию и обратите особое внимание на разделение доступа и защиту информации.
- Проанализируйте статистику времени прихода и ухода сотрудников месяц за месяцем. Ищите заметное увеличение задержек персонала на работе, свидетельствующее о перегрузке сотрудников или о хронических затруднениях в работе инфраструктуры.

1.9. Необходимо проводить слияния и поглощения

- Если планируется серия слияний и поглощений, договоритесь, чтобы вам предоставляли информацию как можно раньше, даже если назначенные сотрудники получат сведения, которые не позволят им вести сделки с акциями в течение определенного периода.
- Некоторые слияния требуют мгновенного подключения нового подразделения. В других случаях запрещено полностью подключать филиал в течение месяца или около того, пока не будут подписаны необходимые документы. В первом случае предупредите, что это невозможно, если вас не известят заранее (см. предыдущий пункт). Во втором случае у вас будет небольшая передышка, но действуйте быстро!
- Если вы – директор, то должны привлечь директора по информационным технологиям (CIO) заранее, до объявления о слиянии.
- Если вы – системный администратор, постарайтесь выяснить, кто в другой компании принимает серьезные решения.
- Выработайте четкую процедуру принятия окончательного решения.
- Выберите по одному ответственному за слияние от каждой компании.
- Начните диалог с системными администраторами из другой компании. Выясните структуру их службы поддержки, уровни сервисов, сетевую архитектуру, модель и политики безопасности. Определите, как будет выглядеть новая модель.

- Организуйте хотя бы одну личную встречу с системными администраторами из другой компании. На знакомых людей злиться намного сложнее.
- Переходите к техническим подробностям. Возникнет ли конфликт в пространстве имен? Если да, определите, каким образом вы намерены этот конфликт устранить. Глава 8.
- Используйте лучшие наработки обеих компаний. Не стоит слепо следовать политике компании только потому, что она крупнее.
- Учитывайте культурные различия между сотрудниками обеих компаний. Разница во мнениях может принести пользу, если люди научатся уважать друг друга. Разделы 32.2.2.2 и 35.1.5.
- Удостоверьтесь, что системным администраторам в обеих компаниях предоставлен доступ к детализированным диаграммам обеих сетей, а также к подробным картам локальной сети (Local Area Network, LAN) обеих компаний. Глава 7.
- Определите, как должна выглядеть новая сетевая архитектура. Глава 7. Каким образом будут связаны две сети? Будут ли создаваться удаленные подразделения? Как будет выглядеть новая модель безопасности или периметр безопасности? Глава 11.
- Узнайте у руководства подробности, касающиеся корпоративной политики: именование учетных записей пользователей, формат адресов электронной почты и имя домена. Корпоративная политика будет единой или она будет различаться? Каким образом это повлияет на инфраструктуру электронной почты и интернет-служб?
- Выясните, как к слиянию относятся все пользователи или деловые партнеры и не хотят ли они защитить свою интеллектуальную собственность от другой компании. Глава 7.
- Сравните разные виды политики безопасности, описанные в главе 11. В частности, изучите разницу в политиках секретности, политиках безопасности и их взаимосвязи с деловыми партнерами.
- Сравните таблицы маршрутизации обеих компаний. Удостоверьтесь, что используемые пространства IP-адресов не пересекаются. В частности, такая проблема может возникнуть, если обе компании используют адресное пространство RFC 1918 (Lear et al. 1994, Rekhter et al. 1996).
- Обдумайте возможность установки брандмауэра между двумя компаниями до обеспечения совместимости их политик безопасности. Глава 11.

1.10. Необходимо справиться с частыми сбоями в работе компьютеров

- Используйте временные приемы для устранения ошибок и сообщите пользователям, что это временные меры.
- Установите истинную причину сбоев. Глава 15.
- Устраните истинную причину, а не симптомы. Глава 16.
- Если основная причина заключается в оборудовании, приобретите лучшее оборудование. Глава 4.
- Если основная причина заключается в условиях, улучшите физические условия для вашего оборудования. Глава 6.

- Переустановите систему. Глава 18.
- Обучите ваших системных администраторов эффективнее использовать инструменты диагностики. Глава 15.
- Как можно быстрее запустите производственную систему. Не стоит играть в диагностические игры с производственными системами. Для этого существуют лаборатории и заранее объявленные профилактические перерывы (которые, как правило, устраиваются в выходные или поздно вечером).

1.11. Необходимо предупредить возможность массового простоя в работе

- Попробуйте смоделировать свои действия при простое в системе контроля инцидентов (СКИ). Эта специальная система управления совершенствовалась на протяжении многих лет ведомствами общественной безопасности с целью разработки гибких методик действий в чрезвычайных ситуациях. Самая эффективная стратегия в таких случаях – определить последовательность действий в критической ситуации *до того, как возникнут проблемы*.
- Сообщите пользователям, что вы в курсе возникших проблем, по информационным каналам, предназначенным для связи с вами: раздел простоев в службе поддержки во внутренней сети, исходящее сообщение на телефон системного администратора и т. д.
- Сформируйте «группу быстрого реагирования», в которую войдут системные администраторы, члены руководства и основные заинтересованные лица. Проведите короткое собрание (15–30 мин) с целью определения конкретных задач, таких как «заставить разработчиков возобновить работу», «восстановить пользователям доступ к службе поддержки» и т. д. Сделайте все возможное, чтобы добиться намеченного, а не просто продублировать те или иные функциональные возможности.
- Определите затраты на реализацию обходных путей или запасных вариантов по сравнению с потерями из-за простоя в работе. Пусть вопрос о времени, которое стоит потратить на решение проблемы, решают руководители и заинтересованные стороны. Если для определения цифр недостаточно информации, на общем собрании обязательно назначьте время следующей попытки.
- На сбор информации потратьте не больше часа. Затем проведите общее собрание и представьте руководству и заинтересованным сторонам варианты решения проблемы. Сотрудники должны каждый час предоставлять пассивные уведомления о состоянии работы.
- Если коллектив примет решение устранить проблему и попытаться применить обходной путь, распланируйте порядок внедрения исправлений. Обращайтесь за помощью к заинтересованным сторонам после того, как узнаете, сработало то или иное решение либо нет. Хотя бы кратко документируйте свои действия, чтобы предотвратить повторение решений, если вам снова придется столкнуться с этой проблемой через несколько часов или дней.
- При попытке исправить проблему внедряйте по два-три решения, чтобы в целом на это ушло не более часа. Собирайте сообщения об ошибках или

ведите журнал относящихся к делу данных, а на следующем общем собрании сделайте по ним отчет.

- Не позволяйте ни одному сотруднику, даже обладающему очень высокой квалификацией, спонтанно предпринимать какие-то меры. Так как у вас нет возможности предсказать, сколько именно продлится простой в работе, необходимо следовать четким правилам и всех держать в курсе происходящего.
- Назначьте ответственного за доставку еды, документирование, а также за то, чтобы мягко, но настойчиво отстранять людей от решения проблемы, если они слишком устали или расстроены и не могут продолжать работу.

1.12. Какие рабочие инструменты должны быть у каждого системного администратора

- Ноутбук со средствами сетевой диагностики, такими как сетевой анализатор пакетов, DHCP-клиент в режиме расширенного вывода, TELNET/SSH-клиент с шифрованием, TFTP-сервер и т. п., а также проводная и беспроводная сеть Ethernet.
- Программный эмулятор терминала и последовательный кабель. Ноутбук может сыграть роль последовательной консоли в экстренных ситуациях, например при сбое консольного сервера, сбое в консоли вычислительного центра или при необходимости получить доступ к серверу за пределами вычислительного центра.
- Дополнительный компьютер или сервер для экспериментов с новыми конфигурациями. Раздел 19.2.1.
- Портативный принтер для ярлыков. Раздел 6.1.12.
- КПК или неэлектронный органайзер. Раздел 32.1.2.
- Набор отверток всех размеров, используемых для компьютеров.
- Кабельный тестер.
- Устройство для обжимки кабеля.
- Патч-кабели разной длины, в том числе один или два 30-метровых. Они могут быть полезны в самых непредсказуемых ситуациях.
- Компактный цифровой фотоаппарат. При необходимости можно отправить в службу поддержки снимок, который поможет расшифровать непонятные сообщения в консоли, определить номер модели или станет подтверждением повреждений.
- Портативный жесткий диск с подключением через USB/FireWare.
- Рация для поддержания связи в здании. Глава 6 и раздел 20.1.7.3.
- Шкаф с рабочими инструментами и комплектующими. Раздел 6.1.12.
- Высокоскоростная связь с домами сотрудников отдела и необходимые средства связи.
- Библиотека со стандартным набором справочников по технологиям, с которыми работают системные администраторы. Разделы 33.1.1, 34.1.7 и список литературы.

- Членство в профессиональных сообществах, таких как USENIX и LOPSA. Раздел 32.1.4.
- Самые разнообразные лекарства от головной боли. Очень сложно решать серьезные проблемы, если болит голова.
- Распечатанный и помещенный в рамку Этический кодекс системных администраторов. Раздел 12.1.2.
- Стратегический запас чипсов (только для экстренных ситуаций).
- Копия этой книги!

1.13. Необходимо обеспечить возврат рабочего инструмента

- Упростите процесс возврата рабочих инструментов. На каждый из них наклейте ярлык с надписью «Вернуть [кому]».
- Если кто-то что-то у вас берет, откройте заявку в службе поддержки и закройте ее только после того, как вам вернут вашу вещь.
- Смиритесь с тем фактом, что ваши вещи могут вам и не вернуть. Зачем расстраиваться из-за ситуации, которую вы не в силах контролировать?
- Создайте общую базу инструментов и составьте график ответственных лиц, которые будут следить за наличием необходимых инструментов и отслеживать должников.
- У вас всегда должны быть запасные наборы компьютерных отверток. Если кто-нибудь попросит у вас одну отвертку, улыбнитесь и ответьте: «Нет, но можете взять в подарок весь набор». Обратно набор не берите.
- Не давайте отвертки тем, кто отвечает только за программное обеспечение. Вежливо поинтересуйтесь, для чего им нужна отвертка, и все сделайте сами. Это сэкономит вам время на исправление чужих ошибок.
- Если вы отвечаете лишь за программное обеспечение, пользуйтесь отверткой только под присмотром взрослых.
- У вас должен быть запас недорогих наборов для ремонта очков.

1.14. Для чего нужна документация к системам и процедурам

- Качественная документация описывает, для *чего* и *как* все делается.
- Если все делаешь правильно и все «просто получается», даже вы забудете подробности, когда необходимо будет исправить или усовершенствовать созданные проекты.
- Она позволяет уйти в отпуск. Раздел 32.2.2.
- Можно заняться более интересными проектами, вместо того чтобы делать одно и то же, будучи единственным человеком, понимающим принцип работы созданного проекта. Раздел 22.2.1.

- У вас будет репутация одного из лучших работников компании: вас ждут повышение зарплаты, премии, повышение по службе (или, по крайней мере, слава и деньги).
- Вам не придется сходить с ума в поисках информации, если инвесторы или аудиторы срочно ее потребуют.

1.15. Для чего нужны письменные инструкции

- Чтобы удовлетворить требования федеральных законов о здравоохранении и предпринимательской деятельности.
- Чтобы не производить впечатление, будто вы «придумываете все на ходу». Чтобы у других сотрудников не возникали проблемы из-за решений старших руководителей.
- Другие люди не умеют читать ваши мысли. Раздел A.1.17.
- Чтобы не обмануть ожидания не только ваших пользователей, но и вашего коллектива. Раздел 11.1.2 и глава 12.
- Люди должны быть уведомлены о том, что вступает в силу инструкция, которая их касается.
- Чтобы люди не были наказаны за то, что не умеют читать ваши мысли. Раздел A.1.17.
- Чтобы дать компании шанс конструктивно изменить методы работы или оттеснить конкурентов.

1.16. Необходимо определить основные проблемы в окружении

- Просмотрите раздел «Основы» в каждой главе.
- Проведите опрос среди руководителей, которые отвечают за финансирование. Глава 30.
- Проведите опрос двух-трех пользователей, прибегающих к вашим услугам. Раздел 26.2.2.
- Проведите опрос пользователей.
- Определите, на решение каких проблем у вас уходит больше всего времени. Раздел 26.1.3.
- Узнайте у сотрудников службы поддержки, с каким проблемами к ним чаще всего обращаются. Разделы 15.1.6 и 25.1.4.
- Узнайте у тех, кто отвечает за конфигурирование устройств, с какими проблемами им чаще всего приходится сталкиваться и какие претензии им чаще всего предъявляют пользователи.
- Определите, является ли ваша архитектура достаточно простой, чтобы вы могли нарисовать ее план на доске. Если нет, возможно, и управлять ею будет слишком сложно. Раздел 18.1.2.

1.17. Необходимо увеличить финансирование проектов

- Сделайте так, чтобы ваше руководство осознало всю необходимость этого.
- Выясните, что требуется руководству, и объясните, каким образом послужат этой цели проекты, для которых вам нужны деньги.
- Участвуйте в бюджетном планировании. Разделы 33.1.1.12 и 34.1.6.
- Добивайтесь максимальных результатов при минимальных затратах. Удостоверьтесь, что ваши сотрудники обладают хорошими навыками тайм-менеджмента. Раздел 32.1.2.
- Научитесь лучше руководить своим начальником. Раздел 32.2.3.
- Выясните, какие методы общения использует руководство, и используйте совместимые методы. Главы 33 и 34.
- Не работайте сверхурочно. Откажитесь от методов кризисного управления. Демонстрируйте руководству «истинную стоимость» инструкций и решений.

1.18. Необходимо обеспечить выполнение проектов

- Как правило, проекты не выполняются, потому что системные администраторы параллельно работе над проектами вынуждены устранять текущие аварии. Прежде всего разберитесь с этой проблемой.
- Найдите спонсора-организатора. Данный проект необходим для компании или это лишь инициатива системных администраторов? В первом случае найдите спонсора, который будет заниматься сбором ресурсов и отклонять конфликтующие требования. Во втором случае, возможно, за завершением проекта вообще следить не стоит.
- Удостоверьтесь, что в распоряжении системных администраторов есть все необходимые ресурсы (не стоит гадать, спросите их об этом напрямую).
- Ваши сотрудники должны отчитываться по окончании сроков и завершении определенных этапов работы.
- Расскажите системным администраторам о приоритетах, перераспределите ресурсы на более важные проекты. Раздел 33.1.4.2.
- Удостоверьтесь, что все участники проекта обладают хорошими навыками тайм-менеджмента. Раздел 32.1.2.
- Распределите задачи таким образом, чтобы одни сотрудники работали исключительно над проектами, а остальные занимались текущими делами, давая возможность первой группе не отвлекаться. Раздел 31.1.3.
- Уменьшите количество проектов.
- Не стоит тратить время на проекты, не имеющие ощутимой ценности. Рис. 33.1.
- Расставьте приоритеты → сконцентрируйтесь → добейтесь успеха.
- Для завершения самых значимых проектов воспользуйтесь услугами приглашенного консультанта, обладающего опытом в данной области. Разделы 21.2.2, 27.1.5 и 30.1.8.

- Наймите младших служащих для выполнения простых задач, таких как поддержка настольных систем, ежедневное резервирование данных и т. д. Таким образом, у системных администраторов будет больше времени на более значимые проекты.
- Для написания необходимого кода нанимайте программистов по краткосрочному договору.

1.19. Пользователи должны быть довольны

- Произведите хорошее впечатление на новых пользователей. Раздел 31.1.1.
- *Больше общайтесь* с уже имеющимися пользователями. Раздел 31.2.4 и глава 31.
- Приглашайте их на обед. Будьте хорошим слушателем. Раздел 31.2.7.
- Создайте веб-страницу о состоянии системы. Раздел 31.2.1.
- Создайте локальный корпоративный портал для сети, которую вы администрируете. Раздел 31.2.1.
- Избавьтесь от худших работников, особенно если их ошибки создают дополнительную работу для других. Глава 36.
- Проанализируйте, не подает ли определенный пользователь или группа пользователей необычное количество претензий или жалоб по сравнению со средним показателем. Если это так, договоритесь о встрече с руководителем пользователя или своим руководителем и сообщите ему о создавшейся ситуации. Организуйте собрание по решению этой проблемы, в котором примут участие руководитель пользователя и заинтересованные стороны, назначенные руководством. Определитесь с приоритетами и разработайте план действий по решению этой проблемы.

1.20. Начальство должно быть довольно

- Если у руководителя возникли к вам претензии, организуйте с ним личную встречу. *Не пытайтесь* решить такие вопросы по электронной почте.
- Выясните, каковы приоритеты вашего руководства, и сделайте их своими приоритетами. Раздел 32.2.3.
- Выясните, какие методы общения использует руководство, и используйте совместимые методы. Главы 33 и 34.
- Убедитесь, что сотрудники, выполняющие специализированные задачи, понимают эти задачи. Приложение А.

1.21. Системные администраторы должны быть довольны

- Убедитесь, что их непосредственный руководитель умеет эффективно управлять ими. Глава 33.
- Убедитесь, что руководство поддерживает руководителя системных администраторов. Глава 34.

- Убедитесь, что системные администраторы могут сами о себе позаботиться. Глава 32.
- Убедитесь, что системные администраторы понимают и хотят выполнять свою работу. Приложение А.
- Если у системных администраторов слишком много работы, убедитесь, что они эффективно распределяют свое рабочее время. Раздел 32.1.2. Или наймите дополнительных сотрудников и разделите обязанности. Глава 35.
- Увольняйте любого системного администратора, который провоцирует недовольство других работников. Глава 36.
- Убедитесь, что все новые работники обладают позитивным настроем. Раздел 13.1.2.

1.22. Необходимо предотвратить слишком медленную работу систем

- Дайте точное определение слову «*медленный*».
- Используйте системы мониторинга, чтобы определить узкие места. Глава 22.
- Анализируйте информацию подстройки производительности, характерную для каждой архитектуры, чтобы знать, что именно необходимо контролировать и как это нужно делать.
- Порекомендуйте решение, основанное на ваших выводах.
- Точно выясните, в чем заключается проблема, прежде чем начнете ее решать. Глава 15.
- Вы должны понимать разницу между временем ожидания и пропускной способностью. Раздел 5.1.2.

1.23. Необходимо справиться с резким увеличением числа компьютеров

- Вы должны понимать *экономическую разницу* между оборудованием для *обычного компьютера* и *сервера*. Сделайте так, чтобы ваш руководитель или финансовый директор понял эту разницу, иначе он откажется приобретать дорогостоящие серверы. Раздел 4.1.3.
- Вы должны понимать физическую разницу между оборудованием для *обычного компьютера* и *сервера*. Раздел 4.1.1.
- Определитесь с небольшим количеством стандартных конфигураций оборудования и приобретите это оборудование оптом. Раздел 3.2.3.
- Убедитесь, что вы обеспечили автоматическую установку, конфигурирование и обновление узла сети. Глава 3.
- Проверяйте энергоснабжение, размещение, системы отопления, вентиляции и кондиционирования воздуха в вашем вычислительном центре. Глава 6.
- Удостоверьтесь, что даже в небольших компьютерных залах и кабинетах установлены кондиционеры. Раздел 2.1.5.5.
- Если новые компьютеры предназначены для новых работников, см. раздел 1.24.

1.24. Необходимо справиться с резким увеличением числа новых пользователей

- Процедура найма сотрудников должна гарантировать, что новые компьютеры и учетные записи будут настроены до того, как сотрудники приступят к своим обязанностям. Раздел 31.1.1.
- У вас должен быть резерв стандартно настроенных и готовых к использованию компьютеров.
- Обеспечьте автоматическую установку, конфигурирование и обновление узла сети. Глава 3.
- Подготовьте соответствующие инструкции для новых пользователей. Удостоверьтесь, что обучение новых пользователей будет проводить квалифицированный персонал. Раздел 31.1.1.
- Удостоверьтесь, что на каждом компьютере установлено не менее одной простой игры, а также CD/DVD-проигрыватель. Это поможет новым пользователям быстрее освоиться с новыми машинами.
- Удостоверьтесь, что электросеть помещения выдержит повышение энергопотребления.
- Если каждую неделю в вашу компанию приходят десятки новых сотрудников, договоритесь с отделом кадров, чтобы все они приступали к работе в определенный день недели, например в понедельник. Таким образом все задачи, относящиеся к информационным технологиям, можно будет решать одновременно, что сэкономит время.

1.25. Необходимо справиться с резким увеличением числа системных администраторов

- Назначьте наставников для младших системных администраторов. Разделы 33.1.1.9 и 35.1.5.
- Проведите инструктаж для системных администраторов всех уровней, чтобы новые сотрудники понимали ключевые процессы и правила. Удостоверьтесь, что они понимают, к кому именно они должны обращаться за помощью.
- Ведите необходимую документацию, особенно важно использовать wiki. Глава 9.
- Приобретите необходимые справочники, как технические, так и вспомогательные: по тайм-менеджменту, общению, навыкам персонала. Глава 32.
- Оптом приобретите оборудование, перечисленное в разделе 1.12.

1.26. Необходимо справиться с высокой текучестью кадров в отделе системного администрирования

- Когда системный администратор увольняется, лишите его доступа ко всем системам. Глава 36.

- Удостоверьтесь, что отдел кадров оформляет увольнение сотрудников должным образом.
- Ваши сотрудники должны знать, что вы готовы выслушать их жалобы в частном порядке.
- Проводите собрания, на которых ваши сотрудники смогут оценивать вашу работу.
- Дайте возможность сотрудникам анонимно оценивать вашу работу.
- Определите, в чем вы как руководитель можете ошибаться. Главы 33 и 34.
- Используйте способы повышения морального духа. Пусть ваши сотрудники вместе разработают дизайн футболки. Футболки стоимостью около десяти долларов могут гораздо эффективнее повысить мотивацию сотрудников, чем тысячи долларов прибыли компании.
- Сделайте так, чтобы все сотрудники отдела прочли главу 32.
- Если многие уходят из-за одной паршивой овцы в отделе, избавьтесь от нее (или от него).

1.27. Необходимо справиться с высокой текучестью кадров среди пользователей

- Удостоверьтесь, что руководство своевременно дает указания системным администраторам заблокировать регистрационные записи, удаленный доступ и т. д. Глава 36.
- Удостоверьтесь, что сотрудники при увольнении возвращают все оборудование и программное обеспечение, принадлежащие компании.
- Примите необходимые меры, предотвращающие воровство при увольнении сотрудников.
- Примите необходимые меры, предотвращающие кражу интеллектуальной собственности. По возможности заблокируйте удаленный доступ.

1.28. Вы только что устроились на работу в отдел

- Прежде чем высказывать свое мнение, задавайте вопросы, чтобы вы были уверены, что правильно понимаете ситуацию.
- Организуйте частную встречу с каждым своим коллегой.
- Организуйте формальные и неформальные встречи с пользователями. Глава 31.
- Старайтесь произвести хорошее первое впечатление, особенно на пользователей. Раздел 31.1.1.
- Доверяйте своим коллегам, когда они рассказывают вам о проблемах в отделе. Не стоит немедленно отвергать их мнение.
- Не стоит слепо верить коллегам, когда они рассказывают вам о проблемах в отделе. Сначала проверьте их слова.

1.29. Вы только что устроились на работу руководителем отдела

- Готовится запуск новой системы или переоборудование? Остановите запуск, пока не удостоверитесь, что все соответствует вашим самым высоким требованиям. Не допускайте, чтобы некомпетентность вашего предшественника стала вашей первой серьезной ошибкой.
- Организуйте частную встречу с каждым своим подчиненным. Спросите, чем он (или она) занимается, к какой должности стремится, кем видит себя через год. Спросите, что вы можете сделать, чтобы добиться максимальной отдачи от этого подчиненного. Цель таких встреч – слушать, а не говорить самому.
- Организуйте еженедельные групповые собрания сотрудников.
- Добейтесь частной встречи со своим руководителем. Организуйте частные встречи с коллегами, чтобы узнать их мнение.
- С самого первого дня на работе дайте своим подчиненным понять, что вы верите в успех каждого из них. Глава 33.
- Организуйте формальные и неформальные встречи с пользователями. Глава 31.
- Спросите у каждого, какие проблемы могут возникнуть в отделе. Внимательно выслушайте всех, а затем рассмотрите доказательства и сделайте собственные выводы.
- Прежде чем высказывать свое мнение, задавайте вопросы, чтобы вы были уверены, что правильно понимаете ситуацию.
- Если вас наняли для того, чтобы вы подтянули отстающий отдел, отложите реализацию рискованных проектов, таких как общая замена системы электронной почты, до тех пор, пока вы не проведете необходимые реформы в коллективе или не найдете новых сотрудников.

1.30. Вы ищете новую работу

- Решите для себя, почему вы хотите сменить работу. Определитесь со своими целями.
- Определите для себя, какую должность вы хотите занять на новой работе. Приложение А.
- Определите для себя, в организациях какого типа вам больше всего нравится работать. Раздел 30.3.
- Организуйте встречу с максимально возможным количеством ваших потенциальных коллег, чтобы побольше узнать о коллективе. Глава 35.
- Не стоит сразу же соглашаться на первое предложение. Первое предложение – это всего лишь предложение. Торгуйтесь! Но помните, что до третьего предложения дело может и не дойти. Раздел 32.2.1.5.
- Требуйте письменное подтверждение важных для вас аспектов: участие в конференциях, обучение, отпуск.

- Не стоит устраиваться на работу в компанию, если вам отказывают в собеседовании с вашим потенциальным начальником.
- Если кто-то абсолютно серьезно говорит: «Нет никакой необходимости показывать этот договор вашему адвокату», вам определенно стоит показать договор адвокату. И мы это говорим абсолютно серьезно.

1.31. Необходимо быстро нанять много новых системных администраторов

- Прочитайте советы в главе 35.
- Используйте как можно больше разных методов подбора кадров. Организуйте увлекательные мероприятия на соответствующих конференциях, пользуйтесь интернет-форумами, спонсируйте местные пользовательские группы, организуйте открытые семинары в компании с участием знаменитостей, приглашайте людей по совету системных администраторов и пользователей. Глава 35.
- Удостоверьтесь, что у вас работает квалифицированный специалист по кадрам, а в отделе кадров знают, что такое хороший системный администратор.
- Определите для себя, какого уровня и подготовки вам нужны системные администраторы и сколько их должно быть. Используйте систему классификации, выработанную ассоциацией SAGE. Раздел 35.1.2.
- Когда найдете подходящего кандидата, *действуйте быстро*.
- Наняв одного человека, уточните требования к остальным должностям, чтобы заполнить возможные пробелы. Раздел 30.1.4.

1.32. Необходимо повысить надежность всей системы

- Поставьте перед собой точную цель и определите, насколько реализуемой она является.
- Создайте систему мониторинга, чтобы выявить проблемы, мешающие бесперебойной работе. Глава 22.
- Для ключевых приложений используйте методы сквозного мониторинга. Раздел 24.2.4.
- Избавляйтесь от зависимостей. Ничто в вычислительном центре не должно зависеть от каких-либо внешних элементов. Разделы 5.1.7 и 20.1.7.1.

1.33. Необходимо уменьшить расходы

- Снизьте затраты, централизовав некоторые службы. Глава 21.
- Просмотрите договоры об обслуживании. Не платите ли вы до сих пор за обслуживание машин, которые уже не являются критически важными серверами? Не платите ли вы до сих пор за обслуживание старого оборудования, которое будет дешевле заменить на новое? Раздел 4.1.4.

- Снизьте текущие расходы, например на удаленный доступ, с помощью аутсорсинга. Глава 27 и раздел 21.2.2.
- Определите, сможете ли вы уменьшить расходы с помощью стандартизации и/или автоматизации службы поддержки. Глава 3.
- Попробуйте снизить накладные расходы на поддержку, организовав курсы обучения для пользователей или усовершенствовав пользовательские инструкции.
- Попробуйте распределить расходы напрямую по соответствующим группам, например расходы на обслуживание, на удаленный доступ, на специальное оборудование, на широкополосное подключение к глобальной сети. Раздел 30.1.2.
- Узнайте, платят ли пользователи за предоставляемые вами услуги. Если за услуги не хотят платить, значит, они не так важны.
- Контролируйте процесс заказов и инвентаризацию дополнительного оборудования, такого как компьютерные мыши, мини-хабы и т. п. Не позволяйте пользователям без разрешения брать нужные им устройства или давать распоряжения вашим сотрудникам их заказывать.

1.34. Необходимо расширить функциональность

- Проводите опросы пользователей, чтобы узнать об их потребностях и расставить приоритеты функций.
- Определитесь с требованиями. Глава 5.
- Удостоверьтесь, что обеспечивается достаточная поддержка уже существующих служб и уровней доступности.
- При изменении существующей службы разработайте план отката.
- Рассмотрите возможность создания абсолютно новой системы и перехода к ней вместо изменения уже существующей.
- Если необходимо внести ряд крупных изменений в инфраструктуру, подумайте над введением технических перерывов. Глава 20.
- Проведите децентрализацию, чтобы уделить внимание и локальным функциям.
- Тестируйте, тестируйте и еще раз тестируйте!
- Документируйте, документируйте и еще раз документируйте!

1.35. Хочется избавиться от страдания при выполнении «этого кошмара»

- Не выполняйте «этот кошмар».
- Автоматизируйте процессы, выполняющие «этот кошмар».

> **Если вам от этого больно, просто не делайте этого**
>
> В небольшое периферийное отделение транснациональной компании прибыл новый системный администратор, отвечающий за техническую

поддержку в международных отделениях. Местная сотрудница, временно выполнявшая обязанности системного администратора, сказала ему по телефону, что при работе в сети «можно получить травму». Системный администратор предположил, что имелась в виду психологическая травма от слишком медленной работы сети. Однако, прибыв на место и приступив к работе, он получил мощный удар током от сети 10Base-2. Он тут же отправил всех сотрудников домой и закрыл офис, после чего вызвал электрика для выявления и решения возникшей проблемы.

1.36. Необходимо укрепить доверие пользователей

- Проследите, чтобы ваши сотрудники выполняли все порученные им задачи. Раздел 32.1.1.
- Сконцентрируйтесь на проектах, которые важны для пользователей и окажут максимальное воздействие на их работу. Рис. 33.1.
- Откажитесь от проектов, которые вы не можете выполнить, до тех пор, пока у вас не будет на это достаточно времени.
- Больше общайтесь. Глава 31.
- Приглашайте пользователей на обед. Будьте хорошим слушателем. Раздел 31.2.7.
- Старайтесь произвести положительное первое впечатление на людей, которые приходят к вам в организацию. Раздел 31.1.1.

1.37. Необходимо укрепить уверенность сотрудников в себе

- Начните с простых, легко выполнимых проектов. Только после этого стоит вовлекать сотрудников в реализацию более сложных проектов.
- Узнайте у сотрудников, в какой сфере им необходимо повысить квалификацию. Обеспечьте им соответствующее обучение.
- Обучайте своих сотрудников. Найдите инструктора, который научит вас обучать!

1.38. Необходимо заставить сотрудников лучше выполнять инструкции

- Выясните причины, по которым ваши сотрудники не выполняют переданные им инструкции.
- Удостоверьтесь, что ваша система уведомлений о неисправностях помогает сотрудникам отслеживать претензии пользователей, а не просто служит для отслеживания сиюминутных запросов. Система не должна быть слишком сложной, иначе люди будут избегать ее использования. Раздел 13.1.10.

- Создайте единую базу, в которую все сотрудники смогут вносить свои требования и предложения. Раздел 32.1.1.
- Отговорите сотрудников от попыток запомнить список всех задач. Раздел 32.1.1.
- Приобретите КПК для всех сотрудников, которым они нужны и которые обещают ими пользоваться. Раздел 32.1.1.

1.39. Поступила неэтичная или сомнительная просьба

- Прочтите раздел 12.2.2.
- Ведите журнал учета всех запросов, событий и действий.
- Все запросы должны поступать в письменном или электронном виде. Попробуйте применить спокойный подход, например сказать: «Послушайте, не могли бы вы отправить свою просьбу по электронной почте, а я просмотрю письмо после обеда?» Если податель понимает, что его требование противоречит этическим нормам, он постарается не оставлять следов.
- Узнайте, что на эту тему говорят должностные инструкции. Глава 12.
- Если в должностных инструкциях такие случаи не предусмотрены, обязательно потребуйте письменного изложения просьбы.
- Проконсультируйтесь со своим руководителем *прежде*, чем предпринимать что-либо.
- Если у вас возникли вопросы по поводу поданной просьбы, передайте ее руководству.

1.40. После мытья в посудомоечной машине на стаканах остаются пятна

- Самая распространенная причина появления пятен – недостаточно высокая температура воды. И уже на втором месте – неправильно подобранные моющие средства или программа мойки.
- Проверьте подключение горячей воды к посудомоечной машине.
- Регулируйте температуру воды.
- Перед включением посудомоечной машины откройте кран и не закрывайте, пока вода не станет горячей.

1.41. Необходимо сохранить свою должность

- Просмотрите последние отзывы и оценки вашей работы. Улучшите аспекты, которые «требуют улучшения», независимо от того, согласны вы лично с этими утверждениями или нет.
- Пройдите обучение в областях, в которых, по мнению руководства, вам не хватает квалификации.

- Будьте лучшим системным администратором в коллективе. Сделайте так, чтобы вас заметили. Глава 31.
- Документируйте все: инструкции, техническую информацию, данные конфигурации и последовательность действий.
- Выполняйте все возложенные на вас задачи.
- Помогайте другим, насколько это возможно.
- Будьте хорошим наставником.
- Эффективно используйте свое время. Раздел 32.1.2.
- Автоматизируйте все, насколько это возможно. Глава 3 и разделы 16.2, 26.1.9 и 31.1.4.3.
- Всегда учитывайте потребности пользователей. Разделы 31.1.3 и 32.2.3.
- Не говорите плохо о своих коллегах. Этим вы лишь испортите себе репутацию. Молчание – золото. Молча можно и за умного сойти.

1.42. Требуется пройти обучение

- Посещайте обучающие конференции, такие как LISA.
- Посещайте семинары поставщиков, чтобы получить специфические знания и информацию о продукции из первых рук.
- Найдите себе наставника.
- Посещайте собрания местного сообщества системных администраторов.
- Выступайте на собраниях местного сообщества системных администраторов. Обучая других, можно многому научиться.
- Найдите в сети форумы или сообщества, посвященные интересующим вас темам. Прочтите архивы, станьте активным участником этих форумов.

1.43. Необходимо расставить приоритеты

- В зависимости от того, на какой стадии вы находитесь в данный момент, следует сосредоточиться на следующих вопросах инфраструктуры.
  - Основные службы, такие как электронная почта, печать, удаленный доступ и безопасность, должны быть созданы с самого начала.
  - Автоматизация однотипных задач, таких как установка компьютеров, настройка конфигурации, обслуживание, создание и удаление учетных записей, должна быть внедрена на ранних стадиях. То же касается создания основных политик.
  - Документацию необходимо создавать по мере внедрения соответствующих элементов, иначе впоследствии у вас не будет на это времени.
  - Создайте систему хранения и развертывания программного обеспечения.
  - Проведите мониторинг до того, как решите внедрить улучшения или масштабировать. Эти важно для достаточно развитых корпоративных сетей.
  - Подумайте о внедрении службы поддержки. Раздел 13.1.1.
- Больше общайтесь с пользователями, чтобы выяснить, каковы их приоритеты.

- Внесите улучшения в систему выдачи уведомлений пользователям после регистрации ими неисправностей. Глава 13.
- Просмотрите список 10% людей, подающих заявки чаще всего. Раздел 13.2.1.
- Улучшите систему управления версиями конфигурационных файлов. Глава 17, особенно раздел 17.1.5.1.

1.44. Необходимо сделать всю работу

- Выбирайтесь из ямы. Глава 2.
- Усовершенствуйте свои навыки тайм-менеджмента. Пройдите обучающий курс по тайм-менеджменту. Разделы 32.1.2 и 32.1.2.11.
- Используйте консольный сервер, чтобы не приходилось тратить время и бегать по всему вычислительному центру. Разделы 6.1.10, 4.1.8 и 20.1.7.2.
- Обрабатывайте похожие запросы серийно. Группируйте все задачи, которые требуют от вас присутствия в той или иной части здания.
- Каждый день начинайте с работы над проектом, а не с проверки электронной почты.
- Решайте все вопросы с коллегами «на ходу», вместо того чтобы искать свободный конференц-зал и прерывать работу на пару часов.

1.45. Необходимо избежать стресса

- Возьмите наконец отпуск (трехдневные выходные отпуском не считаются)!
- Пусть ваш отпуск будет достаточно длительным, чтобы за это время точно выяснилось, какая информация недостаточно документирована. Лучше отложить решение проблем до вашего возвращения через несколько дней, чем из-за переутомления (боже упаси!) попасть под автобус.
- Совершайте прогулки. На некоторое время попробуйте сменить обстановку.
- Не обедайте за своим рабочим столом.
- Не забывайте, что в жизни есть не только работа.
- Раз в неделю или в месяц ходите к массажисту.
- Запишитесь на занятия йогой или медитацией.

1.46. Чего системные администраторы должны ожидать от своих менеджеров

- Четкой расстановки приоритетов. Раздел 33.1.1.1.
- Достаточного финансирования, позволяющего достичь намеченных целей. Раздел 33.1.1.12.
- Своевременных и конкретных отзывов. Раздел 33.1.3.2.
- Разрешения свободно выражать свое мнение в частном порядке в обмен на соблюдение правил приличия на публике. Раздел 31.1.2.

1.47. Чего менеджеры должны ожидать от системных администраторов

- Выполнения своих обязанностей. Раздел 33.1.1.5.
- Вежливого обращения с пользователями. Глава 31.
- Своевременного выполнения задач в рамках заданного бюджета.
- Способности учиться на своих ошибках.
- Желания обращаться за помощью. Раздел 32.2.2.7.
- Пессимистической оценки времени выполнениия при планировании проектов. Раздел 33.1.2.
- Честной оценки состояния этапов выполнения проектов. Раздел 33.1.1.8.
- Участия в бюджетном планировании. Раздел 33.1.1.12.
- Высоких моральных стандартов. Раздел 12.1.2.
- Системный администратор должен брать не менее одного полноценного отпуска в год. Раздел 32.2.2.8.
- Системный администратор должен быть в курсе самых инновационных технологий. Раздел 32.1.4.

1.48. Чего руководство компании должно ожидать от менеджеров системных администраторов

- Доступа к мониторингу и отчетам, чтобы руководитель мог в любое удобное время получить интересующую его информацию.
- Своевременных финансовых отчетов. Раздел 33.1.1.12.
- Пессимистической оценки времени выполнениия при планировании проектов. Раздел 33.1.2.
- Честной оценки состояния этапов выполнения проектов. Раздел 33.1.1.8.
- Разумной степени стабильности.

Глава 2

Как выбраться из ямы

Системное администрирование может быть проблемным. Многие IT-организации застревают в яме и пытаются из нее выбраться. Надеемся, что эта книга поможет вам улучшить ситуацию.

Яма

Один парень упал в такую глубокую яму, что не мог сам из нее выбраться. Вдруг он услышал, что мимо кто-то идет, и попытался привлечь внимание прохожего. Прохожий выслушал парня, пару минут подумал и спрыгнул в яму.

– Ты что наделал? Мы же теперь оба здесь застряли!

– Ага, – ответил прохожий. – Но зато теперь тебе будет не так одиноко.

В области информационных технологий очень важно уметь расставлять приоритеты проблем. Если сбои в ваших системах возникают каждый день, глупо тратить время на обсуждение, в какой цвет перекрасить стены в вычислительном центре. Однако, если ваша система работает эффективно и стабильно и при этом постоянно расширяется, вас могут попросить отремонтировать помещение вычислительного центра, чтобы его можно было показывать посетителям. В этом случае вопрос о покраске стен выходит на первое место.

В случае с сетями, с которыми нам обычно приходится работать, проблема покраски стен в центре отодвигается на самый задний план. Более того, нам очень часто приходится иметь дело с сетями, в которых существует настолько огромное количество проблем, что большинство советов в нашей книге могут показаться такими же далекими и идеалистичными, как выбор подходящего цвета стен. Образно говоря, в этих сетях столько времени тратят на вытирание воды с пола, что совершенно забывают о необходимости починить протекающую трубу.

2.1. Советы по повышению эффективности системного администрирования

Вот несколько советов, которые помогут вам разорвать порочный круг по вытиранию воды на полу.

- Используйте систему регистрации неисправностей.
- Принимайте соответствующие меры по срочным запросам.
- Используйте три инструкции для экономии времени.
- Каждый новый узел сети запускайте с известными параметрами.
- Следуйте другим нашим советам.

Если вы не будете этого делать, у вас рано или поздно возникнет масса проблем в той или иной области. Эти советы помогут вам выбраться из ямы.

2.1.1. Используйте систему регистрации неисправностей

Системным администраторам поступает слишком много запросов, чтобы они могли помнить их все. Вам необходима программа для управления потоком поступающих запросов. Можете называть эту программу *системой обработки запросов* или *системой регистрации неисправностей*, но она вам необходима. Если вы единственный системный администратор в компании, вам нужен хотя бы КПК, с помощью которого вы сможете планировать свои действия. Без такой системы вы рано или поздно забудете чью-нибудь просьбу или не выполните определенную задачу, потому что решите, что над ней работает ваш коллега. Пользователи могут серьезно расстроиться, если решат, что их просьбы игнорируют.

Как сделать, чтобы работа выполнялась до конца

Том приступил к работе над сетью, не использующей систему обработки запросов. В первый же день работы коллеги пожаловались ему, что у них с пользователями натянутые отношения. На следующий день Том обедал с некоторыми из этих пользователей. Они сообщили Тому, что высоко оценивают работу системных администраторов, *когда* те выполняют их просьбы! Однако, по их мнению, большую часть запросов системные администраторы просто-напросто игнорировали.

Следующую пару дней Том потратил на установку системы обработки запросов. Парадоксально, но при этом ему пришлось отложить выполнение просьб, которые поступили в этот период от пользователей. Впрочем, пользователи к тому времени уже привыкли к подобным задержкам. Месяц спустя Том встретился с теми же пользователями, которые на этот раз выразили большую удовлетворенность работой системных администраторов. Пользователи знали, что их просьбы услышаны. Каждому запросу присваивался номер, и пользователи получили возможность узнать, когда был выполнен их запрос. Если же запрос не был выполнен своевременно, пользователи могли показать контрольную запись руководству, чтобы были приняты необходимые меры. В результате было снижено количество необоснованных обвинений. Система обработки запросов не стала панацеей, но в значительной мере помогла избавиться от жалоб. Появилась возможность сконцентрироваться на более насущных проблемах вместо жалоб. Процедуры обработки были выведены из тупика, в котором они оказались.

> Удовлетворенность системных администраторов также повысилась. Слишком много нервов они тратили раньше на разбирательство с жалобами на игнорируемые запросы, когда не было даже доказательств существования этих самых запросов. Теперь жалобы поступали лишь по вопросам, которые системные администраторы вполне могли решить: во-первых, выполняются ли поставленные задачи, а во-вторых, были ли решены проблемы, указанные в запросах. Деятельность системных администраторов стала контролируемой. Кроме того, теперь они получили возможность информировать руководство о том, сколько запросов обрабатывается еженедельно. Вместо вопроса «Кто виноват?» (малоэффективный метод решения проблем) зазвучал вопрос «Сколько системных администраторов потребуется на решение всех проблем по запросам?». И оказалось, что именно в этом и заключается основная проблема.

В разделе 13.1.10 программы для обработки запросов описываются более подробно. Рекомендуем использовать пакет с исходным кодом Request Tracker компании Best Practical (*http://bestpractical.com/rt/*). Программа бесплатная и достаточно проста в установке.

В главе 13 вы найдете полное описание процесса управления службой поддержки. Возможно, вам стоит дать вашему начальнику прочитать эту главу. Глава 14 посвящена процессу обработки запроса. Там же вы найдете советы по сбору запросов, их сортировке и выполнению.

2.1.2. Принимайте соответствующие меры по срочным запросам

Вы когда-нибудь обращали внимание, насколько сложно выполнять работу, когда вас постоянно отвлекают? Чем чаще вас отвлекают, тем меньше шансов вообще закончить какой-нибудь долгосрочный проект. Чтобы решить эту проблему, распределите обязанности среди системных администраторов таким образом, чтобы один человек вас *прикрывал*, выполняя повседневные задачи и позволяя всем остальным спокойно работать над своими проектами.

Если вас отвлекают простыми запросами, пусть ими занимается прикрывающий. Если же запрос оказался более сложным, прикрывающий должен передать его другому сотруднику – то есть *перенаправить* его кому-либо в вашей программе службы поддержки – или, если возможно, начать работу над запросом в перерыве между простыми просьбами. В идеале прикрывающий должен справляться с 80% всех запросов, а остальные 20% распределять между сотрудниками.

Если в отделе работают всего два системных администратора, меняйтесь ролями по очереди. Один из вас может заниматься отвлекающими запросами по утрам, а второй – после обеда. Если же у вас большой коллектив системных администраторов и ежедневно приходится обрабатывать десятки или сотни запросов, проведите реорганизацию, чтобы одни сотрудники занимались запросами, а другие – долгосрочными проектами.

Во многих компаниях до сих пор бытует мнение, что все системные администраторы должны обладать одинаковой квалификацией во всем. Это мнение может

быть оправданно, если компания небольшая. Но по мере того как она развивается, на первый план выходит специализация.

Пользователи, как правило, имеют представление о том, сколько времени должна занимать та или операция. Если ваша работа соответствует этому представлению, ваши пользователи будут намного довольнее вами. Более подробно эта тема освещена в разделе 31.1.3. Например, пользователи считают, что смена паролей должна производиться быстро, так как невозможность зайти в систему под своим именем прерывает общий процесс работы. А вот установка нового настольного компьютера, по мнению тех же пользователей, может занять пару дней, так как компьютер необходимо принять, распаковать, подключить и настроить. Если вы сможете быстро решать проблемы с паролями, пользователи будут вами довольны. А если при этом установка нового компьютера займет чуть больше времени, никто этого даже не заметит.

Порядок действия для вас неважен. Если вы сначала решите проблему с паролями, а затем займетесь настройкой новых компьютеров, вы потратите столько же времени, как и на те же действия в обратном порядке. Однако этот порядок действий важен для других. Если кто-то вынужден прождать целый день, пока вы выдадите ему пароль, только потому, что вы сначала настраивали новые компьютеры, этот человек может серьезно разозлиться. Ведь вы на целый день отсрочили для него выполнение его работы.

В течение недели вам придется выполнять тот же объем работы, но если вы правильно распланируете порядок выполнения задач, пользователи будут очень довольны тем, как вы реагируете на возникающие проблемы. Все очень просто. Достаточно совместить свои приоритеты с ожиданиями пользователей.

Этот прием можно использовать при планировании своего рабочего времени даже в том случае, если вы – единственный системный администратор в компании. Сообщите своим пользователям, что по текущим вопросам вас лучше отвлекать в первой половине дня, так как после обеда вы занимаетесь долгосрочными проектами. Разумеется, вы должны заверить пользователей, что срочные проблемы вы будете решать незамедлительно. Можете сказать им следующее: «Наивысший приоритет я отдаю аварийным ситуациям. Однако остальные проблемы я буду стараться решать в первой половине дня, чтобы после обеда заниматься своими проектами. В первой половине дня вы можете подходить ко мне и излагать свою просьбу. А после обеда, если у вас не срочный случай, пожалуйста, присылайте мне запрос по электронной почте. Я займусь им в специально отведенное время. Если же вы обратитесь ко мне с несрочной просьбой во второй половине дня, я запишу ее и приму все необходимые меры позже».

Глава 30 посвящена созданию общей структуры в вашей организации. В главе 32 вы найдете немало советов по тайм-менеджменту для системных администраторов.

Убедить вашего руководителя вложить деньги в такую систему может быть нелегко. Однако вы можете внедрить ее неофициально, в уме следуя указанному плану и не слишком это афишируя.

2.1.3. Используйте три инструкции для экономии времени

Ваше руководство может утвердить три служебные инструкции по приведенным ниже вопросам, что поможет вам побыстрее убрать воду с пола.

1. Каким образом люди должны получать помощь.
2. Каковы границы ответственности системных администраторов.
3. Что можно считать «*аварийной ситуацией*».

Достаточно часто нам приходится наблюдать, как люди понапрасну тратят время из-за разрыва связей между этими тремя пунктами. Руководство должно обдумать эти инструкции перед утверждением и внедрить их по всей организации. Руководство должно взять на себя ответственность за утверждение и внедрение этих инструкций, а также за негативную реакцию пользователей, которая может возникнуть впоследствии. Люди не любят, когда их заставляют менять устоявшийся образ жизни, но без изменений не будет и улучшений.

Первая инструкция посвящена тому, каким образом люди должны получать помощь. Если вы уже установили систему обработки запросов, эта инструкция не только сообщит сотрудникам о ее существовании, но и объяснит, как ее использовать. Важный аспект этой инструкции – указать, что людям придется изменить свои привычки и прекратить толпиться у вашего стола, отвлекая вас от работы (если же это до сих пор разрешается, пусть они перейдут к столу прикрывающего). В разделе 13.1.6 вы найдете больше советов по написанию этой инструкции.

Вторая инструкция определяет границы ответственности системных администраторов. Этот документ предназначен как для системных администраторов, так и для пользователей. Системным администраторам, которые только что устроились на работу, как правило, бывает трудно сказать «нет». В результате они оказываются перегруженными работой, выполняя чужие обязанности. Вместо того чтобы подсказать пользователю, что делать, они говорят: «Давай я это сам сделаю», а просьба дать полезный совет может окончиться тем, что системный администратор станет тратить время на обслуживание программ и оборудования, не требуемых для работы в компании. Старшие системные администраторы вырабатывают привычку слишком часто говорить грубое «нет», даже в ущерб интересам компании. В разделе 13.1.5 вы найдете советы по составлению этой инструкции.

Третья инструкция дает точное определение аварийной ситуации. Если системный администратор не может отказать пользователям, так как они считают, что каждый их запрос является срочным, эта инструкция позволит системным администраторам заняться ремонтом протекающей трубы, вместо того чтобы

Определение аварийной ситуации в Google

В Google разработали сложное определение *аварийной ситуации*. Для *событий первостепенной важности* (красный код) составлены конкретные описания, относящиеся к качеству обслуживания, доходам и другим приоритетам корпорации. К *событиям второй степени важности* (желтый код) относятся проблемы, которые напрямую могут привести к проблемам красного кода, если их не исправить. Как только руководство объявляет аварийную ситуацию, сотрудники, занимающиеся решением возникшей проблемы, получают определенные ресурсы и приоритетную помощь других сотрудников. В службе поддержки предусмотрены соглашения об уровне службы для запросов от людей, которые работают над проблемами красного и желтого кода.

все дни напролет вытирать воду с пола. В одних организациях составить эту инструкцию проще, чем в других. В редакции газеты аварийной ситуацией считается все, что может помешать своевременной печати и выходу следующего выпуска. Такие помехи могут быть вполне очевидными. В торговой организации аварийной ситуацией может быть событие, напрямую препятствующее проведению презентации или составлению квартального отчета о продажах. В этом случае точно определить, какие события считать критичными, может быть гораздо сложнее. В исследовательском институте аварийной ситуацией может быть любое событие, препятствующее своевременной подаче запроса на грант. Более подробно эта инструкция описана в разделе 13.1.9.

Эти три инструкции обеспечивают перегруженным работой системным администраторам передышку, необходимую для изменения ситуации.

2.1.4. Каждый новый узел сети запускайте с известными параметрами

И наконец, просто удивительно, сколько компаний не имеют единого метода загрузки операционной системы (ОС) на узлы развертываемой сети. Для всех современных операционных систем предусмотрен способ автоматической установки. Как правило, система загружается с сервера. Сервер загружает небольшую программу, которая подготавливает диск, загружает операционную систему и приложения, а затем выполняет все локальные сценарии установки. Так как последний этап мы способны контролировать, можно добавить приложения, изменить настройки и т. д. После этого систему нужно перезагрузить – и она будет готова к использованию[1].

Подобная автоматизация имеет два преимущества: экономию времени и воспроизводимость. Время экономится благодаря тому, что все процессы, выполняемые ранее вручную, автоматизируются. Можно запустить процесс и заниматься другой работой, пока производится автоматическая установка. Воспроизводимость означает, что вы можете в точности повторить ту же последовательность действий при установке на других машинах. Правильная последовательность означает, что впоследствии понадобится гораздо меньше тестировать (вы ведь тестируете рабочую станцию, прежде чем предоставить ее кому-либо, правда?). Воспроизводимость экономит время в службе поддержки; пользователи могут рассчитывать на лучшее обслуживание, если сотрудники службы поддержки знают уровень единообразия обслуживаемой ими системы. Кроме того, воспроизводимость означает, что все пользователи обслуживаются на одном уровне. Никому не придется удивляться, что на его компьютере отсутствуют программы или возможности, установленные на компьютерах коллег.

Не исключено, что вы обнаружите и дополнительные преимущества. Так как сам процесс теперь намного упрощен, системные администраторы гораздо охотнее будут обновлять старые машины, которые подверглись энтропии и которым не помешает переустановка. Если приложения с самого начала настроены правильно, это означает, что при первом запуске программ в службу поддержки поступит меньше просьб о помощи. Эффективность системы безопасности повышается благодаря периодической установке патчей и включению функций

[1] Более дешевый вариант – составить список с подробными инструкциями, включая настройки, которые необходимо изменить в различных приложениях и т. д. Кроме того, можно использовать систему клонирования дисков.

безопасности. Теперь сотрудникам, не являющимся системными администраторами, не придется самостоятельно загружать операционную систему, что снижает количество случайных настроек.

После того как установка ОС будет автоматизирована, необходимо перейти к следующему крупному этапу – автоматизации установки патчей и обновлений. Автоматизация установки патчей и обновлений означает, что системным администраторам не придется так много бегать от компьютера к компьютеру для обеспечения единообразия. Безопасность повышается, так как процесс установки патчей ускоряется и упрощается. Единообразие повышается, так как снижается шанс, что при настройке будет пропущена одна из машин.

В примере, рассмотренном в разделе 11.1.3.2, отображены многие из этих вопросов применительно к системе безопасности в крупной организации, занимающейся электронной коммерцией, в сеть которой было совершено незаконное проникновение. После установки новых машин проникновение в них совершалось быстрее, чем консультанты успевали устанавливать патчи и исправлять ошибки. Консультанты поняли, что основная проблема их сети заключается в отсутствии автоматизированного и согласованного способа загрузки машин. Вместо того чтобы решать проблемы безопасности, консультанты установили систему автоматической установки ОС и патчей, и это вскоре решило проблемы в области безопасности.

Почему системные администраторы, работающие в этой компании, с самого начала не создали такую инфраструктуру? В учебниках описано, как автоматизировать установку ОС, но понять, насколько это важно, можно только из собственного опыта. У системных администраторов в этой компании не было инструкторов, которые могли бы их этому научить. Естественно, были и другие оправдания: не хватает времени; слишком сложно; оно того не стоит; сделаем в следующий раз. Однако компания не потратила бы лишние деньги, не получила бы негативные отзывы в прессе и ее акции не упали бы в цене, если бы системные администраторы с самого начала все делали как следует.

Помимо снижения уровня безопасности, несогласованная настройка ОС усложняет работу службы поддержки, так как в каждой машине присутствуют различия, которые становятся ловушками на пути системного администратора и мешают ему выполнять свою работу. Пользователи приходят в замешательство, если видят, что на различных компьютерах все настроено по-разному. Из-за несогласованности настроенные программы не найдут файлы, которые должны быть в определенных каталогах.

Если в вашей сети нет системы автоматизации настройки новых машин, немедленно создайте такую систему. Более подробную информацию по этой теме вы найдете в главе 3.

2.1.5. Другие советы

2.1.5.1. Электронная почта должна работать стабильно

Люди, которые определяют размер вашей зарплаты, занимают достаточно высокие руководящие посты, чтобы позволить себе пользоваться только электронной почтой и календарем, если они у них есть. Удостоверьтесь, что эти приложения работают должным образом. Если работа этих приложений станет надежной и стабильной, доверие руководства к вашим сотрудникам повысится.

Вам будет проще убедить их пойти на дополнительные затраты, если это необходимо. Наличие стабильной системы электронной почты даст вам отличное прикрытие в других ваших битвах. Сделайте так, чтобы улучшения заметили и сотрудники канцелярии руководства. Часто бывает так, что именно эти люди по-настоящему руководят компанией.

2.1.5.2. Документируйте в процессе

Не стоит превращать документирование в тяжелую обязанность. Создайте собственную Википедию или просто каталог с текстовыми файлами на сервере. Составьте списки основных задач для таких ситуаций, как инструктаж нового работника или настройка клиента электронной почты. После того как вы опишете эти задачи, вы сможете поручать их выполнение младшему персоналу или новому сотруднику.

Также могут быть полезны списки критических серверов для каждого приложения или службы. Не забывайте о ярлыках на оборудовании, так как они помогают предотвратить ошибки и позволяют новичкам оказывать помощь другим. Даже если у вас мало времени, обязательно позаботьтесь о том, чтобы наклеить ярлык на немаркированное устройство до того, как вы начнете с ним работать. Наклеивайте ярлыки на переднюю и заднюю части машин. Одинаковые ярлыки наклейте на блок питания и подключаемое к нему устройство (глава 9).

2.1.5.3. Устраните самую крупную утечку времени

Выберите одну проблему, на которую у вас уходит больше всего времени, и выделите одного человека на ее решение. Возможно, остальным сотрудникам отдела придется работать в более жестком режиме, пока проблема решается, но дело того стоит. Человек, занятый в решении этой проблемы, должен периодически отчитываться и при необходимости обращаться за помощью, если возникнет слишком много технических или политических зависимостей.

Удачное устранение самой крупной утечки времени

Когда Том работал в Cibernet, он обнаружил, что команда системных администраторов лондонского филиала не может справиться с критически важными, высокоприоритетными проектами, так как они завалены заявками на обслуживание индивидуальных компьютеров. У Тома не было возможности нанять старшего системного администратора для работы над высокоприоритетными проектами, так как время на его подготовку превысило бы сроки выполнения проекта. Вместо этого он подумал о технике для простейшего обслуживания компьютеров с ОС Windows – такого работника нетрудно найти, ему не надо много платить и для него не потребуется долгая подготовка. Руководство не разрешило ему нанять такого сотрудника, но он получил согласие привлечь кого-нибудь по временному контракту на полгода (логично, за полгода вполне можно отладить компьютеры настолько, что такой работник больше не понадобится). В обязанности нового сотрудника входили типичные компьютерные проблемы: защита от вирусов, подготовка к эксплуатации новых компьютеров, смена паролей и т. д. А остальные системные администра-

торы освободились для работы над высокоприоритетными, ключевыми для компании проектами.

К концу шестимесячного контракта руководство увидело улучшение производительности труда системных администраторов. Традиционные простои исчезли, потому что у старших системных администраторов появилось время на то, чтобы выбраться из ямы, а временный сотрудник устранил множество мелких проблем на компьютерах с ОС Windows. В результате контракт с ним был продлен, и в конце концов он стал постоянным сотрудником, когда руководство оценило преимущества специализации.

2.1.5.4. Выберите то, что можно легко исправить

Остальная часть этой книги посвящена поиску долгосрочных, постоянных решений. Тем не менее, когда нужно выбраться из ямы, стратегически оправданным будет правильно выбрать некоторые быстро решаемые проблемы, чтобы завершить несколько важных, высокоприоритетных проектов. Сохраните список долгосрочных решений, которые могут быть отложены. Когда вы достигнете стабильности, используйте этот список при планировании следующей серии проектов. К тому времени у вас, возможно, появятся новые сотрудники с более хорошими идеями о том, как продолжить (подробнее об этом в разделе 33.1.1.4).

2.1.5.5. Обеспечьте достаточное энергоснабжение и охлаждение

Удостоверьтесь, что в каждом компьютерном зале достаточное энергоснабжение и охлаждение. Каждое устройство должно быть подключено к источнику бесперебойного питания (UPS). Тем не менее, когда вы только выбираетесь из ямы, достаточно того, чтобы к UPS были подключены лишь наиболее важные серверы и сетевые устройства. Индивидуальные UPS – по одному на стойку – будут отличным временным решением. Емкость батарей UPS должна быть достаточной для того, чтобы серверы могли работать в течение часа и безопасно отключиться, прежде чем истощится заряд батарей. Перебои длительностью больше часа случаются крайне редко. Большинство отключений исчисляется секундами. Небольшие UPS являются хорошим решением, пока не будут установлены UPS большей емкости, способные обслуживать весь вычислительный центр. Приобретая небольшие UPS, не забудьте уточнить у поставщика, какие разъемы требуются для подключения данной конкретной модели. Вы будете удивлены тем, как много существует особых требований.

Охлаждение даже более важно, чем энергоснабжение. Каждый ватт мощности, потребляемый компьютером, выделяет определенное количество тепла. В соответствии с законами термодинамики, вам придется затратить более 1 ватта электроэнергии для отвода тепла, выделяемого 1 ваттом потребляемой компьютером мощности. Таким образом, как правило, более 50% энергии будет затрачено на охлаждение.

У организаций, пытающихся выбраться из ямы, зачастую имеются небольшие вычислительные центры, но размещенные в тесных помещениях, иногда даже

без охлаждения. Эти организации пытаются обойтись тем, что просто включают систему охлаждения в здании. Это подходит для одного сервера, максимум двух. Если установлено больше серверов, в помещении будет жарко, но системы охлаждения здания будет достаточно. Однако все забывают, что система охлаждения здания отключается на выходные и в воскресенье в помещении очень жарко. А ведь бывают и долгие выходные, и ваш отдых может быть испорчен, если к понедельнику все ваши серверы перегреются. В США неофициально началом лета считаются трехдневные выходные в конце мая, приуроченные ко Дню памяти павших в гражданской войне. Так как это длительные выходные и к тому же первые жаркие выходные в году, зачастую именно тогда люди понимают, что их система охлаждения недостаточно эффективна. Если в эти выходные происходит сбой, то и все лето будут проблемы. Будьте предусмотрительны – проверяйте все системы охлаждения в апреле.

Примерно за 400 долларов или меньше можно установить портативную систему охлаждения, которая будет отводить тепло из тесного компьютерного помещения за потолочные перекрытия или за окно. Это неплохое временное решение, достаточно недорогое, чтобы не требовалось его утверждение у руководства. Для больших площадей быстрым решением станет охлаждающая система на 19,5 или 37,5 кВт.

2.1.5.6. Проводите простой мониторинг

Хотя мы и предпочитаем всеобъемлющие системы мониторинга с массой дополнительных функций, но многого можно достичь и с помощью простых систем, пингующих ключевые серверы и оповещающих людей о проблемах по электронной почте. У некоторых пользователей складывается впечатление, что серверы чаще всего ломаются по понедельникам с утра. На самом деле без мониторинга сбои накапливаются за выходные и обнаруживаются в понедельник утром. С простой системой мониторинга случившийся в выходные сбой может быть исправлен до прихода людей в понедельник (если никто не слышал, как упало дерево в лесу, не имеет значения, шумно ли оно падало). Это не значит, что системы мониторинга надо использовать для того, чтобы скрывать перебои, которые случаются по выходным. Всегда отправляйте отчеты об устранении неисправностей по электронной почте. Это хорошая реклама.

2.2. Заключение

Остальная часть этой книги посвящена более высоким и идеалистичным целям организации труда системных администраторов. В этой главе рассмотрено несколько высокоэффективных изменений, которые можно применить к сетям, утонувшим в проблемах.

Во-первых, мы выяснили, как разобраться с запросами пользователей. Пользователи – это те люди, которых мы обслуживаем; часто их называют юзерами. Использование системы уведомлений о неисправностях для работы с заявками позволяет системным администраторам тратить меньше времени на обработку заявок и дает пользователям возможность отслеживать состояние выполнения своих заявок. Система регистрации неисправностей помогает системным администраторам доводить до конца работы по запросам пользователей.

Чтобы правильно обрабатывать запросы, создайте систему, где запросы, которые блокируют выполнение других задач, будут обслуживаться в первую очередь.

Взаимное прикрытие от перерывов позволяет системным администраторам переадресовывать неотложные заявки, пока они работают над проектами. Такая организационная структура позволяет системным администраторам переадресовывать заявки в соответствии с ожиданиями пользователей.

Зачастую многие проблемы, с которыми мы сталкиваемся, возникают из-за разногласий или различных ожиданий насчет того, как и когда обращаться за помощью. Чтобы устранить эти несоответствия, важно уменьшить путаницу, введя три инструкции, в которых описано, как получить компьютерную помощь, определены рамки ответственности системных администраторов и чрезвычайные ситуации в сфере информационных технологий.

Важно запускать каждый новый узел сети с известными параметрами. Это упрощает развертывание компьютерной сети, поддержку пользователей и делает обслуживание пользователей более упорядоченным.

Другие советы тоже важны. Электронная почта должна работать стабильно – от этой критически важной службы в значительной степени зависит ваша репутация. Документируйте в процессе – чем больше вы документируете, тем меньше придется открывать заново. Устраните самую крупную утечку времени – у вас появится больше времени на другие задачи. При нехватке персонала стоит сконцентрироваться на решении краткосрочных проблем. Достаточные энергоснабжение и охлаждение помогут избежать долгих простоев.

Теперь, когда мы решили неотложные задачи, можно сосредоточиться на более серьезных концепциях – на основных элементах.

Задания

1. Какую систему обработки запросов вы используете? Каковы ее преимущества и недостатки?
2. Каким образом вы контролируете выполнение всех заявок системными администраторами?
3. Как расставляются приоритеты заявок? Как расставляются приоритеты невыполненных заявок за день? Как расставляются приоритеты проектов, рассчитанных на квартал или на год?
4. В разделе 2.1.3 описаны три инструкции, позволяющие сэкономить время. Существуют ли эти служебные инструкции в вашей организации? Если нет, как бы вы охарактеризовали практикуемую политику в этом направлении?
5. Если хоть одна из трех инструкций, описанных в разделе 2.1.3, отсутствует в вашей организации, обсудите этот вопрос со своим руководителем и объясните ему все преимущества и возможности такой инструкции.
6. Если все три инструкции, описанные в разделе 2.1.3, существуют, попросите одного из коллег найти их, не давая ни одной подсказки. Смог ли ваш коллега выполнить просьбу? Каким образом можно облегчить поиск этих инструкций?
7. Перечислите в порядке популярности все операционные системы, используемые в вашей корпоративной сети. Какая система автоматизации используется для загрузки каждой из них? Или автоматизация загрузки каких операционных систем принесет вам максимальные преимущества?

8. Каким образом организована автоматизация установки патчей и обновлений для самых распространенных операционных систем в вашей сети? Какие основные преимущества вы получите от внедрения такой автоматизации в своей сети? Какую программу или систему вы хотите использовать для автоматизации?
9. Насколько стабильно работает электронная почта директора вашей компании?
10. Охарактеризуйте самую крупную утечку времени в вашей работе. Назовите два способа решения этой проблемы.
11. Проведите простую проверку всех компьютерных и сетевых помещений. Определите, в которых из них недостаточное охлаждение или неудовлетворительная защита по электропитанию.
12. Нарисуйте схему всех компьютерных и сетевых помещений. Укажите в ней системы охлаждения, тип защиты по электропитанию (если таковая имеется) и объем потребляемой электроэнергии. Составьте рейтинг всех помещений. Сделайте все возможное, чтобы исправить проблемы с охлаждением воздуха до первого дня лета.
13. Если вы не используете систему мониторинга, установите пакет с открытым исходным кодом, такой как Nagios, который будет просто сообщать вам о сбоях ваших трех главных серверов.

Часть II

Основные элементы

Глава 3

Рабочие станции

При правильном обслуживании рабочих станций (как настольных компьютеров, так и ноутбуков) у новых сотрудников с первого дня на работе будет все необходимое, включая основную инфраструктуру, в том числе электронную почту. Остальные сотрудники даже не заметят появления новой рабочей станции (сотрудника). Развертывание новых приложений не будет прерывать рабочий процесс. Исправление всех ошибок будет производиться своевременно. Все будет «просто работать».

Обслуживание операционных систем на рабочих станциях сводится к выполнению трех основных задач: первоначальная установка системного программного обеспечения и приложений, обновление системного программного обеспечения и приложений, настройка сетевых параметров. Мы называем эти задачи «большой тройкой».

Если вам не удастся должным образом решить эти три задачи, если они не будут выполняться единообразно на всех системах или если вы будете вообще их игнорировать, остальная ваша работа значительно осложнится. Если вы не будете *всякий раз* загружать операционную систему на узлах сети, обязанности по их поддержке превратятся в сущий кошмар. Если у вас нет *простого* способа установки обновлений и патчей, у вас не будет и желания это делать. Если сетевые настройки не администрируются централизованно, например через DHCP-сервер, внесение даже минимальных изменений в параметры сети может принести вам немало проблем. Автоматизация этих задач значительно изменит ситуацию к лучшему.

Рабочая станция в нашем понимании – компьютерное оборудование, выделенное для работы одного пользователя. Как правило, имеется в виду настольный компьютер или ноутбук пользователя. В современной сети у нас также есть среди прочего компьютеры с удаленным доступом, виртуальные машины и ноутбуки с док-станциями.

Рабочие станции, как правило, используются в больших количествах и отличаются долгим жизненным циклом (рождение, использование, смерть). В результате, если вам необходимо внести изменения во все рабочие станции, сделать это правильно будет сложно и критически важно. Если что-то пойдет не так, вам, возможно, придется задерживаться на работе по вечерам, из последних сил пытаясь разгрести гору проблем, а по утрам вас будет встречать ворчание пользователей.

Проанализируйте жизненный цикл компьютера и его операционную систему. Реми Эвард (Remy Evard) подробно описал этот процесс в своей работе «*An Analysis of UNIX System Configuration*». И хотя его работа посвящена машинам под управлением UNIX, эту информацию можно экстраполировать на другие операционные системы. Созданная Эвардом модель представлена на рис. 3.1.

Рис. 3.1. *Модель жизненного цикла машины и ее ОС, разработанная Эвардом*

На схеме отображено пять состояний: новое, чистое, сконфигурированное, неизвестное и отключенное.

- **Новое** состояние относится к совершенно новой машине.
- **Чистое** состояние относится к машине с установленной, но еще не настроенной ОС.
- **Сконфигурированное** состояние означает, что система настроена и функционирует должным образом.
- **Неизвестное** состояние относится к компьютеру, который был неправильно сконфигурирован или конфигурация которого устарела.
- **Отключенное** состояние относится к машине, которая была списана и отключена.

Существует множество способов перевести машину из одного состояния жизненного цикла в другое. В большинстве сетей процессы *сборки* и *инициализации* машин, как правило, проводятся в один этап. В результате операционная система загружается и приводится в состояние, пригодное для использования. *Энтропия* – процесс нежелательной амортизации, приводящий компьютер в неизвестное состояние, которое можно исправить с помощью *отладки*. Со временем проводятся обновления, как правило в виде патчей и пакетов обновления системы безопасности. Иногда может потребоваться удалить и переустановить систему на машине, так как наступила пора для глобального обновления ОС, необходимо восстановить систему для новых целей или это вынуждает сделать серьезная степень энтропии. Проводится процесс *восстановления*, данные на машине стираются, и система заново устанавливается, возвращая машину к сконфигурированному состоянию.

Эти различные процессы повторяются в течение месяцев и лет. И наконец машина устаревает и списывается. Она умирает трагической смертью, или, как отражено в модели, переводится в отключенное состояние.

Какую информацию мы можем получить из этой схемы? Во-первых, необходимо признать, что существуют различные состояния и переходы. Мы планируем время установки, признаем тот факт, что будут возникать сбои и их необходимо будет исправлять, и т. д. Не стоит удивляться каждому сбою. Необходимо раз-

работать план исправления или создать целый ремонтный отдел, если того требуют обстоятельства. Для всего этого потребуется планирование, кадры и другие ресурсы.

Во-вторых, видно, что, несмотря на существование нескольких видов состояний, компьютер можно использовать только в сконфигурированном состоянии. Необходимо до максимума увеличить время, проводимое в этом состоянии. Большинство других процессов относятся к приведению или возвращению компьютера в сконфигурированное состояние. Таким образом, эти процессы установки и восстановления должны проводиться быстро, эффективно и, будем надеяться, автоматически.

Чтобы продлить время пребывания компьютера в сконфигурированном состоянии, необходимо сделать так, чтобы деградация ОС протекала как можно медленнее. Главным фактором здесь являются архитектурные решения поставщика ОС. Некоторые операционные системы требуют установки новых приложений посредством загрузки файлов в различные системные каталоги. При этом достаточно сложно определить, какие файлы к каким пакетам принадлежат. Другие операционные системы позволяют загружать дополнения практически в любые каталоги. ОС Microsoft Windows известна своими проблемами в этой области. С другой стороны, UNIX предоставляет разграничение доступа к каталогам, благодаря чему приложения, установленные пользователем, не могут разрушить целостность ОС.

Архитектурное решение, принятое системным администратором, может усилить или ослабить целостность операционной системы. Существует ли строго определенное место для установки сторонних приложений за пределами системной области (глава 28)? Предоставлялись ли пользователю права `root` или Администратора, что могло усилить энтропию? Разработал ли системный администратор способ для пользователей выполнять задачи администрирования, не обладая при этом верховной властью `root`[1]? Системные администраторы должны найти необходимый баланс между предоставлением пользователям полного доступа и ограничением их прав. Этот баланс влияет на скорость разрушения операционной системы.

Установка вручную всегда предполагает возможность ошибок. Если ошибки возникают в процессе установки, узел сети начнет свой жизненный цикл с тенденцией к разрушению. Если процесс установки полностью автоматизирован, новые рабочие станции будут развернуты должным образом.

Переустановка (процесс восстановления) подобна установке с той разницей, что в первом случае, возможно, понадобится перенести старые данные и приложения (глава 18). Решения, принимаемые системным администратором на ранних стадиях, определяют, насколько простым или сложным будет этот процесс. Переустановка будет проще, если на машине не хранится никаких данных. В случае рабочих станций это означает, что как можно больше данных должно храниться на файловом сервере. Это позволит предотвратить случайное удаление данных при переустановке. В случае серверов это означает, что данные необходимо переместить на удаленную файловую систему (глава 25).

---

[1] «Человеку свойственно ошибаться, но, чтобы по-настоящему напортачить, необходим пароль `root`». Аноним.

И наконец, эта модель показывает, что машины в конце концов списываются. И этому не стоит удивляться: машины не могут работать вечно. Со списанием машины связаны различные задачи. Как и в случае переустановки, некоторые данные и приложения необходимо перенести на машину, которая заменит старую, или сохранить на внешнем носителе информации для последующего использования. В противном случае они безвозвратно канут в лету.

Руководство зачастую ничего не знает об управлении жизненным циклом компьютеров. Руководители должны узнать о финансовом планировании: списание активов в связи с износом необходимо совместить с ожидаемым сроком службы актива. Предположим, в вашей компании списание основных средств производится каждые пять лет. Ожидаемый срок службы компьютеров – три года. Таким образом, вы не сможете в течение двух лет избавиться от списанных компьютеров, что может стать довольно серьезной проблемой. В современных компаниях списание компьютерного оборудования производится каждые три года. Когда руководство поймет жизненный цикл компьютера или его упрощенную модель, которая лишена ненужных технических подробностей, системным администраторам будет проще получить финансирование для выделенной группы развертывания, отдела ремонта и т. д.

В этой главе термин **платформа** используется для обозначения определенной комбинации поставщика оборудования и ОС. Вот некоторые примеры: персональный компьютер с процессором AMD Athlon под управлением Windows Vista, Mac с процессором PPC под управлением OS X 10.4, настольный компьютер с процессором Intel Xeon под управлением Ubuntu 6.10 Linux, Sun Sparc Ultra 40 под управлением Solaris 10 или Sun Enterprise 10000 под управлением Solaris 9. В некоторых компаниях компьютеры от разных поставщиков под управлением одной и той же операционной системы могут считать разными платформами. Например, настольный компьютер и ноутбук под управлением Windows XP считаются разными платформами. Обычно разные версии одной и той же операционной системы считаются разными платформами, если их требования поддержки значительно различаются[1].

3.1. Основы

С обслуживанием операционных систем рабочей станции связаны три критически важных аспекта:

1. Первоначальная установка системного ПО и приложений.
2. Обновление системного ПО и приложений.
3. Настройка сетевых параметров.

Если вы хотите, чтобы управление вашей сетью производилось с минимальными затратами, эти три задачи необходимо автоматизировать для любой платформы, которая используется в вашей сети. Грамотное решение этой проблемы облегчит выполнение многих других задач.

Если же в вашей сети есть лишь несколько узлов, являющихся различными платформами, создание полной автоматизации может и не требоваться. Вло-

[1] Таким образом, компьютер с процессором Intel Xeon под управлением SUSE 10, сконфигурированный в качестве веб-сервера, и такой же компьютер, сконфигурированный в качестве рабочей станции САПР, считаются разными платформами.

следствии, когда сеть станет расширяться, вы можете увидеть необходимость создания полной автоматизации. Очень важно (будь то с помощью интуиции, бизнес-плана по расширению компании или мониторинга потребностей пользователей) не пропустить этот этап.

Привилегированные объекты

Когда Том работал в Bell Labs, его группе было поручено обеспечить поддержку практически всех типов компьютеров и операционных систем, которые только можно себе представить. Так как выполнить подобную просьбу физически невозможно, было принято решение, что некоторые платформы получат лучшую поддержку по сравнению с другими платформами в зависимости от корпоративных потребностей. «Привилегированные объекты» – платформы, которые должны были получать полноценную поддержку. Системные администраторы прошли обучение по обслуживанию оборудования и программного обеспечения этих систем, пользователям предоставили документацию по этим системам, и все три важнейшие задачи (установка, обновление и конфигурирование сети) были автоматизированы, что позволило проводить обслуживание этих узлов сети при минимальных затратах. Не менее важен тот факт, что автоматизация этих узлов сети снизила нагрузку системных администраторов, что, в свою очередь, устранило необходимость расширять их штат (раздел 35.1.11).

Все остальные платформы получали меньшее обслуживание, которое, как правило, заключалось в предоставлении IP-адреса, соблюдении требований безопасности и необходимой поддержке. Пользователи работали сами по себе. Системный администратор не мог тратить больше часа на любую проблему, связанную с этими системами. Системные администраторы поняли, что лучше просто мягко напоминать пользователям об этом ограничении времени до того, как приступать к работе, чем удивлять пользователя после того, как лимит времени исчерпан.

Платформа могла получить статус «привилегированного объекта» по целому ряду причин. Запросы пользователей могли продемонстрировать, что определенные проекты требуют именно конкретной платформы. Иногда системные администраторы могли проявить инициативу, если замечали тенденцию раньше пользователей. Например, системные администраторы старались не поддерживать одновременно больше двух версий Windows и внедрять последние версии параллельно с избавлением от самых старых версий.

Порой было дешевле обеспечить поддержку платформы, чем разбираться с проблемами, вызванными неумелой установкой, самостоятельно выполненной пользователями. Одна платформа, установленная некомпетентными техниками, которые включили все доступные возможности, рискуя обрушить всю сеть, была случайно зарегистрирована в сети как мост 802.3 STP («В тот момент это казалось хорошей идеей!»). После многочисленных сбоев, вызванных включением этой функции, платформу решили поддержать, чтобы отстранить пользователей от процесса установки и предотвратить подобные перебои в работе. Кроме того, иногда дешевле обеспечить поддержку ОС, чем работать в небезопасной ис-

ходной конфигурации и разбираться с вызванными этим проблемами безопасности. Университеты и организации, работающие без брандмауэров, часто оказываются в таких ситуациях.

Создание автоматизации зачастую требует значительных вложений ресурсов и, соответственно, нуждается в утверждении руководством. Со временем руководство Bell Labs осознало важность этих вложений при привилегированной поддержке новой платформы. Руководители поняли, что эти вложения окупаются за счет качественного обслуживания.

Не всегда просто автоматизировать некоторые процессы. В некоторых случаях Bell Labs приходилось создавать все с самого начала (Fulmer and Levine 1998) или возводить громоздкие программные надстройки поверх программного решения от поставщика, чтобы сделать его управляемым (Heiss 1999). Иногда кому-то приходилось жертвовать другими проектами или временем реакции на другие заявки, чтобы выделить время на построение подобных систем. Но в конечном итоге дело того стоило.

Когда поставщики пытаются продать нам новую продукцию, мы всегда интересуемся, можно ли автоматизировать ее работу и как это сделать. Мы отклоняем предложения поставщиков, не понимающих проблем внедрения. Все больше поставщиков понимают, что невозможность быстрого развертывания их продукции снижает вероятность ее приобретения пользователями.

3.1.1. Установка ОС

Каждый поставщик ОС дает свое название системе автоматической установки ОС: JumpStart в Solaris, KickStart в RedHat Linux, RoboInst в SGI IRIX, Ignite-UX в HP-UX, служба удаленной установки (Remote Installation Service) в Microsoft Windows. Автоматизация решает огромное количество проблем, но не все из них являются техническими. Во-первых, автоматизация экономит деньги. Разумеется, одним из основных преимуществ является время, выигранное за счет замены ручных процессов автоматическими. Кроме того, автоматизация устраняет два вида скрытых затрат. Первый относится к *ошибкам*: при ручном выполнении процессов существует вероятность ошибок. Для любой рабочей станции существуют тысячи потенциальных комбинаций настроек (иногда даже в одном приложении). Небольшая ошибка в конфигурации может вызвать серьезный сбой. Иногда решить эту проблему достаточно просто. Если кто-то открывает проблемное приложение сразу после введения в эксплуатацию рабочей станции и немедленно сообщает об ошибке, системный администратор тут же придет к выводу, что проблема заключается в конфигурации машины. Однако подобные проблемы достаточно часто могут скрываться месяцами или даже годами, пока пользователь не откроет определенное приложение. В этот момент системному администратору может не прийти в голову спросить пользователя, в первый ли раз он использовал это приложение. В таких ситуациях системный администратор часто тратит немало времени на поиск проблемы, которой бы даже не существовало, если бы процесс установки был автоматизирован. Как вы думаете, почему простая переустановка программы решает так много проблем, заявленных пользователями?

Второй тип скрытых затрат относится к *неоднородности*. Если вы вручную устанавливаете операционную систему, вы никогда не добьетесь той же конфигурации на другой машине. Никогда. Когда мы вручную устанавливали приложения на компьютеры, мы выяснили, что невозможно добиться одинаковой конфигурации приложений на разных машинах, сколько бы мы ни учили системных администраторов. В некоторых случаях техник забывал о той или иной настройке, в других случаях эти новые настройки были эффективнее. В результате пользователи зачастую обнаруживали, что их новые рабочие станции не были настроены должным образом. Или же пользователь при смене рабочих станций понимает, что их настройки отличаются, а в работе приложений возникают сбои. Автоматизация решает эту проблему.

Пример: автоматизация установки Windows NT снижает стресс

Перед тем как в Bell Labs была автоматизирована установка Windows NT, Том выяснил, что системные администраторы тратят около четверти своего времени на решение проблем, которые возникли из-за ошибок при ручной установке. Работа пользователей на новых машинах становилась действительно продуктивной только после того, как они несколько дней, обычно не меньше недели, постоянно обращались в службу поддержки, чтобы решить возникающие проблемы. Системные администраторы работали в стрессовых условиях, но представьте себе стресс пользователей! Все это производило неприятное первое впечатление. Первая встреча каждого нового сотрудника с системным администратором происходила по той причине, что машина с самого начала не работала должным образом. Неужели они ничего не могут делать как надо?

Естественно, системным администраторам необходимо было найти способ снизить количество проблем, возникающих из-за установки. Решением стала автоматизация. Процесс установки был автоматизирован с помощью собственной системы, получившей название AutoLoad (Fulmer and Levine 1998). Эта программа устанавливала ОС, а также все приложения и драйверы.

После того как установка была автоматизирована, системным администраторам стало намного проще жить. Утомительный процесс установки теперь стал быстрым и простым. Он позволял избежать всех ошибок, которые возникали при ручной установке. Теперь системные администраторы тратили намного меньше времени на исправление собственных ошибок. И что самое главное, жизнь пользователей тоже стала намного проще.

3.1.1.1. Удостоверьтесь, что ваша автоматизированная система действительно автоматизирована

Настройка системы автоматической установки требует больших усилий. Однако в результате эти усилия окупятся и сэкономят вам больше времени, чем вы потратите на настройку. Помните об этом, если вы в процессе настройки вдруг потеряете терпение. Кроме того, помните, что, раз уж вы собираетесь установить

автоматизированную систему, выполнить это необходимо должным образом. В противном случае впоследствии у вас будет в два раза больше проблем, чем раньше.

Самый важный аспект автоматизации заключается в том, что установка должна быть *полностью* автоматизирована. На первый взгляд это кажется очевидным, но реализация этого аспекта – совсем другое дело. Мы считаем, что стоит потратить дополнительные усилия, чтобы впоследствии не возвращаться к машине снова и снова для подтверждения того или иного действия или перехода к следующему этапу установки. Это означает, что при подтверждении будет выбран верный вариант ответа и об этих этапах никто не забудет и не пропустит их. Кроме того, системные администраторы могут более эффективно управлять своим временем. Они смогут сконцентрироваться на следующей задаче, вместо того чтобы думать о том, не пора ли вернуться к машине, чтобы запустить следующий этап установки.

Машина сообщает: «Все готово!»

Один системный администратор изменил систему JumpStart в Solaris таким образом, чтобы в службу поддержки по электронной почте отправлялось письмо, когда процесс установки будет завершен. Письмо отправлялось с новой машины, что позволяло протестировать работу машины. В теле письма генерировался текст с именем узла сети, типом оборудования и другой информацией, необходимой для службы поддержки, чтобы добавить машину в список учетных записей. Когда много работы, можно запросто забыть о том, что необходимо вернуться к машине и удостовериться, что установка успешно завершена. Благодаря этому решению системному администратору можно было не тратить время на проверку машин. Вместо этого ему достаточно было просто внести в свой список задач пункт о проверке электронной почты в определенное время.

Лучшие системы установки все взаимодействие с человеком выполняют в самом начале, а затем завершают работу полностью автоматически. В некоторых системах вообще ничего не нужно вводить, так как автоматика «знает», что делать, основываясь на MAC-адресе узла сети Ethernet. У техников должна быть возможность покинуть машину, будучи уверенными, что процедура завершится самостоятельно. Процедуру, требующую возвращения человека посреди установки для ответа на тот или иной вопрос, нельзя назвать полностью автоматизированной, и она теряет эффективность. Например, если системный администратор забудет об установке и отправится на обед или совещание, машина будет простаивать, пока администратор не вернется. Если системного администратора нет в офисе и только он может помочь сотрудникам, прервавшим работу, то всем, кому требовалась эта машина, придется его ждать. Или еще хуже: кто-то еще может попытаться самостоятельно завершить установку, создав тем самым узел сети, который затем потребует отладки.

Система JumpStart для ОС Solaris – безупречный образец полностью автоматизированной программы установки. Программа на сервере JumpStart запрашивает, какой шаблон использовать для нового пользователя. Старший системный администратор может настроить эти шаблоны заранее. Когда приходит время

устанавливать операционную систему, техник – возможно, даже офисный служащий, направленный для запуска процесса, – должен просто ввести команду `boot net - install`. Служащий ожидает подтверждения, что процесс установки начался, а затем уходит. Через 30–90 мин, в зависимости от скорости сети, машина загружена, сконфигурирована и готова к работе.

Устраните из процесса автоматической установки все операции, выполняемые вручную

Том был наставником для нового системного администратора, который занимался установкой JumpStart. Системный администратор передал Тому демонстрационный ролик, в котором установка ОС проходила должным образом. После установки системный администратор продемонстрировал, каким образом с помощью простого скрипта можно завершить конфигурирование. Том поздравил его с этим достижением, но вежливо попросил системного администратора интегрировать последний этап в процесс установки JumpStart. В результате новая система JumpStart была полностью автоматизирована только после четырех попыток провести эту процедуру.

Мораль этой истории в том, что системный администратор не совершил никакой ошибки. Но при этом он не полностью автоматизировал процесс. Очень просто забыть, что после автоматического процесса установки необходимо вручную запустить тот самый простой скрипт. Кроме того, важно помнить, что при автоматизации того или иного процесса, особенно в первый раз, зачастую приходится повозиться, чтобы все сделать правильно.

Когда вы решите, что закончили автоматизацию того или иного процесса, попросите опробовать вашу систему какого-нибудь человека, незнакомого с вашей работой. Проинструктируйте его одним предложением и больше ему не помогайте. Если у него возникнут проблемы, значит, вам необходимо улучшить данный аспект вашей системы. Повторяйте эту процедуру до тех пор, пока ваш помощник не сможет самостоятельно использовать систему.

3.1.1.2. Частично автоматизированная установка

Частичная автоматизация лучше, чем ее полное отсутствие. До тех пор пока система установки не будет работать идеально, необходимо обеспечить какие-то временные средства для некоторых этапов. Автоматизация оставшегося 1% может занять больше времени, чем автоматизация первых 99%.

Отсутствие автоматизации может быть оправданно, если используется небольшое количество тех или иных платформ, если затраты на полную автоматизацию превышают экономию времени или если поставщик оказал нам медвежью услугу, сделав автоматизацию невозможной (или неподдерживаемой).

Основная временная мера – документирование всего процесса, которое позволит впоследствии воспроизводить его в точности[1]. Документирование может произ-

[1] Это, однако, не означает, что автоматизация устраняет необходимость документирования.

водиться в виде записей при создании первой системы, чтобы на различные запросы можно было давать одни и те же ответы.

Можно автоматизировать различные этапы установки. Некоторые из них отлично поддаются автоматизации. Например, процесс инициализации, представленный на рис. 3.1, конфигурирует ОС, установленную с настройками по умолчанию, в соответствии с конкретным сетевым окружением. Как правило, сюда входят установка определенных файлов, настройка доступа и перезагрузка. Спасительным решением здесь может быть скрипт, копирующий определенный набор файлов в определенное место на диске. Можно даже упаковать в архив tar или zip файлы, измененные во время настройки, а затем распаковать их на машины после стандартной процедуры установки.

Можно придумать и более изощренные временные решения.

Пример: частично завершенная установка

В первых версиях AutoLoad в Microsoft Windows NT 4.0 (Fulmer and Levine 1998) не поддерживалась автоматическая установка драйверов сторонних поставщиков. Например, драйвер звуковой карты нужно было устанавливать вручную. Если установка производилась на компьютере на рабочем месте сотрудника, для последнего выводилось сообщение от системного администратора, информирующее о том, что клиент сможет войти в систему и использовать ее, но звук при этом работать не будет. В том же сообщении указывалось время, в которое подойдет системный администратор и решит эту проблему. Естественно, в таких случаях автоматизация системы была бы предпочтительнее, но используемый метод стал хорошим временным решением.

Временные меры

Вопрос: Что необходимо сделать, чтобы временные меры не стали постоянным решением?

Ответ: Следует создать заявку, в которой будет отмечена необходимость в постоянном решении.

3.1.1.3. Клонирование и другие методы

В некоторых сетях для создания новых машин используется клонирование жестких дисков. Клонирование жесткого диска подразумевает создание узла с точной конфигурацией ПО, которая необходима для всех развертываемых узлов. Затем жесткий диск этого узла клонируется (копируется) на все новые компьютеры. Первую машину часто называют «золотым узлом». Вместо того чтобы снова и снова копировать жесткий диск, его содержимое можно скопировать на компакт-диск, ленточный накопитель или файловый сервер, которые впоследствии будут использоваться при установке. Некоторые поставщики предоставляют компаниям помощь в этой области, выпуская специализированное оборудование и программное обеспечение для клонирования.

Мы предпочитаем автоматизированный процесс установки копированию диска по нескольким причинам. Во-первых, если по аппаратному обеспечению новая машина значительно отличается от старой, необходимо создать отдельный мастер-образ. Даже при отсутствии воображения можно представить себе огромное количество мастер-образов, которое может понадобиться в итоге. Ситуация может осложниться еще больше: если вы захотите внести хотя бы одно изменение, вам придется вносить его во все мастер-образы. И наконец, наличие резервных машин для каждого типа оборудования, требующего новых образов, значительно повышает расходы и усилия, необходимые для установки.

Поставщики некоторых ОС не поддерживают клонированные диски, так как процесс установки может изменяться на основе таких факторов, как тип обнаруженного оборудования. Windows NT генерирует в процессе установки уникальный идентификатор безопасности (Security Identifier, SID) для каждой машины. Первоначальное ПО для клонирования Windows NT не было способно воспроизводить эту функциональность, что вызывало немало проблем. Впоследствии эта проблема была решена.

Можно достичь золотой середины, применяя как автоматизацию, так и клонирование. В некоторых сетях клонируют диски для минимальной установки ОС, а затем используют автоматическую систему установки приложений и патчей поверх ОС. В других сетях используют стандартную систему установки ОС, а затем «клонируют» приложения или модификации системы на машины.

И наконец, некоторые поставщики ОС не предоставляют возможности автоматизировать установку. Однако можно найти способы усовершенствовать этот процесс. В SunOS 4.x не было ничего подобного JumpStart системы Solaris, поэтому во многих сетях ОС загружали с компакт-диска, а затем запускали скрипт, завершающий процесс. Установка с компакт-диска приводила машину в известное состояние, а скрипт завершал процесс.

PARIS: автоматизированная установка SunOS 4.x

При наличии достаточного количества времени и денег возможно все. Вы можете даже создать собственную систему установки. Всем известно, что установка SunOS 4.x не поддается автоматизации. Всем, кроме Виктора Духовны (Viktor Dukhovni), создавшего в 1992 году программируемую службу автоматической удаленной установки PARIS (Programmable Automatic Remote Installation Service) для компании Lehman Brothers. Система PARIS автоматизировала процесс параллельной сетевой установки SunOS 4.x на несколько узлов сети задолго до появления JumpStart в Sun OS 5.x.

В то время наилучшее решение требовало установки ОС с компакт-диска на каждый узел сети. Служба PARIS позволила системным администраторам в Нью-Йорке удаленно запускать обновление ОС на всех машинах в офисе филиала. После этого администраторы могли отправляться домой или на обед, а некоторое время спустя получить информацию о том, что установка на всех машинах завершилась успешно. Возможность назначить одновременную автоматизированную установку на группу машин – функция PARIS, которой до сих пор нет в большинстве систем установки от производителей ОС.

До тех пор пока в компании Sun не создали JumpStart, во многих сетях приходилось применять собственные решения.

3.1.1.4. Стоит ли доверять установкам от поставщиков

Обычно компьютеры поставляются с предустановленной ОС. Зная это, вы можете решить, что вам не надо переустанавливать ОС, если кто-то сделал это за вас. Мы не согласны. На самом деле мы считаем, что переустановка ОС в конечном итоге упростит вам жизнь.

Переустановка ОС с нуля предпочтительнее по нескольким причинам. Во-первых, прежде чем машина сможет работать в вашей сети, вам, вероятно, потребуется установить другие приложения и локализации поверх установленной поставщиком ОС. Автоматизация всего процесса установки с нуля зачастую проще, чем установка приложений и конфигурирование предустановленной ОС. Во-вторых, поставщики вносят изменения в конфигурацию предустановленной ОС в собственных целях, никого об этом не уведомляя. Установка с нуля дает вам *известное состояние* каждой машины. Использование предустановленной ОС означает отклонения от вашей стандартной конфигурации. Порой эти отклонения могут вызвать проблемы.

Другая причина для отказа от использования предустановленной ОС – то, что время от времени ОС узлов сети приходится переустанавливать. Например, жесткий диск может выйти из строя и быть заменен на чистый или у вас может существовать правило переустанавливать ОС при передаче рабочей станции от одного сотрудника другому. Если часть ваших машин работает с предустановленной ОС, а остальные – с установленной вами, у вас появляются две платформы, требующие поддержки. Между ними существуют различия. Если в аварийной ситуации вы обнаружите, что не можете провести загрузку или установку на определенном узле сети без помощи поставщика, *вряд ли* это вас обрадует.

История про ОС с обязательной предустановкой поставщиком

Жил-был Том, и решил он однажды поэкспериментировать с системой UNIX от японской компании, которая тогда только появилась на рынке рабочих станций. Поставщик продавал компьютеры с предустановленной видоизмененной версией UNIX. К сожалению, когда системные администраторы портировали приложения, на машине произошел неисправимый сбой. Том связался с поставщиком, и тот ответил, что вышлет жесткий диск с предустановленной ОС – из самой Японии! Несмотря на то что старый жесткий диск был исправен и мог быть отформатирован и повторно использован, поставщик не предусмотрел метода, с помощью которого пользователи могли бы переустановить ОС, даже с резервных копий на ленточных накопителях.

К счастью для Тома, эта рабочая станция не использовалась для критически важных служб. Представьте, что случилось бы, если бы Том внезапно обнаружил, что его сеть не работает, или, еще хуже, невозможен расчет заработной платы, пока машина не начнет работать! Раздражительные пользователи вряд ли обрадуются тому, что они не получат зарплаты, пока жесткий диск не приедет из Японии.

Если эта машина выполняет критически важные функции, имеет смысл держать под рукой запасной жесткий диск с предустановленной системой.

> Также стоит написать указания, как физически установить его и вернуть систему в рабочее состояние.
>
> Мораль этой истории в том, что, если вам *приходится* пользоваться предустановленной системой от поставщика, лучше узнать, как восстановить систему с нуля, сразу после поставки оборудования, а не тогда, когда произойдет сбой.

В приведенной выше истории рассказывалось про ОС давних времен. Тем не менее история повторяется. Поставщики компьютеров предустанавливают ОС и часто вместе с ней специальные приложения, дополнения и драйверы. Всегда проверяйте, поставляются ли на диске для восстановления системы дополнения, включенные в ОС. Иногда эти приложения не слишком нужны, так как представляют собой бесплатные инструменты, которые не стоят отданных за них денег. Но это могут быть и драйверы критически важных устройств. В особенности это важно для ноутбуков, которым часто требуются драйверы, не входящие в состав основной версии ОС. У Тома были такие проблемы во время написания этой книги. После переустановки Windows NT на его ноутбуке ему нужно было установить драйверы для работы слотов PCMCIA. Драйверы нельзя было загрузить на ноутбук через модем или сетевую карту, так как они сами подключались через PCMCIA. Пришлось записывать драйверы на дискеты с помощью другого компьютера. Если бы не было второго компьютера, получился бы замкнутый круг.

Со временем таких проблем стало меньше, по мере того как специфичные устройства в ноутбуках уступали место широко распространенным стандартизированным компонентам. Компания Майкрософт также уступила требованиям сделать свои операционные системы менее зависимыми от оборудования, на котором они установлены. Хотя ситуация и улучшилась со времен драйверов низкого уровня, поставщики пытаются выделяться, включая в поставку программное обеспечение, уникальное для каждой модели. Но это сводит на нет попытки создать единый образ, который будет одинаково работать на всех платформах.

Некоторые поставщики могут предустанавливать систему с предоставленного вами образа диска. Такая услуга не только избавляет вас от необходимости самостоятельно устанавливать системы, но и дает вам знание того, что именно было установлено. Однако на вас по-прежнему лежит обязанность обновлять мастер-образ по мере появления новых устройств и моделей.

3.1.1.5. Контрольные списки при установке

Какой бы способ установки ОС вы ни использовали – ручной или полностью автоматизированный, – вы можете улучшить согласованность процесса с помощью контрольных списков. Эти списки помогают удостовериться, что техники не пропустят ни одного этапа. Польза таких списков очевидна, если процесс установки полностью выполняется вручную. Даже если установку проводит один системный администратор, полностью уверенный в согласованности установки всех ОС («я все делаю сам»), он поймет преимущества использования контрольных списков. И конечно же, эти списки могут послужить основой для системы обучения новых системных администраторов или подготовки толкового служащего, который будет выполнять эту работу в соответствии с пунктами списка (более подробную информацию по контрольным спискам вы найдете в разделе 9.1.4).

Даже если процесс установки ОС полностью автоматизирован, грамотный контрольный список все же может принести пользу. Некоторые действия невозможно автоматизировать, так как их необходимо выполнить физически (например, запустить процесс установки; удостовериться, что мышь работает; протереть экран монитора; предоставить пользователю на выбор несколько ковриков для мыши). В ваш контрольный список могут входить и другие подобные задачи: обновление инвентаризационных описей, составление заказов на сетевые кабели (если их количество меньше определенного числа), проверка неделю спустя, не возникли ли у пользователей проблемы или какие-либо вопросы.

3.1.2. Обновление системного ПО и приложений

Не правда ли, было бы здорово, если бы обязанности системного администратора ограничивались установкой операционной системы и приложений? К сожалению, с течением времени обнаруживаются новые ошибки и новые бреши в системе безопасности, и все их необходимо исправлять. Кроме того, появляются прекрасные новые приложения, которые необходимо устанавливать. Все эти задачи относятся к области **обновления программного обеспечения**. Кто-то обязан эти задачи выполнять, и этот кто-то – вы. Не волнуйтесь, вам не придется тратить все свое время на обновление ПО. Как и в случае с установкой, процесс обновления можно автоматизировать, сэкономив время и силы.

Каждый поставщик дает собственное название своей системе автоматизации обновления ПО: в Solaris это AutoPatch; в Microsoft Windows – SMS; различные пользователи создали собственные оболочки поверх RPM в Red Hat Linux, RoboInst в SGI IRIX и Software Distributor (SD-UX) в HP-UX. Существуют и кросс-платформенные системы (Ressman and Valdés 2000).

Системы обновления ПО должны быть достаточно универсальными, чтобы они позволяли устанавливать новые приложения и обновлять уже имеющиеся, а также устанавливать патчи ОС. Если система способна только устанавливать патчи, новые приложения можно упаковать и использовать их в качестве патчей. Такие системы также можно использовать для внесения незначительных изменений на большом количестве узлов сети. Небольшие изменения конфигурации, такие как новый файл /etc/ntp.conf, можно упаковать в патч и установить автоматически. Большинство систем позволяет включать п**остустановочные скрипты** – программы, которые при запуске выполняют изменения, необходимые для установки пакета. Для внесения сложных изменений можно даже создать отдельный пакет, содержащий *только* постустановочный скрипт.

Пример: установка новой системы печати

Одна компания, которой была необходима новая система печати, наняла системного администратора. Новая система была разработана, настроена и протестирована за очень короткое время. Однако консультант потратил несколько недель, выполняя черную работу по установке нового клиентского ПО на каждую рабочую станцию. Дело в том, что в сети не было автоматизированного способа обновления ПО. Некоторое время спустя консультанта пригласила другая компания для установки подобной системы. На этот раз в корпоративной сети использовалась отличная (и документированная!) система обновления ПО. Внести изменения мож-

но было достаточно просто. Клиентское ПО было упаковано и быстро установлено на все рабочие станции. В первой компании бóльшая часть затрат на создание новой системы печати ушла на ее установку на рабочие станции. Во второй компании основные затраты ушли на выполнение главной задачи, а именно на новую систему печати. В первой компании считали, что отказ от внедрения системы автоматизации обновлений позволяет сэкономить деньги. Вместо этого компания тратила крупные суммы каждый раз, когда возникала необходимость внедрить новое программное обеспечение. Компании не хватило предусмотрительности понять, что в будущем придется внедрять новое ПО. А вторая компания экономила деньги, заранее вложив определенную сумму.

3.1.2.1. Процесс обновления отличается от установки

Автоматизация обновления ПО схожа с автоматизацией первичной установки, но между ними есть и несколько существенных различий.

- *Узел сети находится в рабочем состоянии.* Обновление устанавливается на машины, которые находятся в рабочем состоянии, а при первичной установке необходимо выполнить ряд дополнительных задач, таких как создание разделов на дисках и определение сетевых параметров. На самом деле первичная установка проводится на узле, который находится в отключенном состоянии (например, на машине с абсолютно чистым жестким диском).
- *Узел сети находится в офисе.* Система обновления должна быть способна выполнять задачи в собственной сети узла. Она не должна прерывать работу сети или других узлов. Процесс первичной установки можно проводить в лаборатории, где имеется доступ к специализированному оборудованию. Например, в крупных компаниях, как правило, выделяют отдельное **помещение для установки** (с широкополосной сетью), где машины подготавливают к работе и только после этого переносят в офис новых владельцев.
- *Отсутствует необходимость в физическом доступе.* При обновлении ПО нет необходимости в физическом доступе к рабочей станции (что может помешать работе пользователей). Кроме того, координация такого доступа может потребовать больших затрат. Пропущенные встречи, отпуска пользователей, машины в запертых кабинетах – все это может привести к кошмарной необходимости перепланирования встреч. Физический доступ к компьютерам автоматизировать нельзя.
- *Узел сети уже используется.* Обновление ПО проводится на машинах, которые используются на протяжении какого-то времени. А значит, клиент ожидает, что машину можно будет и дальше использовать после завершения процесса обновления. Вы не имеете права испортить машину! Если же что-то пойдет не так при первичной установке, вы можете просто стереть диск и начать все заново.
- *Узел сети может не находиться в «известном состоянии».* Поэтому автоматизация должна быть более точной, так как с момента первичной установки в ОС могли возникнуть ошибки. При первичной установке состояние машины является более контролируемым.
- *Узел сети может использоваться сотрудниками в процессе обновления.* Некоторые обновления невозможно установить в то время, когда машина

используется. Microsoft System Management Service решает эту проблему с помощью установки пакетов после того, как пользователь ввел свое имя и пароль при входе в систему, но до того, как он получает доступ к машине. Система AutoPatch, используемая в Bell Labs, отсылает электронное письмо клиенту за два дня и позволяет клиенту отложить обновление на несколько дней, создав файл с определенным именем в каталоге /tmp.

- *Узел сети может отсутствовать.* В нашу эпоху ноутбуков есть большая вероятность того, что узел не присутствует в сети в момент установки обновлений. Система обновления не может больше априори допускать, что узел присутствует. Либо она должна отслеживать его появление в сети, либо сам узел должен запускать ее по определенному расписанию, а также при каждом подключении к своей домашней сети.
- *Узел сети может иметь мультисистемную загрузку.* В нашу эпоху узлов с мультисистемной загрузкой система обновления, предназначенная для настольных компьютеров, должна точно контролировать доступ к нужной ОС. Персональный компьютер с мультитсистемной загрузкой Windows в одном разделе и Linux в другом может месяцами работать на Linux. При этом обновления ОС Windows будут пропускаться. Системы обновления как для Linux, так и для Windows должны быть достаточно «интеллектуальными», чтобы справиться с такой ситуацией.

3.1.2.2. Одна, несколько, много

Последствия ошибок при установке патчей отличаются от таковых при установке ОС. Пользователь, скорее всего, даже не узнает, были ли ошибки при установке ОС, так как до этого узел сети фактически не используется. Однако узел сети, на который устанавливается обновление, как правило, уже находится на рабочем столе сотрудника. Ошибки обновления, которые перевели машину в нерабочее состояние, гораздо заметнее и вызывают гораздо большее раздражение у пользователей.

Вы можете снизить риск ошибок обновления, применив метод **«одна, несколько, много»**.

- *Одна.* Прежде всего установите патч на одну машину. Лучше всего на свою собственную – тогда у вас будет дополнительный стимул все сделать правильно. Если при обновлении возникнут ошибки, вносите в процесс изменения до тех пор, пока он не будет работать на одной машине без ошибок.
- *Несколько.* Далее попробуйте установить патч на несколько других машин. Если это возможно, стоит протестировать автоматизированный процесс обновления на рабочих станциях остальных системных администраторов, прежде чем задействовать машины пользователей. Системные администраторы проявляют чуть больше понимания. Затем протестируйте систему на нескольких машинах дружелюбно настроенных к вам пользователей (не системных администраторов).
- *Много.* Протестировав свою систему и убедившись, что она не уничтожит ничей жесткий диск, начинайте постепенно переходить ко все большим и большим группам пользователей, нетерпимых к риску.

Автоматизированная система обновления потенциально способна нанести обширные повреждения. Весь процесс *должен* быть хорошо документирован, чтобы обеспечить максимальную степень управления риском. Необходимо обеспечить грамотное описание и повторяемость процесса, и вы *должны* пытаться улучшить его после каждого использования. Вы сможете избежать больших

проблем, если будете следовать этой системе. При каждой установке чего-либо вы идете на риск. Ненужный риск недопустим.

Автоматизированная система установки патчей аналогична клиническим испытаниям нового экспериментального противогриппозного препарата. Вы не станете давать препарат, не прошедший испытания, тысячам пациентов. Сначала необходимо провести испытания на небольшой группе осведомленных добровольцев. Точно так же нельзя внедрять автоматизированную систему установки патчей до тех пор, пока вы не убедитесь, что она не станет причиной серьезных повреждений. Представьте себе, как сильно могут рассердиться пользователи, если ваш патч уничтожит их машины, а они даже не замечали ошибки, которую тот самый патч должен был исправить!

Ниже приведены советы по первым этапам в процессе обновления.

- Создайте строго определенное обновление, которое будет установлено на все узлы сети. Представьте это обновление на утверждение. После представления начнется этап согласования для утверждения всеми заинтересованными сторонами. Такой порядок предотвратит установку обычных, не критически важных для бизнеса программных пакетов чрезмерно активными системными администраторами.
- Составьте план оповещения, чтобы те, кого касаются обновления, не были удивлены. Следуйте этому плану *каждый раз*, так как постоянство удобно для пользователей.
- Когда вы будете готовы перейти к этапу *«несколько»*, определите (и используйте!) критерии успешности, например, такие: *если сбоев не было, каждая следующая группа будет больше предыдущей примерно на 50%; если произошел один сбой, размер группы снова сокращается до одного узла и начинает расти заново.*
- И наконец выработайте способ для пользователей остановить процесс обновления, если произойдет опасный сбой. Документация процесса должна отображать, кто имеет полномочия потребовать остановки, как это сделать, кто обладает полномочиями для утверждения запроса и что следует предпринять дальше.

3.1.3. Конфигурирование сети

Третий компонент, необходимый для сетей, объединяющих большое количество рабочих станций, – это способ автоматизации обновления **сетевых параметров** – тех считанных битов информации, от которой часто зависит загрузка компьютеров и их объединение в сеть. Эта информация может значительно различаться в отдельных подсетях или даже в отдельных узлах сети. А следовательно, такое обновление должно производиться иначе, чем, скажем, установка приложений, когда одно и то же приложение устанавливается на всех узлах сети с одинаковой конфигурацией. Поэтому система автоматизации обновления сетевых параметров обычно создается отдельно от остальных систем.

Наиболее распространенная система автоматизации этого процесса – DHCP. Серверы DHCP от некоторых поставщиков настраиваются за несколько секунд, другие серверы – значительно дольше. Создание глобальной архитектуры DNS/DHCP с десятками или сотнями сетей требует основательного планирования и специальных знаний. У некоторых поставщиков DHCP есть профессиональные обслуживающие организации, которые помогают в этом процессе, что особенно ценно для глобальных предприятий.

Для малых компаний может быть неочевидна ценность затраты пары дней на изучение того, что, скорее всего, поможет вам сэкономить лишь минуту-другую во время настройки машины. Ввести вручную IP-адрес несложно, и, если уж на то пошло, почему бы не ввести вручную сетевую маску и пару других параметров, верно?

Неверно. Конечно, вы сэкономите день или два, если не настроите DHCP-сервер. Но вот в чем проблема: помните, в начале этой главы мы упоминали о возможной расплате за беспечность? Если вы не используете DHCP, то рано или поздно столкнетесь с жестокой реальностью. В конце концов вам потребуется изменить нумерацию IP или маску подсети, IP-адрес DNS-сервера или несколько параметров сети. Если у вас нет DHCP, вы потратите недели или месяцы на одно изменение, потому что вам придется организовать команду сотрудников, чтобы внести изменения на все узлы вашей сети. Незначительные вложения в DHCP в конечном итоге сделают все будущие изменения практически бесплатными.

Все, что должно быть сделано, должно быть сделано хорошо. DHCP тоже можно применять хорошо или плохо. В следующем разделе мы обсудим то, что нам об этом известно.

3.1.3.1. Используйте шаблоны, а не конфигурируйте каждый отдельный узел

Системы DHCP должны иметь систему шаблонов. Некоторые системы DHCP хранят отдельные параметры, присвоенные каждому отдельному узлу сети. Другие системы DHCP хранят шаблоны, описывающие, какие параметры присваиваются узлам различных классов. Преимущество шаблонов в том, что при внесении изменений на множестве узлов вам нужно будет просто изменить шаблон, что значительно лучше, чем прокручивать длинный список узлов сети, пытаясь найти те, которые требуется изменить. Еще одно преимущество в том, что значительно уменьшается вероятность появления ошибки в синтаксисе, если конфигурационный файл генерируется программой. Исходя из того, что шаблоны синтаксически правильны, конфигурация тоже будет верной.

Такая система необязательно должна быть сложной. Многие системные администраторы пишут небольшие программы, чтобы создать свою систему шаблонов. Список узлов сети хранится в базе данных (или даже в простом текстовом файле), и программа использует эти данные для конфигурирования сервера DHCP. Вместо того чтобы вводить информацию по каждому отдельному узлу сети в новый файл или создавать сложную базу данных, информацию можно внедрить в вашу существующую базу данных или файл с перечнем оборудования. Например, в UNIX-сетях достаточно просто ввести эту информацию в уже ведущийся файл /etc/ethers. Этот файл затем используется программой, которая генерирует конфигурацию DHCP. Ниже приведен пример строк из подобного файла:

```
8:0:20:1d:36:3a         adagio          #DHCP=sun
0:a0:c9:e1:af:2f        talpc           #DHCP=nt
0:60:b0:97:3d:77        sec4            #DHCP=hp4
0:a0:cc:55:5d:a2        bloop           #DHCP=any
0:0:a7:14:99:24         ostenato        #DHCP=ncd-barney
0:10:4b:52:de:c9        tallt           #DHCP=nt
0:10:4b:52:de:c9        tallt-home      #DHCP=nt
0:10:4b:52:de:c9        tallt-lab4      #DHCP=nt
0:10:4b:52:de:c9        tallt-lab5      #DHCP=nt
```

Маркер `#DHCP=` должен обрабатываться как комментарий всеми действующими программами, обращающимися к файлу. Но программа, генерирующая конфигурацию для DHCP-сервера, использует эти коды для определения того, что следует генерировать для данного узла сети. Узлы `adagio`, `talpc` и `sec4` получат правильную конфигурацию для рабочей станции Sun, узла Windows NT и принтера HP LaserJet 4 соответственно. Узел `ostenato` – это X-терминал NCD, загружающий TFTP-сервер `barney`. Шаблон NCD принимает параметр, благодаря которому становится достаточно универсальным для всех узлов, требующих считывания конфигурационного файла с TFTP-сервера. Последние четыре строки показывают, что ноутбук Тома должен получить разные IP-адреса в зависимости от подсети, к которой он может быть подключен: в офисе, дома или в лаборатории на четвертом либо пятом этаже. Обратите внимание, что, даже если мы и используем статическое назначение, у узлов по-прежнему остается возможность сменить сеть[1].

Внедрив эту информацию в файл /etc/ethers, мы снизили вероятность появления ошибок. Если бы информация была в отдельном файле, данные могли бы противоречить друг другу.

Другие параметры можно добавить тем же способом. Информация о сети записывается в комментариях в файл UNIX-системы /etc/hosts наряду с другими маркерами, отображающими JumpStart и иные параметры. Скрипт извлекает эту информацию для использования в файлах конфигурации JumpStart и DHCP и в других системах. Отредактировав один-единственный файл, системный администратор может выполнить огромное количество работы! Проект с открытым кодом HostDB[2] является развитием этой идеи – достаточно отредактировать один файл, чтобы сгенерировать конфигурационные файлы для DHCP и DNS, а также распределить их на соответствующие серверы.

3.1.3.2. Когда применять динамическую аренду адресов

Как правило, DHCP назначает отдельный IP-адрес каждому узлу сети. Функция **динамической аренды адресов** позволяет вам указать диапазон IP-адресов, которые можно присваивать узлам сети. Эти узлы смогут при каждом подключении к сети получать новый IP-адрес. Преимущество в том, что облегчается работа администраторов и повышается удобство для пользователей.

Так как эта функция используется очень часто, многие считают, что адреса, назначаемые с помощью DHCP, *должны* распределяться именно так. На самом деле это не так. Зачастую лучше закрепить конкретный IP-адрес за конкретным узлом сети. Это особенно важно для серверов, чьи IP-адреса прописываются в конфигурационных файлах других узлов, таких как DNS-серверы и межсетевые экраны. Этот метод называется **статическим назначением адресов** в RFC или **постоянной арендой адресов** в DHCP-серверах компании Майкрософт.

Динамическое распределение следует использовать в случаях, когда много узлов конкурируют за малое количество IP-адресов. Например, у вас может быть сервер удаленного доступа (RAS, Remote Access Server) на 200 модемов для тысяч

---

[1] Системным администраторам следует помнить, что этот метод применим к IP-адресам, указанным в другом месте или назначенным через DHCP из пространства адресов.

[2] *http://everythingsysadmin.com/hostdb/*

узлов, которые могут с ним соединиться. В этой ситуации имеет смысл организовать динамическое пространство на 220 адресов[1]. Можно привести еще один пример: сеть с часто сменяющимися временными узлами, такая как лабораторный испытательный стенд, комнаты настройки компьютеров или сеть для ноутбуков посетителей. В этих случаях может быть достаточно физического пространства или портов только для определенного количества компьютеров. Пространство IP-адресов можно несколько расширить сверх этого максимума.

Типичная офисная локальная сеть лучше подходит для динамически назначаемой аренды. Тем не менее есть преимущества в выделении статической аренды адресов для отдельных машин. Например, удостоверившись, что конкретные машины всегда получают одни и те же адреса, вы предотвратите вероятность того, что эти машины не смогут получить IP-адрес, когда диапазон адресов будет исчерпан. Представьте, что произойдет, если из-за наплыва посетителей будут исчерпаны адреса и директор не сможет получить доступ куда-либо из-за того, что его компьютер не способен получить IP-адрес.

Еще одна причина для назначения статических IP-адресов – повышение удобства использования файлов журнала. Если рабочим станциям всегда присваиваются одни и те же IP-адреса, в файлах журнала они будут отображаться, соответственно, с теми же IP-адресами. Кроме того, некоторые программные пакеты могут некорректно работать с узлом с изменяющимся IP-адресом. Хотя эта ситуация чрезвычайно редкая, выделение статических адресов предотвращает подобные проблемы.

Использование только статических IP-адресов не является достаточной мерой для безопасности. В некоторых сетях отключают любое динамическое назначение адресов, считая, что это предотвратит использование их сети незваными гостями. В действительности же кто-нибудь все еще может вручную конфигурировать сетевые настройки. Программное обеспечение, позволяющее отслеживать сетевые пакеты, быстро выдаст достаточно информации, чтобы кто-то смог догадаться, какие IP-адреса не используются, какая маска у подсети, какими должны быть настройки DNS, шлюз по умолчанию и т. д.

Лучшее решение здесь – IEEE 802.1x. Этот стандарт **управления доступом к сети** определяет, будет ли разрешено новому узлу подключиться к сети. Изначально применявшееся в сетях WiFi, управление доступом к сети все шире используется и в проводных сетях. Коммутатор Ethernet, поддерживающий стандарт 802.1x, не дает новому узлу подключаться к сети, пока тот не пройдет определенную процедуру аутентификации. В зависимости от того, пройдена аутентификация или нет, разрешается передача данных либо узел получает отказ в доступе к сети.

3.1.3.3. Использование DHCP в сетях общего пользования

Многие использовали подобные решения еще до изобретения стандарта 802.1x. Наверняка вы бывали в отелях или других общественных местах, где сеть была

[1] Хотя в этой ситуации вам требуется пространство только на 200 IP-адресов, лучше иметь несколько больший диапазон. Например, если узел отключается, не прерывая аренду, IP-адрес будет занят до тех пор, пока не истечет срок аренды. Имеет смысл выделить дополнительные 10% IP-адресов для устранения потенциальных проблем.

сконфигурирована следующим образом: в сеть выйти очень легко, но можно получить доступ только к веб-странице авторизации. После авторизации (с помощью либо какого-то способа идентификации, либо платежа с кредитной карты) можно получить полный доступ. В таких ситуациях системные администраторы предпочитают решение plug-in-and-go (подключись-и-работай) для выделения пространства адресов, но при этом должна быть возможность проверки, есть ли у пользователей разрешение на использование ресурсов корпорации, университета или отеля. Более подробную информацию по ранее используемым средствам и методам вы найдете в следующих работах: Beck 1999, Valian and Watson 1999. Их системы позволяют незарегистрированным узлам зарегистрироваться от имени человека, который берет на себя ответственность за любой ущерб, нанесенный этими неизвестными узлами.

3.1.4. Старайтесь не использовать динамический DNS–сервер с DHCP

Нас не устраивает работа DHCP-систем, которые обновляют динамические DNS-серверы. Эта впечатляющее на первый взгляд свойство излишне усложняет систему и создает ненужный риск для безопасности.

В системах с динамическим DNS-сервером клиентский узел сообщает серверу DHCP, каким должно быть имя узла сети, а сервер DHCP отправляет обновления на DNS-сервер (клиентский узел также может отправлять обновления напрямую на DNS-сервер). Неважно, к какой сети подключена машина, информация DNS для этого узла соответствует имени узла.

Узлы со статической арендой всегда имеют одно и то же имя в DNS, так как они всегда получают один и тот же IP-адрес. При использовании динамической аренды IP-адрес узла выбирается из пространства адресов в DNS, каждый из которых, как правило, обладает шаблонным именем. Например, `dhcp-pool-10`, `dhcp-pool-11`, `dhcp-pool-12`. Неважно, какой узел сети получит десятый адрес из пространства, его имя в DNS всегда будет `dhcp-pool-10`. Это явно не соответствует имени узла, которое хранится в его локальной конфигурации.

Это несоответствие имеет значение лишь в том случае, если данная машина является сервером. То есть, если узел не запускает никакие службы, никто не будет обращаться к нему по имени, а поэтому не имеет значения, какое имя для него прописано в DNS. Если же узел запускает службы, эта машина должна получить постоянную аренду DHCP и всегда иметь одно и то же фиксированное имя. Службы, которые созданы для прямого общения с пользователями, не используют DNS для поиска узлов. Одним из примеров являются службы, которые разрешают узлам передавать друг другу файлы или устанавливать голосовую либо видеосвязь. При подключении к такой службе каждый узел регистрирует свой IP-адрес в центральном реестре, который использует фиксированное имя и/или IP-адрес. Этот метод используют средства связи стандарта H.323, такие как Microsoft Netmeeting.

Если позволить узлу определять собственное имя, появится риск нарушения безопасности. Имена узлов должны контролироваться централизованной системой, а не пользователем узла. Что если кто-то присвоит своему узлу имя, аналогичное имени критически важного сервера? Как система DNS/DHCP определит, какой узел является настоящим сервером? Большинство динамических систем DNS/DHCP позволяют заблокировать имена важных серверов, а это означает, что список важных серверов является новым пространством имен,

которое необходимо контролировать и обслуживать (глава 8). Если вы случайно забудете включить имя нового сервера, может произойти трагедия.

Старайтесь не допускать ситуаций, в которых простые ошибки одних пользователей могут помешать работе других. Архитекторы локальной сети давно поняли это в отношении разрешения клиентам самим устанавливать IP-адреса. И нам не стоит повторять эту ошибку, позволяя клиентам выбирать собственные имена узлов. До появления DHCP пользователи часто «вешали» локальную сеть, случайно устанавливая IP-адрес, аналогичный IP-адресу маршрутизатора. Клиентам выдавался список IP-адресов, которые можно использовать для настройки своих компьютеров. «Это первый предназначен для шлюза по умолчанию или все-таки второй? Да какого черта, шансы ведь 50/50, могу и угадать». Если же клиент установил неверный адрес, связь с маршрутизатором прерывалась.

Использование DHCP в значительной мере снижает шанс повторения подобной ситуации. Разрешение клиентам устанавливать собственное имя узла – один из вариантов той же ситуации, который приведет к подобным результатам. Например, может начаться эпидемия новых проблем, если пользователи в качестве имени узла выберут предоставленное им имя сервера электронной почты, имя домена или другой базовой службы.

Еще один вопрос относится к тому, каким образом аутентифицируются обновления DNS. Протоколы защиты для этих обновлений гарантируют, что узел, который добавил запись в DNS, – это тот же самый узел, который запрашивает удаление или замену этой записи. Протоколы не могут предотвратить первичный ввод данных и не могут контролировать формат или лексикон разрешенных имен. Мы уже предвидим ситуации, в которых пользователи настраивают свои компьютеры, используя дезориентирующие имена в попытке запутать или обмануть других (подобные аферы часто встречаются в Интернете[1]). И подобные ситуации вы сможете наблюдать в локальной сети.

Столько рисков ради какой-то одной сомнительной возможности! Защитники таких систем спорят, что всеми этими рисками можно управлять или их можно уменьшить с помощью дополнительных возможностей и настраиваемых средств. Наш ответ таков: добавление новых уровней сложных баз данных ради управления рисками требует массы усилий, и этого можно избежать, если просто-напросто не использовать упомянутую возможность.

Кое-кто может поспорить, что эта возможность улучшает отслеживаемость, так как в журналах всегда указывается одно и то же имя узла. Но мы возразим тем, что для улучшения отслеживаемости есть и другие способы. Если вам необходимо отследить несанкционированное поведение узла до конкретного пользователя, лучше всего воспользоваться системой регистрации и слежения (раздел 3.1.3.3).

Динамический DNS-сервер с DHCP создает систему, которая является более запутанной, более сложной для управления, более подверженной сбоям и менее безопасной. И все это в обмен на небольшую эстетическую приятность. Оно того не стоит.

Несмотря на эти недостатки, поставщики ОС начали создавать системы, которые при выключении обновления динамического DNS-сервера работают хуже. Ком-

[1] В течение многих лет *www.whitehouse.com* был порносайтом. Можете себе представить удивление пользователей, которым на самом деле был нужен сайт *www.whitehouse.gov*?

пании попадают в сложную ситуацию. Им приходится выбирать между внедрением новой технологии и снижением своих стандартов безопасности. К счастью, в индустрии безопасности существует такое понятие, как ограничение распространения. **Ограничение распространения** означает ограничение риска безопасности таким образом, чтобы он распространялся только в пределах определенной области. Рекомендуем ограничивать динамический DNS-сервер определенными сетевыми субдоменами, от которых не требуется высокая надежность. Например, все узлы, использующие динамический DNS-сервер, могут иметь такие имена, как uzel.dhcp.corp.primer.com. У имен узлов в зоне dhcp.corp.primer.com могут возникать конфликты и другие проблемы, но эти проблемы будут изолированы в этой одной зоне. Этот прием можно распространить на весь ряд обновлений динамического DNS-сервера, которых требуют контроллеры домена в Microsoft ActiveDirectory. Можно создать множество ограниченных областей для зон DNS с забавными именами, такими как _tcp.corp.primer.com и _udp.corp.primer.com (Liu 2001).

3.1.4.1. Управление сроками аренды DHCP

Управление сроками аренды может помочь в распределении обновлений. DHCP-клиентам задается определенный набор параметров, который будет использоваться в течение определенного периода времени. По истечении этого периода они должны обновить свою аренду. Изменения вносятся во время обновления.

Предположим, срок аренды определенной подсети – 2 недели. Предположим, что вы собираетесь изменить маску этой подсети. В обычных условиях можно рассчитывать на двухнедельный период ожидания, прежде чем все узлы получат эту новую маску подсети.

С другой стороны, если вы знаете о грядущих изменениях, то можете уменьшить срок аренды в период перед этими изменениями. После того как вы измените маску подсети в настройках сервера DHCP, обновление будет распределено быстро. Когда вы убедитесь, что изменение не имеет никаких пагубных последствий, вы можете увеличить срок аренды до первоначального значения (2 недели). Благодаря этому приему вы сможете гораздо быстрее вносить изменения.

DHCP для освобождения пользователей от ресурсов

Однажды в Bell Labs Тому необходимо было изменить IP-адрес первичного DNS-сервера. Внесение такого изменения заняло бы пару минут, но на распространение адреса по всем клиентам через DHCP могло уйти несколько недель. Пользователи не могли бы работать должным образом до тех пор, пока не получили бы свое обновление. А это вызвало бы массовый простой.

Том временно настроил сервер DHCP, переведя всех пользователей на совершенно другой DNS-сервер. Это был не самый оптимальный DNS-сервер для пользователей, но, по крайней мере, он работал. После того как первый DNS-сервер прекратил получать запросы, Том смог изменить IP-адрес и спокойно его протестировать. Позже он изменил настройки сервера DHCP и направил пользователей на новый IP-адрес первичного DNS-сервера.

Хотя в течение некоторого времени узлы сети использовали более медленный DNS-сервер, это позволило избежать полной остановки работы.

Определение оптимальной продолжительности стандартного срока аренды – спорный философский вопрос, который выходит за рамки этой книги. По этому вопросу рекомендуем прочесть следующие книги: «*The DHCP Handbook*» (Lemon and Droms 1999), «*DHCP: A Guide to Dynamic TCP/IP Network Configuration*» (Kercheval 1999).

Пример: использование сети ноутбуков в Bell Labs

В отделе компьютерных исследований Bell Labs в знаменитой «комнате UNIX» есть подсеть с пятиминутным сроком аренды адресов. Ноутбуки могут подключаться к этой подсети на короткое время. Срок аренды составляет всего 5 мин, так как системные администраторы пришли к выводу, что пользователю требуется около 5 мин на то, чтобы отнести ноутбук обратно в свой офис из комнаты UNIX. К этому времени срок аренды уже проходит. Теперь этот прием не так важен, поскольку современные DHCP-клиенты лучше справляются с быстрыми изменениями.

3.2. Тонкости

До этого момента мы обсуждали технические основы развертывания рабочей станции. Эти вопросы настолько важны, что правильное выполнение перечисленных задач повлияет практически на все остальные действия. Этот раздел поможет вам подкорректировать некоторые аспекты.

После того как вы разберетесь с основами, следите за появлением новых технологий, которые связаны с автоматизацией других аспектов поддержки рабочих станций (Miller and Donnini 2000a). Как правило, рабочие станции – самые распространенные машины в компании. Любое, даже незначительное снижение нагрузки на поддержку рабочих станций имеет огромное значение.

3.2.1. Полная уверенность в завершении

Существуют автоматизированные процессы, но помимо этого есть и автоматизация процесса. Если мы абсолютно уверены в процессе, мы избавлены от необходимости беспокоиться об ошибках. И поэтому мы начинаем искать новые способы применения этого же процесса.

Кристоф Кальт был полностью уверен, что Solaris JumpStart в Bell Labs работает без ошибок и полностью выполняет процесс. Система не может неожиданно приостановить работу и попросить пользователя произвести то или иное действие. С помощью UNIX он настроил запуск JumpStart[1] на узлах сети в тот момент, когда ни он, ни клиент этим узлом не поль-

[1] Команда Solaris `reboot--'flnet-installfl'` устраняет необходимость вручную запускать процесс из консоли. При необходимости эту команду можно запускать удаленно.

зовались. Таким образом Кристоф полностью изменил способ предоставления услуг пользователям. А это стало возможным только благодаря уверенности Кристофа, что установка завершится без ошибок.

3.2.2. Вовлечение пользователей в процесс стандартизации

Если пользователи будут иметь дело со стандартной конфигурацией, вам необходимо вовлечь их в процесс составления спецификаций и разработки[1]. В идеале пользователи должны принимать участие в процессе разработки с самого начала. Назначенные представители или заинтересованные руководители могли бы выбирать приложения, которые будут включены в конфигурацию. Для каждого приложения составляется соглашение об уровне обслуживания, в котором описывается уровень обслуживания со стороны системных администраторов. Новые версии ОС и приложений отслеживаются и одобряются. Контролируемое внедрение новых версий аналогично описанному автоматизированному процессу обновления.

Однако в реальности платформы контролируются либо руководством (с мучительной точностью), либо отделом системного администрирования, отвечающим за предоставление основной платформы, которую пользователи могут настраивать под себя. В первом случае примером может служить офис приема заказов по телефону, где операторы работают со строго определенным набором приложений. Системные администраторы совместно с руководством определяют, какие именно приложения будут установлены, когда именно будет проведено обновление и т. д.

Вторые случаи более распространенны. В одной сети стандартной платформой для персонального компьютера считается его операционная система; самые необходимые приложения; приложения, требуемые компанией-учредителем; утилиты, которые наиболее часто просят установить пользователи и которые можно лицензировать оптом. Такая среда является очень открытой. Формальные заседания комитета не проводятся. Однако системные администраторы достаточно тесно общаются со многими пользователями и, таким образом, прекрасно представляют себе потребности последних.

Для некоторых приложений предусмотрены более формальные процессы. Например, определенной группе разработчиков требуется тот или иной инструментарий. Для разработки любого ПО предусмотрен набор инструментальных средств, который описывается, тестируется, одобряется и устанавливается. Системные администраторы должны принимать участие в этом процессе, чтобы соотносить ресурсы с планом развертывания.

3.2.3. Разнообразие стандартных конфигураций

Наличие нескольких стандартных конфигураций может быть прекрасно или ужасно, и именно системный администратор определяет, какой эпитет лучше

[1] Хотя для системных администраторов стандартизация имеет массу преимуществ, многие пользователи считают ее помехой, которую необходимо либо терпеть, либо каким-то образом обходить.

применим в его случае[1]. Чем больше стандартных конфигураций используется в корпоративной сети, тем труднее все их обслуживать. Один из способов создать большое количество разнообразных конфигураций – использовать для всех конфигураций один и тот же сервер и механизмы, вместо того чтобы выделить отдельный сервер для каждого стандарта. Однако, если потратить время и создать единую обобщенную систему, способную производить множественные конфигурации и поддаваться масштабированию, вы придете к настоящему успеху.

Общее понятие управляемых стандартизированных конфигураций часто носит название «управление конфигурацией программного обеспечения» (Software Configuration Management, SCM). Этот процесс относится как к серверам, так и настольным компьютерам.

Серверам посвящена следующая глава, а сейчас достаточно лишь отметить, что для установки серверов можно разработать особые конфигурации. Хотя серверы запускают совершенно особые приложения, для них существует некая базовая установка, которую можно впоследствии настроить. Если для повышения пропускной способности развертываются резервные веб-серверы, наличие полностью автоматизированной системы установки может оказаться очень полезным. Например, у многих интернет-сайтов есть резервные веб-серверы, отвечающие за статические страницы, динамические CGI-страницы (Common Gateway Interface) и другие службы. Если эти различные конфигурации выводятся с помощью автоматизированного механизма, развертывание дополнительной пропускной способности в любой области значительно упрощается.

Стандартные конфигурации также могут облегчить процесс обновления ОС. Если у вас есть возможность полностью очистить диск и заново все переустановить, обновление ОС становится простейшей задачей. Для этого потребуется приложить значительные усилия в таких областях, как разделение пользовательских данных и обработка системных данных определенных узлов.

3.3. Заключение

В этой главе мы рассмотрели процессы, связанные с обслуживанием операционных систем на настольных компьютерах. Настольные компьютеры, в отличие от серверов, как правило, развертываются в больших количествах, и все они обладают практически одной и той же конфигурацией. У каждого компьютера есть свой жизненный цикл, который начинается с установки ОС и заканчивается в тот момент, когда машину выключают в самый последний раз. В этот период программное обеспечение компьютера постепенно приходит в негодность в результате энтропии, обновляется и заново переустанавливается в начале нового цикла. В идеале все узлы сети, относящиеся к определенной платформе, в начале своего жизненного цикла должны иметь одну и ту же конфигурацию. Обновляться они должны параллельно. Некоторые стадии жизненного цикла важнее для пользователей, чем другие. Мы стремимся увеличить продолжительность более важных стадий и сократить продолжительность менее значительных.

---

[1] Кто-то в Интернете заметил, что «самое лучшее в стандартах – это их огромное количество: есть из чего выбрать».

Основу всего, чему посвящена данная глава, составляют три процесса:

1. Первичная установка ОС должна быть автоматизирована.
2. Обновление программного обеспечения должно быть автоматизировано.
3. Конфигурация сети должна администрироваться централизованно с помощью такой системы, как DHCP.

Эти три задачи имеют критическое значение для экономного управления. Грамотное их выполнение позволит всем последующим процессам проходить более гладко.

Задания

1. Что считается *платформой* в соответствии с определением из раздела 3.1? Перечислите все платформы, используемые в вашей сети. Сгруппируйте их, выделив платформы, которые можно считать одинаковыми с точки зрения технической поддержки. Объясните, почему вы сделали именно такой выбор.
2. История из раздела 3.1.2 описывает компанию, которая постоянно тратит деньги на ручную установку программного обеспечения, вместо того чтобы один раз вложить деньги в создание системы автоматизации. Возможно, вам сложно понять, как эта компания может быть настолько глупой. Проанализируйте сеть своей компании или компании, в которой вы недавно побывали, и приведите не менее трех примеров, в которых подобные вложения не были сделаны. Для каждого примера перечислите причины отказа от вложений. О чем говорят ваши ответы?
3. В своем сетевом окружении определите тип узла или операционной системы, который не является привилегированным объектом, как описано в примере в разделе 3.1. Каким образом вы могли бы присвоить узлу или ОС статус привилегированного объекта, если бы в этом возникла необходимость? Каким образом платформы в вашей сети могут получить статус привилегированного объекта?
4. В одном из примеров Том был наставником нового системного администратора, который занимался установкой Solaris JumpStart. Скрипт, который было необходимо запускать после завершения установки, просто копировал определенные файлы. Каким образом можно избавиться от этого скрипта (независимо от того, запускается он вручную или автоматически)?
5. DHCP предполагает управление сетью на основе IP-адресов. Эта книга во многом посвящена работе с IP-адресами. Что вы будете делать в сетевом окружении Novell с помощью стека протоколов IPX/SPX? OSI-net (X.25 PAD)? DECnet?

Глава 4

Серверы

Эта глава посвящена серверам. В отличие от рабочих станций, предназначенных для одного пользователя, от сервера зависит множество пользователей. Следовательно, главным приоритетом для них становится надежность и бесперебойная работа. Прилагая усилия для повышения надежности сервера, мы ищем возможности, которые позволят сократить время восстановления, предоставить лучшее рабочее окружение и уделять особое внимание процессу конфигурирования.

К серверу могут подключаться сотни, тысячи или даже миллионы пользователей. Все усилия по повышению производительности или надежности наталкиваются на барьер огромного количества пользователей. Серверы рассчитываются на более продолжительное времени работы, чем рабочие станции, что также подразумевает дополнительные расходы. Покупка сервера с избыточной мощностью становится вложением в продление его срока жизни.

4.1. Основы

Оборудование, продаваемое как сервер, качественно отличается от оборудования, приобретаемого для индивидуальной рабочей станции. У серверного оборудования другие возможности, а при его разработке учитывается другая экономическая модель. При установке и поддержке серверов используются особые процедуры. Как правило, серверы поставляются с контрактом на обслуживание, системами резервного копирования, операционной системой и возможностью удаленного доступа. Кроме того, серверы размещают в вычислительных центрах с контролируемым микроклиматом и с ограниченным доступом к серверному оборудованию. Понимание этих различий поможет вам в принятии верного решения при закупке.

4.1.1. Покупайте для серверов серверное оборудование

Системы, продаваемые как серверы, отличаются от систем, предназначенных для использования в качестве клиентов или настольных рабочих станций. Часто предпринимаются попытки сэкономить за счет покупки настольного компьютера и установки на него серверного программного обеспечения. Такое решение может помочь на короткий срок, но это не лучший выбор для долгосрочных или крупных проектов, которые должны быть надежнее карточного домика. Сервер-

ное оборудование обычно стоит дороже, но дополнительные возможности оправдывают вложения. Вот некоторые из этих возможностей:

- *Расширяемость.* Как правило, в серверах больше физического пространства для жестких дисков и больше слотов для карт расширения и центральных процессоров либо они оснащены разъемами с высокой пропускной способностью для подключения специализированных периферийных устройств. Обычно поставщики предоставляют дополнительные конфигурации оборудования и программного обеспечения для кластеризации, распределения нагрузки, автоматизации переключения на резервные мощности при отказе оборудования и других подобных возможностей.
- *Бóльшая производительность центральных процессоров.* Серверы часто оборудованы несколькими ЦП, а также обладают дополнительными возможностями оборудования, такими как упреждающая выборка данных, многоступенчатая проверка процессоров и динамическое распределение ресурсов между ЦП. Процессоры различаются частотами, на которых работают; их цена находится в прямой зависимости от частоты. Цена на наиболее скоростные ЦП обычно бывает непропорционально завышена – это плата за передовые технологии. Такие дополнительные расходы могут быть оправданы на сервере, который поддерживает множество пользователей. Так как серверы подразумевают длительный срок службы, зачастую имеет смысл приобретать более скоростные ЦП, которые дольше не будут устаревать. Заметим, что скорость процессора на серверах не всегда определяет эффективность, потому что скорость работы многих приложений зависит от скорости обмена информацией (ввода-вывода), а не от частоты ЦП.
- *Высокопроизводительные системы обмена информацией (ввода-вывода).* Серверы, как правило, более производительны в плане обмена информацией (ввода-вывода), чем клиенты. Возможности ввода-вывода часто пропорциональны количеству пользователей, что оправдывает применение скоростных подсистем ввода-вывода. Это может означать использование жестких дисков с интерфейсами SCSI или FC-AL вместо IDE, высокоскоростных внутренних шин или сетевых интерфейсов, на порядок более скоростных, чем у пользователей.
- *Возможности модернизации.* Серверы чаще модернизируют, а не просто заменяют, они предназначены для растущих потребностей. На серверах, как правило, имеется возможность добавлять процессоры или заменять отдельные процессоры на более быстрые, не требующая дополнительных аппаратных изменений. Как правило, серверные процессоры размещаются на отдельных разъемах в шасси или находятся в съемных разъемах на системной плате на случай замены.
- *Возможность монтирования в стойку.* Серверы должны иметь возможность установки в стойки. В главе 6 мы обсудим преимущества монтирования серверов в стойки по сравнению с укладкой их в штабель. Хотя серверы, не предназначенные для стоек, и можно поставить на полки в стойках, это бесполезная трата пространства и просто неудобно. Если настольный компьютер может размещаться в пластмассовом корпусе обтекаемой формы, сервер должен иметь прямоугольную форму для эффективного использования пространства в стойке. Все крышки, которые требуется снимать при ремонте, должны сниматься без необходимости извлечения сервера из стойки. Еще важнее то, что сервер должен быть сконструирован с учетом охлаждения и вентиляции при монтировании в стойку. Система, у которой

вентиляционные отверстия расположены только с одной стороны, не сможет поддерживать свою температуру в стойке так же хорошо, как система со сквозной вентиляцией от передней панели к задней. Слова «*сервер*» в названии компьютера недостаточно. Вам нужно будет позаботиться о том, чтобы он соответствовал выделенному для него месту. Разъемы должны выбираться с учетом размещения в стойках, например для подключения последовательных консолей стоит использовать стандартный патч-кабель категории 5 вместо разъемов db-9 с винтами.

- *Не требуется доступ с боковых сторон.* Компьютер должно быть проще ремонтировать и обслуживать, если он установлен в стойку. Выполнение этих задач не должно требовать доступа к боковым стенкам машины. Все кабели должны быть сзади, а все отсеки приводов и дисков – спереди. Мы видели отсеки для CD-приводов, расположенные сбоку, а это свидетельствует о том, что при конструировании возможность установки в стойку не учитывалась. Некоторые системы, часто это сетевое оборудование, требуют доступа только с одной стороны. Это означает, что устройство может быть расположено «впритирку» в тесном шкафу и по-прежнему быть пригодным для обслуживания. Некоторые серверы можно установить в стандартную стойку, только сняв полностью или частично внешний пластиковый корпус. Обязательно убедитесь, что это не помешает охлаждению или работе сервера. Выключатели питания должны быть доступны, но не слишком, чтобы избежать случайного нажатия.
- *Дополнения для повышенной надежности.* Многие серверы обладают дополнительными возможностями, повышающими надежность, такими как дублированные источники питания, RAID, несколько сетевых карт и компоненты с поддержкой «горячей» замены.
- *Контракт на обслуживание.* Поставщики предоставляют контракты на обслуживание оборудования, где, как правило, оговариваются и гарантийные сроки замены запасных частей.
- *Альтернативные варианты управления.* В идеале серверы должны иметь поддержку функций удаленного управления, таких как доступ через последовательный порт, который может быть использован для диагностики и решения проблем, чтобы восстановить сбойную машину. Некоторые серверы также поставляются со встроенными датчиками температуры и другими аппаратными средствами мониторинга, которые могут генерировать оповещения при обнаружении проблем.

Поставщики постоянно совершенствуют конструкцию серверов для удовлетворения потребностей бизнеса. В частности, влияние рынка заставляет поставщиков улучшать серверы, чтобы было возможно размещать больше единиц в **колокейшн-центрах** – арендуемых вычислительных центрах, где оплата идет за единицу площади. Возможности дистанционного управления для серверов в колокейшн-центрах могут означать разницу между минутами и часами простоя.

4.1.2. Выбирайте поставщиков, известных надежностью продукции

Очень важно выбирать поставщиков, продукция которых известна своей надежностью. Некоторые поставщики экономят за счет использования компонентов потребительского класса, другие используют компоненты, которые соот-

ветствуют требованиям военного стандарта MIL-SPEC[1]. Некоторые поставщики имеют многолетний опыт разработки серверов. Более опытные поставщики обеспечивают функции, перечисленные выше, а также другие дополнительные возможности, востребованность которых можно выяснить, только имея многолетний опыт на рынке. Неопытные или малоопытные поставщики не могут обеспечить какого-либо технического обслуживания, помимо замены вышедших из строя узлов.

Может быть, полезно узнать у других системных администраторов, с какими поставщиками они работают, а каких стараются избегать. Можно порекомендовать для общения два ресурса сообщества системных администраторов: SAGE (System Administrators' Guild, Гильдия системных администраторов, *www.sage.org*) и LOPSA (League of Professional System Administrators, Лига профессиональных системных администраторов, *www.lopsa.org*).

Оборудование может быть однотипным (все от одного поставщика и/или из одной линейки продукции) или разнотипное (от разных поставщиков и/или из разных линеек продукции). Однотипное оборудование проще обслуживать, так как требуется меньше времени на подготовку; обслуживание и ремонт упрощаются за счет одного набора запасных частей, а также легче найти виновных в случае возникновения проблем. Однако разнотипное оборудование тоже имеет свое преимущество – оно заключается в том, что вы не зависите от одного поставщика, а конкуренция между поставщиками обернется для вас лучшим обслуживанием. Этот момент дополнительно обсуждается в главе 5.

4.1.3. Реальные расходы на серверное оборудование

Чтобы иметь представление о дополнительных расходах на серверы, вы должны знать, из чего складывается цена компьютера.

У большинства поставщиков есть три[2] серии продукции: для дома, для бизнеса и серверное оборудование. Домашняя серия обычно продается по наименьшей начальной цене, так как клиенты чаще всего принимают решение о покупке на основании рекламируемой цены. Дополнения и возможность расширения в будущем доступны по более высокой цене. При описании компонентов используются общие технические характеристики, такие как разрешение экрана, вместо указания конкретного производителя и модели видеокарты. Дело в том, что ради поддержания минимальной покупной цены поставщики вынуждены ежедневно или еженедельно менять компоненты от разных производителей. Эти машины обычно имеют аппаратные дополнения для игр, такие как джойстики, высокопроизводительные графические ускорители и модные аудиосистемы.

---

[1] MIL-SPEC – военные спецификации США для электронных компонентов и оборудования – определяют уровень качества для получения наилучших результатов. Как правило, но не всегда, стандарт MIL-SPEC требует более высокого качества, чем гражданские стандарты. Эти требовательные спецификации обычно приводят к значительному увеличению затрат.

[2] Иногда больше, иногда меньше. Поставщики часто предлагают специализированные серии оборудования для вертикальных рынков, например для нужд высококачественной графики, интенсивных вычислений и т. д. На специализированных потребительских рынках, таких как рынок многопользовательских игр в реальном времени или домашних мультимедийных центров, граница между оборудованием потребительского и серверного уровня все больше размывается.

Настольные компьютеры для бизнеса обычно разрабатываются с учетом общих затрат в течение всего срока их службы. Начальная закупочная цена выше, чем для домашних компьютеров, но серия для бизнеса должна дольше не устаревать. Компаниям невыгодно содержать большое количество запасных компонентов, не говоря уже о стоимости обучения техников по ремонту для каждой модели. Поэтому в бизнес-сериях редко используют новейшие компоненты, такие как видеокарты и контроллеры жестких дисков. Некоторые поставщики предлагают программы, гарантирующие, что используемая видеокарта будет выпускаться еще по меньшей мере в течение полугода и за 3 месяца до прекращения выпуска поступит извещение, а запасные части для них будут доступны еще в течение года после извещения. Такие специальные меры упрощают тестирование приложений на новых конфигурациях оборудования и инвентаризацию запасных частей. Оборудование бизнес-класса часто арендуется, а не приобретается, и для таких сетей эти гарантии имеют большую ценность.

Серверные серии обычно ориентированы на наилучшее соотношение себестоимости и производительности. Например, файловый сервер может конструироваться с расчетом на минимальную стоимость производительности по тесту SPEC SFS973[1] в пересчете на закупочную цену каждой машины. Подобные тесты существуют для веб-трафика, оперативной обработки транзакций (OLTP), совокупной производительности многопроцессорных систем и т. д. Многие описанные выше возможности серверов увеличивают закупочную цену машины, но при этом повышают предполагаемое время бесперебойной работы, что делает соотношение цены и производительности более привлекательным.

Серверы стоят дороже и по другим причинам. Корпус, который удобнее для обслуживания, может быть дороже в производстве. Существуют ограничения на расположение отсеков для дисководов и других панелей, доступ к которым должен быть только с определенной стороны, – это подразумевает, что их нельзя разместить так, чтобы удешевить конструкцию. Тем не менее более высокая начальная закупочная цена оправдана экономией средств в долгосрочной перспективе за счет сокращения времени на ремонт (MTTR) и упрощения обслуживания.

Неверно считать, что серверы дороже настольных компьютеров, так как это сравнение объектов разного рода. Понимание этого различия моделей ценообразования помогает в обсуждении, когда требуется обосновать кажущуюся дороговизну серверного оборудования. Часто приходится слышать, как люди выражают недовольство ценой сервера в 50 000 долларов, тогда как высокопроизводительный персональный компьютер можно приобрести за 5000 долларов. Когда сервер в состоянии обслуживать миллионы транзакций в день или распределять мощность процессора между десятками пользователей, эти расходы оправданы. Кроме того, простой сервера обходится значительно дороже простоя настольного компьютера. Дополнительное оборудование и компоненты с возможностью «горячей» замены на сервере легко окупаются за счет минимизации остановок в работе.

Более весомый аргумент против решения о приобретении дорогого сервера – то, что его производительность выше, чем это требуется для службы. Производительность часто пропорциональна затратам, и слишком расточительно тратить деньги на излишнюю производительность. Тем не менее покупка сервера

[1] Бывший LADDIS (*http://www.spec.org/osg/sfs93/*).

«с запасом» может отсрочить сложную модернизацию для увеличения производительности в будущем, а это тоже имеет ценность. Пользу прогнозирования потребностей в модернизации и тенденций использования мы обсудим в главе 22.

4.1.4. Контракты на обслуживание и запасные компоненты

При покупке сервера продумайте, как будет происходить ремонт. Все машины рано или поздно ломаются[1]. Поставщики все чаще предлагают самые разные дополнительные контракты на обслуживание. Например, в одной из форм контракта на обслуживание предоставляется выбор срока обслуживания заявки в течение 4 ч, в течение 12 ч или на следующий день. Среди других вариантов – предоставление клиенту возможности приобрести комплект запасных компонентов и пополнять его по мере необходимости.

Вот несколько разумных сценариев, которые помогут вам при выборе подходящего контракта на обслуживание:

- *Не критически важный сервер.* Некоторые серверы не имеют критической важности, например один процессор из многопроцессорного сервера. В этой ситуации контракт со сроком обслуживания заявки на следующий день или в течение двух дней будет приемлемым вариантом. Или контракт на обслуживание может вообще не потребоваться, если стандартного гарантийного обслуживания будет достаточно.
- *Большая группа идентичных серверов.* Иногда в сетях используется большое количество машин одного типа, возможно, предназначенных для различных служб. В этом случае имеет смысл приобрести комплект запасных компонентов, так как ремонт можно будет производить силами своих сотрудников. Стоимость комплекта запасных частей разделяется на большое количество узлов. Для этих узлов может потребоваться только недорогой контракт на обслуживание, предусматривающий лишь замену компонентов из комплекта запасных частей.
- *Постепенная модернизация.* Со временем технологии развиваются, и для сетей, описанных в предыдущем пункте, в конце концов появляется потребность в замене устаревших моделей на новые, для которых может не быть необходимых запасных компонентов. В этом случае вы можете стандартизировать срок обеспечения запасными компонентами отдельной модели или группы моделей, которые используют одинаковый комплект. По окончании этого периода вы можете утвердить новую модель и приобрести соответствующий комплект запасных компонентов. В любой момент времени вам понадобится, например, всего два запасных комплекта. Чтобы внедрить третью модель, вам следует сначала списать все узлы, зависящие от

[1] Настольные рабочие станции тоже ломаются, но мы решили рассказать о контрактах на обслуживание в этой главе, а не в главе 3. Как показывает наш опыт, ремонт настольных компьютеров – менее срочное дело, чем ремонт сервера. Настольные компьютеры более универсальны и, следовательно, более взаимозаменяемы. Из-за этих факторов имеет смысл не заключать контракт на обслуживание, а иметь свои комплекты запасных частей и нанять техника, который сможет делать ремонт, либо заключить контракт с местной ремонтной мастерской.

комплектов запасных частей, которые вышли из обращения. Это помогает управлять расходами.

- *Важные узлы.* Иногда слишком дорого содержать полностью укомплектованный набор запасных частей. Может быть разумным хранить запас только тех компонентов, которые чаще всего выходят из строя, а на остальные приобрести контракт на обслуживание в тот же день. Жесткие диски и источники питания чаще всего выходят из строя и являются взаимозаменяемыми для широкого спектра продукции.
- *Большое количество моделей от одного поставщика.* Особо крупные компании могут заключить контракт на обслуживание, в условия которого входит выделение техника для работы в сети компании-заказчика. Такая возможность оправданна, только когда в сети огромное количество серверов или если в доходах этой компании важную роль играют серверы определенного поставщика. Тем не менее порой и компании среднего размера могут договориться о создании у них склада запасных комплектов, благодаря чему техник всегда будет находиться рядом. Иногда можно договориться с техником о прямом доступе к комплектам запасных частей в случае аварийных ситуаций (обычно это делается без ведома руководства техника). Системный администратор будет уверен, что техник посвящает все свое свободное время вашей сети, если предоставить ему место в офисе и телефон. В обмен на это иногда можно договориться о скидках на выплаты по контракту на обслуживание. В одной сети с такой договоренностью техник, который не был ничем занят, помогал системным администраторам распаковывать и устанавливать новое оборудование.
- *Критически важный узел.* Некоторые поставщики предлагают контракты на обслуживание, предусматривающие выделение техника для работы в сети компании-заказчика и дублирующей машины, готовой к замене сбойного устройства. Это зачастую так же дорого, как и оплата резервного сервера, но может иметь смысл для некоторых компаний, для которых высокие технологии – не основная специализация.

Нужно искать компромисс между хранением запасных частей и сервисным контрактом. Комплектование собственного склада запасных компонентов может быть слишком дорогостоящим для небольшой сети. Контракт на обслуживание включает диагностические услуги, хотя бы по телефону. Иногда, с другой стороны, самый простой способ диагностики – менять запасные части до тех пор, пока проблема не исчезнет. Трудно поддерживать уровень подготовки сотрудников по всем диагностическим и ремонтным методикам для всех используемых моделей, в особенности для нетехнических компаний, которые не могут отвлекать ресурсы на непрофильную деятельность. Аутсорсинг в этой сфере рассматривается в разделах 21.2.2 и 30.1.8.

Иногда системный администратор обнаруживает, что на критически важный узел сети не оформлен контракт на обслуживание. Это открытие, как правило, происходит в критический момент, например когда потребовался ремонт. Решить эту проблему обычно можно, обратившись к продавцу с просьбой отремонтировать машину и добавить ее в контракт той же датой или задним числом. Хорошей политикой будет оформлять на 10% больше сервисных позиций, чем предусматривает цена контракта, с тем чтобы поставщик мог поднимать ежемесячные платежи по мере добавления новых машин в контракт.

Также полезно пересматривать контракт по крайней мере ежегодно или даже ежеквартально, чтобы добавить новые серверы и исключить списанные. Страта

как-то раз помогла клиенту в несколько раз снизить расходы на ее консалтинговые услуги путем пересмотра устаревшего на несколько лет сервисного контракта с поставщиком.

Есть три простых способа предотвратить забывание включения оборудования в контракт. Первый способ заключается в том, чтобы создать хорошую систему инвентаризации и использовать ее для перекрестного пересмотра контракта. Однако хорошую систему инвентаризации трудно найти, и даже лучшие из них могут пропустить несколько узлов.

Второй способ заключается в том, чтобы человек, ответственный за закупки, также отвечал за добавление новых машин в контракт. Этот человек должен знать, к кому обращаться для определения соответствующего уровня обслуживания. Если нет единого отдела закупок, можно попробовать найти какую-то другую процедуру добавления новых узлов в контракт.

Третий способ – решить общие проблемы, связанные с гарантией. Большинство компьютеров обеспечены бесплатным сервисом в первые 12 месяцев по гарантии, и их не нужно включать в контракт на обслуживание в течение этих месяцев. Тем не менее трудно не забыть добавить компьютеры в контракт так много месяцев спустя, к тому же в течение гарантийного срока обеспечивается другой уровень обслуживания. Чтобы решить эту проблему, системному администратору нужно выяснить, может ли поставщик включить машины в контракт сразу, но не брать плату за обслуживание в течение первых 12 месяцев. Большинство поставщиков пойдут на это, поскольку им это будет выгодно. В последнее время большинство поставщиков продают контракты на обслуживание одновременно с продажей оборудования.

Контракты на обслуживание, скорее, борются с последствиями, а не предотвращают проблемы (решения, предотвращающие проблемы, мы рассмотрим в следующей главе). Контракты на обслуживание предусматривают поставку запасных компонентов и своевременный ремонт. Как правило, существует выбор из нескольких типов контрактов. По условиям дешевых контрактов доставка запасных компонентов ложится на плечи заказчика, а более дорогие предусматривают доставку запчастей и их установку.

Налаженный обмен новых компонентов на старые – важная часть оперативного ремонта, и в идеале она должна быть предусмотрена в контракте на обслуживание. Когда возникают проблемы с серверным оборудованием и нужны запасные части, некоторые поставщики требуют возврата старых неисправных компонентов. Это имеет смысл, если замена осуществляется бесплатно в соответствии с контрактом на обслуживание. Возвращаемые компоненты имеют ценность, они могут быть отремонтированы и возвращены другому клиенту, которому потребуются запчасти. Помимо того, клиент может просто запрашивать компоненты один за другим, возможно, продавая их кому-то.

Поставщики, как правило, требуют уведомления и разрешения для возврата неисправных компонентов. Это разрешение называется разрешением на возврат товара (Returned Merchandise Authorization, RMA). Поставщик обычно предоставляет клиенту номер RMA для пометки и отслеживания возвращенных компонентов.

Некоторые поставщики не поставляют компоненты на замену, пока не получат неисправный компонент. Из-за этого время на восстановление может вырасти в два раза и более. Лучшие поставщики отправляют замену немедленно и ожидают возврата неисправного компонента в течение определенного срока. Это называется **перекрестной доставкой** – теоретически компоненты должны доставляться в обе стороны одновременно.

Поставщики обычно требуют номер заказа на закупку или запрашивают номер кредитной карты для обеспечения оплаты в случае, если они не получат компоненты, подлежащие возврату. Это логичный способ защитить себя. Иногда наличие контракта на обслуживание снижает потребность в этом.

Старайтесь не иметь дело с поставщиками, которые продают серверы, но не предоставляют перекрестную доставку ни на каких условиях. Такие поставщики недостаточно серьезно относятся к понятию *«сервер»*. Вы будете удивлены, узнав, сколько крупных поставщиков работают на таких условиях.

Еще больше сократить время на ремонт можно, приобретя **комплект запасных компонентов**, снимающий зависимость от поставщика при срочном ремонте сервера. В комплект должно входить по одному экземпляру каждого компонента системы. Как правило, этот комплект обойдется дешевле, чем покупка дублирующей системы, так как, например, если в системе используется четыре центральных процессора, в запасном комплекте достаточно одного. Также комплект менее дорог за счет того, что ему не требуются лицензии на программное обеспечение. Но даже если у вас есть ремонтный комплект, вам следует заключить контракт на обслуживание, по которому вы сможете дополучить любые компоненты, использованные для ремонта неисправной машины. Приобретайте по одному комплекту запасных компонентов для каждой модели, требующей срочного ремонта.

Большое количество комплектов запасных частей может обойтись чрезвычайно дорого, особенно если для них требуются дополнительные расходы на контракт на обслуживание. Поставщик может предоставить дополнительные возможности, такие как контракт на обслуживание, гарантирующий доставку запасных компонентов в течение нескольких часов, что может снизить общую сумму ваших затрат.

4.1.5. Обеспечение целостности данных

На серверах хранятся критически важные данные и уникальные конфигурации, которые должны быть защищены.

Клиентские рабочие станции, как правило, серийные и с однотипными конфигурациями, а их данные обычно хранятся на серверах, что снимает необходимость в резервном копировании. Если откажет диск рабочей станции, ее конфигурация должна быть идентичной многочисленным аналогичным машинам и немодифицированной по отношению к исходному состоянию, а следовательно, она может быть восстановлена с помощью автоматизированной процедуры установки. Это в теории. Однако люди всегда сохраняют какие-то данные на своих локальных машинах, локально устанавливаются программы, а операционная система сохраняет локально некоторые конфигурационные данные. На Windows-платформах избежать этого невозможно. Переносимые профили сохраняют пользовательские настройки на сервере при каждом выходе из системы, но не защищают локально установленное программное обеспечение и настройки реестра машины.

UNIX-системы в меньшей степени подвержены этому, так как в грамотно сконфигурированной системе без предоставления пользователю доступа с правами `root` на локальном диске защищено от записи все, кроме нескольких специфических файлов. Например, файлы crontab (назначенные задания) и другие, сохраненные в каталоге /var, по-прежнему можно будет модифицировать ло-

кально. Как правило, достаточно простой системы, каждый вечер делающей резервные копии этих нескольких файлов.

Подробно резервное копирование будет рассмотрено в главе 26.

4.1.6. Размещение серверов в вычислительном центре

Серверы должны устанавливаться в условиях с надежными энергоснабжением, противопожарной защитой, сетью, охлаждением и физической безопасностью (глава 5). Лучше всего зарезервировать физическое место для размещения сервера при его приобретении. Если пометить места в соответствующих стойках распечатанными метками, это предотвратит повторное резервирование места. Для разметки мест энергоснабжения и охлаждения потребуется сверяться по списку или таблице.

После сборки оборудование лучше устанавливать в стойку непосредственно перед установкой ОС и другого программного обеспечения. Мы наблюдали следующее явление: новый сервер собирается в чьем-то офисе и на него загружаются ОС и приложения. После установки приложений некоторые пользователи для пробы подключаются к службе. Вскоре сервер уже сильно нагружен, хотя и не готов к использованию, и он по-прежнему находится в чьем-то офисе без надлежащей защиты машинного зала, например без UPS и кондиционирования воздуха. Теперь люди, использующие сервер, будут обеспокоены его отключением перед перемещением в машинный зал. Способ предотвращения этой ситуации заключается в том, чтобы установить сервер в его конечном местоположении, как только он будет собран[1].

Филиалы и даже некоторые компании не всегда достаточно крупны, чтобы иметь вычислительные центры. Тем не менее у всех должна быть выделена комната или шкаф, обеспечивающие как минимум физическую безопасность, источник бесперебойного питания (несколько мелких или один большой) и достаточное охлаждение. Лучше приобрести шкаф для телекоммуникационной аппаратуры с хорошим охлаждением и закрывающейся на замок дверцей, чем делать расчет заработной платы на сервере, стоящем у кого-то под столом. Можно выбрать недорогую систему охлаждения – некоторые из них не нуждаются в отводе и повторном испарении собранной воды и выбросе ее через вентиляционные отверстия.

4.1.7. Конфигурация клиент–серверной ОС

Серверы необязательно должны работать под управлением тех же ОС, что и их клиенты. Серверы могут быть совершенно другими, в точности такими же, или с той же базовой ОС, но с другой конфигурацией для иного предназначения. Для разных случаев подходят различные варианты.

Например, веб-серверу не нужно работать под управлением той же ОС, что и у клиентских машин. Клиенты и сервер должны лишь использовать одинаковый протокол. На однофункциональных сетевых специализированных устройствах часто бывает установлена мини-ОС с программным обеспечением, минимально достаточным для выполнения единственной функции (файл-сервер, веб-сервер, почтовый сервер).

---

[1] Кроме того, в таких ситуациях обычно теряются детали для крепления сервера в стойке, что вызывает еще большие задержки, либо выясняется, что кабель питания или сетевой кабель не дотягивается до нужного места.

Иногда на серверах требуется устанавливать все те же программы, что и на клиентах. Рассмотрим случай UNIX-сети с множеством настольных компьютеров под управлением UNIX и несколькими многопроцессорными UNIX-серверами общего назначения. На клиентах должна устанавливаться одинаковая клонированная ОС, как описано в главе 3. На многопроцессорные серверы следует установить ту же ОС, хотя она может быть иначе настроена для большего количества процессов, псевдотерминалов, буферов и других параметров.

Еще один интересный момент, характерный для серверной ОС, – ориентированность на перспективу. При установке Solaris 2.x вы можете отметить, что этот узел сети – сервер, на котором установлены все программные пакеты, потому что бездисковые клиенты или машины с малым объемом жестких дисков могут использовать NFS для загрузки необходимых пакетов с сервера. С другой стороны, серверная конфигурация при установке Red Hat Linux – это минимальный набор пакетов, предполагающий, что вам нужна только базовая установка, поверх которой вы установите специализированные программные пакеты, необходимые для создания служб. В связи с ростом объема жестких дисков последний подход стал более распространенным.

4.1.8. Обеспечьте удаленный доступ через консоль

Для серверов необходима возможность удаленного обслуживания. В прошлом для каждого сервера в машинном зале была предусмотрена собственная консоль: клавиатура, видеомонитор или консольный вывод на печать и, возможно, мышь. По мере того как системные администраторы устанавливали все новое оборудование в машинном зале, отказ от этих консолей позволил освободить значительное пространство.

Переключатель KBM – устройство, позволяющее нескольким машинам использовать одну клавиатуру, видеоэкран и мышь (KBM). Например, можно установить три сервера и три консоли в одну телекоммуникационную стойку. Однако благодаря коммутатору KBM для этой стойки достаточно только одной клавиатуры, монитора и мыши. Таким образом, в ту же стойку можно установить большее количество серверов. Можно сэкономить еще больше места, если установить один коммутатор KBM на ряд стоек или на весь вычислительный центр. Однако более крупные коммутаторы KBM, как правило, чрезмерно дорогие. Можно освободить еще больше пространства с помощью IP-KBM, то есть KBM, в которых нет ни клавиатуры, ни монитора, ни мыши. Достаточно просто подключиться к консольному серверу KBM по сети с программного клиента на другой машине. Это можно сделать даже с ноутбука в кафе, если ноутбук подключен через VPN к вашей сети!

Предшественник переключателя KBM был предназначен для устройств с последовательным портом. Изначально у серверов не было видеокарт, но имелись последовательные порты, через которые можно было подключиться к терминалу[1]. Эти терминалы занимали очень много места в компьютерном

[1] Юные читатели могут думать, что *терминал VT-100* – это только программный пакет, который, интерпретирует ASCII-коды с целью отображения текста, или часть пакета *TELNET* либо *SSH*. Однако эти программные пакеты эмулируют реальные устройства, которые некогда стоили сотни долларов за штуку и являлись частью каждого крупного сервера. Более того, до появления персональных компьютеров у одного сервера могло быть несколько десятков таких терминалов, которые предоставляли единственный способ доступа к машине.

зале, в котором, как правило, устанавливался длинный стол с десятком или более терминалов, по одному для каждого сервера. Считалось большим технологическим прорывом, когда кто-нибудь додумывался приобрести небольшой сервер с десятком последовательных портов и подключить каждый порт к консоли сервера. Это позволяло зайти на консольный сервер, а затем подключиться к определенному последовательному порту. Теперь, если возникала необходимость что-либо сделать с консолью, не было никакой нужды идти в компьютерный зал.

В настоящее время последовательные консольные концентраторы бывают двух видов: самодельные и специализированные. Самодельное решение подразумевает следующее: вы берете машину с множеством последовательных портов и программное обеспечение (бесплатное, такое как ConServer[1], или коммерческий аналог) и сами создаете систему. Специализированное решение – готовая система от поставщика, которая обычно быстрее поддается настройке и оснащена программным обеспечением в виде прошивки или на твердотельном накопителе на флэш-памяти. Таким образом, вы избавлены от риска отказа жесткого диска.

Последовательные консоли и переключатели KVM дают следующее преимущество: они позволяют вам управлять системной консолью, если сеть не работает или если система в неисправном состоянии. Например, определенные операции можно выполнять только при перезагрузке системы. Среди них нажатие определенных клавиш для выхода в меню BIOS. Разумеется, для IP-KVM требуется работоспособная сеть между вами и консолью IP-KVM, но остальная сеть необязательно должна работать.

Некоторые поставщики предоставляют карты расширения, которые позволяют удаленно управлять машиной. Эта возможность зачастую является основным отличием между серверами и простыми машинами этих поставщиков. Продукция сторонних компаний также может предоставлять эту возможность.

Удаленные консольные системы также позволяют имитировать всякие забавные сочетания клавиш, которые выполняют определенные функции при вводе в консоль. Например, `CTRL-ALT-DEL` для платформы PC или `L1-A` для платформы Sun.

Так как последовательная консоль принимает одиночный поток данных ASCII, информацию достаточно просто записывать и хранить. Таким образом, можно просмотреть все, что происходило с последовательной консолью за несколько месяцев. Это может быть очень полезно, если необходимо найти сообщения об ошибке, переданные консоли.

Сетевые устройства, такие как маршрутизаторы и коммутаторы, оснащены только последовательными консолями. Таким образом, может быть полезно помимо системы KVM иметь доступ и к последовательной консоли.

Бывает интересно понаблюдать, что выводится на последовательный порт. Даже если никто не подключен к маршрутизатору Cisco, сообщения об ошибках и предупреждения отправляются на последовательный порт консоли. Иногда результат вас может удивить.

---

[1] *www.conserver.com*

Ведите мониторинг всех последовательных портов

Однажды Том обратил внимание на порт на одном из устройств. На порте не было ярлыка, и, судя по всему, он не использовался, однако был очень похож на последовательный порт. Устройство поступило от новой компании, и Том был одним из его первых бета-пользователей. Он подключил загадочный последовательный порт к своей консоли и время от времени проверял выводящиеся статусные сообщения. Прошло несколько месяцев, прежде чем с этим устройством начали возникать проблемы. Том заметил, что в момент возникновения проблемы в консоли появилось странное сообщение. Это была секретная система отладки от поставщика! Когда Том сообщил о проблеме поставщику, скопировав сообщение, полученное с последовательного порта, он получил следующий ответ: «Эй! Вы вообще не должны ничего подключать к этому порту!» Позднее компания признала, что это сообщение действительно помогло им исправить проблему.

При приобретении серверного оборудования вам следует обратить особое внимание на то, какой тип удаленного доступа к консоли будет доступен и для решения каких задач может потребоваться такой доступ. В аварийной ситуации нет смысла и времени ждать, пока системные администраторы доберутся до физических устройств, чтобы все исправить. В штатных ситуациях у системных администраторов должна быть возможность исправить небольшие неполадки из дома, в дороге и, оптимально, возможность выполнить любую задачу через удаленное подключение.

Однако у удаленного доступа есть очевидные ограничения из-за того, что отдельные задачи (включение и выключение питания, загрузка сменных носителей, замена неисправного оборудования) требуют присутствия человека возле машины. Дежурный оператор или доброволец, готовый помочь, может стать глазами и руками удаленного специалиста. Некоторые системы позволяют удаленно включать и выключать отдельные разъемы питания, что, в свою очередь, позволяет удаленно производить полную перезагрузку. Однако замена оборудования по-прежнему остается задачей для опытных профессионалов.

Удаленный доступ к консолям позволяет системным администраторам снизить затраты и улучшить факторы безопасности. Машинные залы оптимизированы для машин, а не для людей. В этих помещениях холодно, тесно, и они дороже, чем офисные помещения той же площади. Лучше установить в стойки дополнительные узлы, а не мониторы и клавиатуры. Заставлять машинные залы креслами неудобно и даже небезопасно.

Не стоит ожидать, что системные администраторы будут весь день проводить в машинном зале. Работа системных администраторов в машинном зале вредна и для зала, и для администраторов. Работа непосредственно в машинном зале редко соответствует требованиям эргономики для клавиатуры и мыши и требованиям условий труда, таким как уровень шума. Находиться в холодном машинном зале вредно для здоровья. Системным администраторам нужно создать условия, максимально улучшающие производительность труда, а это проще всего осуществить в офисах. В отличие от машинного зала, в офисе проще раз-

местить такое важное оборудование для системного администратора, как справочная литература, эргономичная клавиатура, телефоны, холодильники и стереосистемы.

Большое количество людей в машинном зале также негативно сказывается и на оборудовании. Присутствие людей в машинном зале повышает нагрузку на системы отепления, вентиляции и кондиционирования. Каждый человек выделяет около 600 БТЕ[1] тепла. Дополнительная энергия для охлаждения 600 БТЕ – это лишние расходы.

При использовании удаленной консоли придется продумать вопросы безопасности. Часто стратегии безопасности узла базируются на размещении консоли за запертыми дверями. Удаленный доступ разрушает эти стратегии. Следовательно, для консольных систем требуются продуманные системы аутентификации и конфиденциальности. Например, вы можете разрешить доступ к консольной системе только через шифрованный канал, такой как SSH, и внедрить аутентификацию на основе системы одноразовых паролей, например считывателей отпечатков пальцев.

При покупке сервера следует убедиться в наличии возможности удаленного консольного доступа. Если поставщик не удовлетворяет ваши потребности, стоит поискать оборудование где-то еще. Удаленный консольный доступ дополнительно обсуждается в разделе 6.1.10.

4.1.9. Зеркалирование загрузочных дисков

Загрузочный диск, или диск с операционной системой, как правило, труднее всего заменить в случае его повреждения. Поэтому необходимо соблюдать особые меры безопасности, чтобы ускорить процесс восстановления. Для загрузочного диска каждого сервера необходимо создать зеркальный диск. Это означает, что установлено два диска и при любом обновлении основного диска тут же обновляется и второй. Если один из дисков откажет, система автоматически переключится на работоспособный диск. Большинство операционных систем позволяют сделать это программно, а многие контроллеры жестких дисков делают это на аппаратном уровне. Этот метод называется RAID 1. Более подробно он описан в главе 25.

С годами стоимость жестких дисков значительно снизилась, и эта некогда слишком дорогая возможность стала более доступной. В идеале все диски должны быть зеркалированы, или защищены RAID-схемой. Однако, если вы не можете себе этого позволить, создайте зеркало хотя бы для загрузочного диска.

Зеркалирование предполагает определенные компромиссы в отношении производительности. Операции чтения производятся быстрее, так как чтение идет параллельно с двух дисков. На вас работают два шпинделя, давая существенную выгоду производительности на занятом сервере. Процесс записи несколько замедлен, так как необходимо записать в два раза больше данных (хотя, как правило, запись идет параллельно). Системы с кэшированием при записи, такие как UNIX, менее подвержены этой проблеме. Так как диск с операционной

[1] Британская тепловая единица (British Thermal Unit, BTU) – количество тепла, необходимое для повышения температуры 1 фунта воды на 1 градус Фаренгейта. 1000 BTU = 0,293 кВт. – *Прим. перев.*

системой чаще подвергается чтению, чем записи, как правило, имеет место чистый выигрыш.

Без зеркального копирования сбой жесткого диска означает простой в работе. Благодаря зеркальному копированию сбой жесткого диска является событием, которое можно не только спокойно пережить, но и контролировать. Если неисправный диск можно заменить во время работы системы, сбой в работе одного компонента не приведет к простою. Если неисправные диски можно заменять только при отключенной системе, перерыв в работе можно запланировать в соответствии с потребностями компании. Благодаря этому простои в работе можем контролировать мы, не позволяя им контролировать нас.

Всегда помните, что зеркальное RAID-копирование защищает от сбоев оборудования. Оно не защищает от программных или пользовательских ошибок. Ошибочные изменения, внесенные на основной диск, немедленно копируются на второй диск, поэтому невозможно восстановить состояние, предшествующее ошибке, просто используя второй диск.

Более подробно экстренное восстановление описано в главе 10.

Даже зеркальным дискам требуется резервное копирование

В одной крупной компании, занимающейся электронной коммерцией, использовалась схема RAID 1 для копирования системного диска основного сервера баз данных. В часы максимальной загрузки системы начали появляться проблемы с повреждением баз данных. Поставщик баз данных и поставщик операционной системы винили друг друга. Системным администраторам в результате пришлось снять дамп памяти системы в процессе искажения данных, чтобы понять, кто виноват на самом деле. Системные администраторы были не в курсе, но операционная система в качестве указателя памяти использовала целое число со знаком вместо целого числа без знака. Когда начался дамп памяти, он достиг отметки, в которой указатель памяти стал отрицательным и начал перезаписывать другие разделы системного диска. RAID-система преданно скопировала повреждения на зеркало, таким образом сделав его бесполезным. Эта программная ошибка вызвала очень долгий простой в работе, который обошелся компании чрезвычайно дорого и получил широкую огласку. В результате компания потеряла миллионы на упущенных сделках, а стоимость ее акций резко упала. Мораль этой истории: зеркальное копирование очень полезно, но нельзя недооценивать грамотные утилиты для резервного копирования, позволяющие вернуться к исправному известному состоянию.

4.2. Тонкости

Разобравшись с основами, перейдем к методам, позволяющим несколько повысить надежность и удобство обслуживания. Кроме того, мы кратко опишем противоположную точку зрения.

4.2.1. Повышение надежности и удобства обслуживания

4.2.1.1. Одноцелевые серверы

Одноцелевое устройство – устройство, созданное для выполнения одной конкретной задачи. Тостеры делают тосты. Миксеры смешивают. Те же действия можно выполнять и с помощью универсальных устройств, но есть определенные преимущества при использовании устройств, предназначенных для качественного выполнения одной конкретной задачи.

В компьютерном мире также есть одноцелевые устройства: файловые серверы, веб-серверы, серверы электронной почты, DNS-сервера и т. д. Первым таким устройством стал выделенный сетевой маршрутизатор. Кое-кто иронизировал: «Кто согласится отдавать такие деньги за устройство, которое только и делает, что занимает место и передает пакеты. Ведь то же самое можно сделать, добавив дополнительные интерфейсы в VAX[1]». Как оказалось, многие были готовы приобрести такое устройство. Вскоре стало очевидно, что устройство, предназначенное для выполнения одной задачи и прекрасно ее выполняющее, во многих случаях является более ценным, чем универсальный компьютер, способный выполнять множество задач. И, черт побери, самое главное – это устройство позволяло перезагружать VAX, не прерывая при этом работу сети.

Одноцелевой сервер представляет собой устройство, в котором воплотился многолетний опыт. Конструирование сервера – сложный процесс. К серверному оборудованию применимы все требования, перечисленные выше в этой главе. Кроме того, системное проектирование и настройка производительности требуют высокой квалификации и большого опыта в соответствующих областях. Программное обеспечение, необходимое для работы той или иной службы, часто подразумевает компоновку различных программных пакетов, их связывание и создание единой общей системы администрирования для них. А это много работы! Одноцелевые устройства прекрасно делают ее за вас.

Хотя старший системный администратор может установить и настроить службу файлового сервера или сервера электронной почты на универсальном сервере, приобретение одноцелевого устройства позволит сэкономить время, которое системный администратор может потратить на выполнение других задач. Каждое приобретенное одноцелевое устройство уменьшает количество систем, которые необходимо устанавливать с нуля, а также дает преимущество поддержки от поставщика в случае неполадок. Кроме того, одноцелевые устройства позволяют организациям получить качественно настроенные системы без необходимости нанимать опытных специалистов.

Еще одно преимущество одноцелевых устройств – наличие возможностей, которых больше нигде нет. Конкуренция побуждает поставщиков добавлять новые возможности, повышать производительность и улучшать надежность. Например, устройства NetApp Filer позволяют делать настраиваемые снимки файловой системы, таким образом устраняя часто возникающую необходимость восстановления файлов.

---

[1] Virtual Address eXtension, 32-битная компьютерная архитектура, была разработана в середине 1970-х годов Digital Equipment Corporation. – *Прим. перев.*

4.2.1.2. Резервные блоки питания

По предрасположенности к сбоям среди всех системных компонентов на втором месте после жестких дисков находятся блоки питания. Поэтому в идеале серверы должны быть обеспечены резервными блоками питания.

Наличие резервных блоков питания не означает, что просто подключено два таких устройства. Это означает, что система сохраняет работоспособность, если один из блоков питания не функционирует: избыточность $n + 1$. В некоторых случаях системе при полной нагрузке требуется два блока питания для обеспечения достаточной мощности. В этом случае *избыточность* обеспечивается тремя блоками питания. Это важный вопрос, который необходимо выяснить с поставщиками при приобретении серверов и сетевого оборудования. Сетевое оборудование особенно предрасположено к этой проблеме. Когда в большой сети сетевые устройства, подключенные по оптоволоконному каналу, полностью нагружены, дублирование блоков питания является необходимостью, а не избыточностью. Поставщики далеко не всегда упоминают об этом.

У каждого блока питания должен быть отдельный кабель питания. На практике самая распространенная причина проблем с питанием – случайно выдернутый из розетки кабель. Официальные исследования надежности питания часто упускают из виду подобные проблемы, ведь они изучают энергоснабжение. Единый кабель питания для всех устройств в такой ситуации только помеха! Любой поставщик, предоставляющий один кабель питания для нескольких блоков питания, тем самым демонстрирует свое невежество в отношении этой основной практической проблемы.

Еще одна причина для применения отдельных кабелей питания – возможность использовать следующий прием. В некоторых случаях устройство необходимо подключить к другому удлинителю, UPS или другой электрической сети. В такой ситуации можно по очереди переключить отдельные кабели питания, избежав простоя в работе системы.

Если работоспособность системы должна быть очень высокой, каждый блок питания необходимо подключить к разным источникам, например к отдельным UPS. Если один UPS даст сбой, система продолжит работу. В некоторых вычислительных центрах прокладывают проводку уже с учетом этого аспекта. Чаще всего каждый блок питания подключается к отдельному электрическому распределительному щиту. Если кто-то, по ошибке подключив слишком много устройств, перегрузит распределительный щит, система будет продолжать работать.

Преимущество отдельных кабелей питания

Однажды у Тома возникла необходимость запланировать отключение UPS, от которого питался весь машинный зал. Однако один маршрутизатор ни в коем случае нельзя было отключать. Он имел важное значение для проектов, на которых не должно было отразиться отключение питания. У этого маршрутизатора имелись резервные блоки питания с отдельными кабелями. Любой из блоков питания мог обеспечить электроэнергией всю систему. Том переключил один кабель в розетку без UPS,

предназначенную для освещения и других приборов, не требующих поддержки UPS. При этом маршрутизатор потерял лишь питание UPS, но продолжил работу. Маршрутизатор функционировал без простоев все время, пока было отключено питание.

4.2.1.3. Полная избыточность, или n + 1

Как уже упоминалось выше, **избыточность *n* + 1** относится к системам, которые спроектированы таким образом, что система продолжает функционировать даже после сбоя одного из компонентов. Примером такой системы являются RAID-массивы, которые продолжают полноценно функционировать даже после выхода из строя одного из дисков, или коммутатор Ethernet с дополнительной многовходовой системой коммутации, который позволяет передавать трафик даже после сбоя одного из сегментов системы коммутации.

Напротив, при **полной избыточности** два полных набора оборудования объединены в *отказоустойчивую* конфигурацию. Первая система обеспечивает исполнение службы, а вторая бездействует в полной готовности взять на себя работу при сбое первой системы. Переключение на резервные мощности может осуществляться вручную (кто-то замечает сбой в первой системе и активирует вторую) или автоматически (вторая система отслеживает работу первой системы и сама активируется при ее отказе).

Другие системы с полной избыточностью используют **распределение нагрузки**. Обе системы полноценно функционируют и распределяют между собой рабочую нагрузку. Каждый сервер обладает достаточной мощностью, чтобы взять на себя всю нагрузку. Если в работе одной из систем возникает сбой, вторая система берет всю нагрузку на себя. Системы можно настроить таким образом, чтобы они отслеживали надежность работы друг друга. Либо можно использовать внешний источник управления потоками и распределением запросов на обслуживание.

Если n равно или больше 2, $n + 1$ выгоднее, чем полная избыточность. Пользователи обычно предпочитают этот метод из-за его экономичности.

Как правило, избыточность $n + 1$ используется только для серверных подсистем, а не для всех видов компонентов. Всегда проверяйте, не пытается ли поставщик вам продать систему с избыточностью $n + 1$, где резервными являются только некоторые части системы. Какой прок в автомобиле с дополнительными покрышками, если сломается двигатель?

4.2.1.4. Компоненты, поддерживающие «горячую» замену

Резервные компоненты должны поддерживать «горячую» замену. **«Горячая» замена** подразумевает возможность отключить и заменить компонент во время работы системы. Как правило, компоненты следует заменять только при отключенной системе. Возможность «горячей» замены аналогична смене покрышки в тот момент, когда автомобиль мчится по шоссе. Очень удобно, когда не приходится останавливаться, чтобы устранить обычную проблему.

Первое преимущество «горячей» замены – возможность устанавливать компоненты во время работы системы. Нет никакой необходимости планировать от-

ключение систем, чтобы установить тот или иной компонент. Однако установка новых компонентов, как правило, является запланированным событием, которое можно перенести на следующий профилактический перерыв. Поэтому главное преимущество «горячей» замены выявляется при сбоях.

При избыточности $n + 1$ система может перенести сбой только одного компонента. Именно поэтому критически важно как можно быстрее заменить нерабочий компонент, чтобы нейтрализовать риск *двойного сбоя компонентов*. Чем дольше будет промедление, тем выше становится этот риск. Если бы не возможность «горячей» замены, системному администратору пришлось бы ждать запланированной перезагрузки, чтобы вернуться к безопасной конфигурации $n + 1$. Благодаря «горячей» замене системный администратор может сменить компонент, не отключая систему. В RAID-системах предусматривают диск с *«горячей» заменой*, который находится системе, но не используется, пока не возникнет необходимость заменить вышедший из строя диск. Если система сможет изолировать неисправный диск, чтобы он не остановил работу всей системы, то она будет способна автоматически активировать диск с «горячей заменой», сделав его частью соответствующего RAID-массива. Таким образом, мы получаем систему $n + 2$.

Чем быстрее система будет возвращена в состояние полной избыточности, тем лучше. RAID-системы, как правило, работают медленнее до тех пор, пока неисправный компонент не будет заменен и RAID-массив не будет восстановлен. Но что самое важное, пока система не возвращена в состояние полной избыточности, существует риск второго сбоя дисков. Если это произойдет, вы потеряете все данные. Некоторые RAID-системы можно настроить таким образом, чтобы они отключались через определенное количество часов работы в неизбыточном состоянии.

Компоненты с возможностью «горячей» замены повышают стоимость системы. В каких же случаях оправдана повышенная стоимость? Когда устранение простоев действительно стоит дополнительных затрат. Если для системы предусмотрены запланированные еженедельные перерывы в работе и работа системы при риске двойного сбоя в течение недели считается приемлемой, не стоит тратить дополнительные средства на компоненты с возможностью «горячей» замены. Если же технический перерыв для системы планируется проводить всего раз в год, такие затраты будут оправданы.

Если поставщик заявляет о возможности «горячей» замены компонентов, всегда задавайте два вопроса: «Какие компоненты не имеют возможности «горячей» замены? Каким образом и на какой период прерывается работа при «горячей» замене компонентов?» Некоторые сетевые устройства оснащены интерфейсными картами, которые поддерживают «горячую» замену, но сам процессор такую возможность не поддерживает. Некоторые сетевые устройства, для которых заявлена возможность «горячей» замены, полностью перезапускают всю систему после установки нового устройства. Такая перезагрузка может занять несколько секунд или минут. Некоторые дисковые подсистемы при замене диска останавливают работу системы ввода-вывода на период до 20 с. Другие системы в течение нескольких часов значительно снижают производительность работы, пока на резервном диске восстанавливаются данные. Вы должны точно представлять себе возможные последствия сбоя компонентов. Не рассчитывайте на то, что возможность «горячей» замены компонентов навсегда устранит простои в работе. Она просто уменьшает их продолжительность.

Поставщики должны (хотя часто этого не делают) указывать на ярлыках компонентов, поддерживают ли они «горячую» замену. Если же поставщик не позаботился о таких ярлыках, вы должны сделать это сами.

«Горячее» подключение или «горячая» замена

Всегда обращайте внимание, не указана ли на ярлыке компонента возможность «горячего» подключения (hot plug). Это означает, что замена компонента во время работы системы безопасна для электроники, однако этот компонент может быть распознан только после следующей перезагрузки системы. Или, что еще хуже, подключить компонент можно к работающей системе, но система будет тут же перезагружена, чтобы распознать этот компонент. А это значительно отличается от «горячей» замены.

Однажды Том вызвал значительный, хотя и кратковременный простой, когда подключил к шасси сетевого коммутатора новую плату с 24 портами FastEthernet. Ему сказали, что эти платы поддерживают возможность «горячего» подключения, и Том решил, что под этим термином поставщик имел в виду «горячую» замену. После подключения карты вся система перезагрузилась. Это был центральный коммутатор серверной и большей части сетей в подразделении, где работал Том. Ой!

Можете себе представить, какой спор разгорелся, когда Том позвонил поставщику с претензиями. Поставщик возразил, что, если бы пришлось отключать систему, подключать плату и снова включать систему, простой в работе был бы значительно длиннее. «Горячее» подключение – улучшенная возможность.

С тех самых пор над устройством до самого момента его списания висел огромный плакат: «Внимание! Подключение новой карты приводит к перезагрузке системы. Поставщик считает, что так и надо».

4.2.1.5. Раздельные сети для административных функций

Дополнительные сетевые интерфейсы на серверах позволяют создать раздельные административные сети. Например, часто создают отдельную сеть для резервного копирования и мониторинга. Резервное копирование требует высокой пропускной способности, и отделение этого трафика от основной сети означает, что резервное копирование не будет мешать пользователям работать с сетью. Подобную отдельную сеть можно спроектировать с помощью довольно простого оборудования, таким образом сделав ее более надежной. Но что самое важное, на эту сеть не будут влиять простои в работе основной сети. Кроме того, она дает системным администраторам возможность получить доступ к машине во время такого простоя. Эта форма избыточности решает очень специфическую проблему.

4.2.2. Альтернатива: множество недорогих серверов

В этой главе мы рекомендовали не экономить на серверном оборудовании, так как повышение быстродействия и надежности стоит дополнительных затрат.

Однако все чаще мы сталкиваемся со встречным доводом, в соответствии с которым лучше использовать несколько недорогих одинаковых серверов, которые будут давать сбои чаще. Если вы умеете неплохо справляться со сбоями, такая стратегия будет для вас более выгодной.

Запуск крупной веб-фермы потребует использования нескольких резервных серверов. Все эти серверы должны быть сконфигурированы абсолютно одинаково – путем автоматической установки. Если каждый веб-сервер способен обрабатывать 500 запросов в секунду, вам понадобится десять серверов, чтобы обрабатывать 5000 запросов в секунду, которые, как вы предполагаете, будут поступать от пользователей Интернета. Механизм распределения нагрузки может распределять нагрузку среди серверов. Но что самое лучшее, системы распределения нагрузки могут автоматически определять машины, в работе которых произошел сбой. Если один сервер «падает», механизм распределения нагрузки распределяет запросы между оставшимися рабочими серверами и пользователи продолжают получать доступ к сервису. При этом загрузка каждого сервера повышается на одну десятую, но это лучше простоя в работе.

Но что если вы используете компоненты худшего качества, которые могут привести к десяти сбоям? Если при закупке вы смогли сэкономить 10%, можно приобрести одиннадцатую машину, которая будет компенсировать частые сбои и сниженную производительность более медленных машин. Однако при этом получается, что вы потратили ту же сумму денег, получили возможность обрабатывать то же количество запросов в секунду и все это при том же периоде работоспособности. Разницы никакой, правда?

В начале 1990-х годов стоимость серверов доходила до 50 тысяч долларов. Настольные компьютеры стоили около 2 тысяч долларов, так как они состояли из серийных компонентов, которые выпускались в массовом производстве в количествах, гораздо превышающих количество серверных компонентов. Если спроектировать сервер на основе серийных компонентов, он не сможет обрабатывать необходимое количество запросов в секунду и интенсивность отказов будет гораздо выше.

Однако к концу 1990-х годов экономика изменилась. Благодаря продолжительному массовому производству компонентов для персональных компьютеров и цены, и производительность со временем стали значительно привлекательнее. Такие компании, как Yahoo! и Google, нашли способы эффективного управления большим количеством машин, оптимальной установки оборудования, обновления программного обеспечения, управления ремонтом оборудования и т. д. Оказывается, если делать все это в больших масштабах, затраты значительно снижаются.

Традиционное мышление подсказывает, что никогда не стоит запускать коммерческую службу на сервере, созданном из серийных компонентов, который может обрабатывать всего 20 запросов в секунду. Однако, если вы можете управлять большим количеством таких серверов, ситуация меняется. Продолжая тот же пример, вам пришлось бы приобрести 250 таких серверов, чтобы добиться производительности 10 традиционных серверов, о которых говорилось ранее. В результате вы заплатите за оборудование ту же сумму.

По мере повышения количества запросов в секунду такое решение стало менее дорогостоящим по сравнению с покупкой крупных серверов. Если они обеспечивали производительность 100 запросов в секунду, можно было для получения той же мощности приобрести 50 серверов по одной пятой от стоимости или потратить те же деньги и получить мощность в пять раз выше.

Отказавшись от компонентов, которые не используются в такой среде, например видеокарт, USB-разъемов и т. д., можно еще больше снизить затраты. Вскоре появилась возможность приобрести от пяти до десяти серверов из серийных компонентов взамен одного традиционного сервера и при этом получить бóльшую процессорную мощность. Оптимизация требований к физическому оборудованию привела к созданию более эффективных конфигураций, и в результате мощные серверы можно вместить в корпус высотой не более одного юнита[1].

Именно благодаря масштабным кластерным системам стала возможной работа крупных веб-служб. В результате становится понятно, почему все больше и больше служб начинают использовать такой тип архитектуры.

Пример: одноразовые серверы

Многие компании, занимающиеся электронной коммерцией, создают гигантские кластерные структуры из недорогих 1U-серверов. Стойки заполняются максимальным количеством серверов, чтобы каждую необходимую службу обеспечить десятками или сотнями серверов. В одной компании пришли к выводу, что при выходе из строя какого-либо блока оборудования выгоднее отключить этот блок и оставить его в стойке, чем ремонтировать его. При удалении вышедших из строя блоков есть риск отключения другого оборудования, если случайно задеть его кабели. В этой компании достаточно долго не возникало необходимости «собирать урожай» из неисправных блоков. Наверное, когда в стойках закончится свободное место, в компании введут ежемесячный день «урожая». Некоторые сотрудники будут внимательно следить за системами мониторинга служб, а другие – вытаскивать из стоек неисправные машины.

Еще один способ разместить большое количество машин на ограниченном пространстве – использовать технологию **блейд-серверов**. Один корпус содержит множество ячеек, в каждую из которых можно подключить плату (блейд) с процессором и памятью. Корпус обеспечивает питание, доступ к сети и системе управления. В некоторых случаях каждая плата оснащена жестким диском. В других случаях у каждой платы должен быть доступ к центральной сети хранения данных. Так как все устройства схожи друг с другом, можно создать автоматизированную систему, которая позволяет заменить неисправное устройство свободным.

В последнее время все более важное значение приобретает новая технология виртуальных серверов. Сегодня серверное оборудование является настолько мощным, что оправдывать затраты на узкоспециализированные машины становится все сложнее. Концепция сервера как набора компонентов (аппаратных и программных) обеспечивает безопасность и простоту. С помощью запуска множества виртуальных серверов на одном крупном мощном сервере можно получить преимущества обеих систем. Виртуальные серверы более подробно описаны в разделе 21.1.2.

---

[1] Юнит (от англ. unit) – шаг крепежных отверстий в стандартной телекоммуникационной стойке. Для этой единицы используется сокращение U. Таким образом, оборудование, выступающее выше или ниже своего крепежа, считается 2U-системой.

Управление блейд-сервером

Подразделение крупной транснациональной компании решило заменить устаревший многопроцессорный сервер на ферму блейд-серверов. Необходимо было переписать код приложения таким образом, чтобы процессы распределялись по блейд-ферме вместо выполнения нескольких процессов на одной машине. Каждая блейд-плата должна была стать одним узлом обширной компьютерной фермы, которой будут передаваться задачи, а результаты будут сводиться на управляющем сервере. Такая система отличается прекрасной масштабируемостью, поскольку новые блейд-платы можно добавлять в ферму за считанные минуты с помощью автоматизированного процесса, если того требует приложение, или так же быстро переназначать на другие цели. Прямого доступа пользователя в систему при этом не требуется, а системные администраторы должны лишь заменять неисправное оборудование и управлять назначением плат на различные приложения. С этой целью системные администраторы разработали высокозащищенное, специальное, с правами минимального доступа решение, которое может быть развернуто за считанные минуты. Сотни блейд-плат были приобретены, установлены и подготовлены для различных целей в соответствии с требованиями пользователей.

Проблемы появились, когда разработчики приложения поняли, что не могут управлять своим приложением. Они не могли исправлять ошибки без прямого доступа. Им был необходим консольный доступ. Им нужны были дополнительные пакеты. Для каждой машины они сохраняли уникальное состояние, поэтому автоматизированные сборки приложений стали невозможны. И тогда системные администраторы оказались в ситуации, в которой они были вынуждены управлять 500 отдельными серверами, а не блейд-фермой. Другие подразделения также нуждались в доступе для обслуживания и предъявляли те же требования.

Эту проблему могли бы предотвратить две меры. Во-первых, большее внимание к деталям на стадии определения потребностей могло помочь предвидеть необходимость в доступе для разработчиков. В этом случае такой доступ можно было бы предусмотреть при разработке. Во-вторых, управление должно быть более организованным. Если разработчикам был предоставлен требуемый доступ, управление должно было установить ограничения, которые помешали бы распаду системы на сотни отдельных машин. Первоначальную цель утилиты, обеспечивающей доступ к множеству сходных процессоров, необходимо было увязать со всем жизненным циклом системы, а не оставлять все на волю случая при проектировании.

4.3. Заключение

Приобретая серверы, мы принимаем различные решения, так как от серверов зависит деятельность множества пользователей, в то время как клиентская рабочая станция предназначена только для одного пользователя. В отличие от рынка настольных компьютеров, на рынке серверного оборудования важнейшее значение имеют иные экономические факторы. Знание этих факторов помогает

принимать более грамотные решения при покупке. Серверы, как и любое другое оборудование, иногда дают сбои, поэтому необходимо заключить контракт на обслуживание или составить план восстановления, а также предусмотреть возможность резервного копирования и восстановления данных. Серверы должны располагаться в специальных машинных залах, обеспечивающих условия для надежной работы (более подробно требования к вычислительным центрам обсуждаются в главе 5). Пространство в машинном зале необходимо распределить до момента покупки, а не когда прибудет сервер. Кроме того, заранее необходимо спланировать электросеть, пропускную способность сети и систему охлаждения.

Одноцелевые серверы – аппаратные или программные системы, которые содержат все необходимое для выполнения определенной задачи: заранее сконфигурированное программное обеспечение, которое установлено на оборудовании, специально настроенном для конкретного приложения. Одноцелевые серверы представляют собой высококачественные решения, разработанные с учетом многолетнего опыта. Они, как правило, являются более надежными и простыми в управлении, чем менее профессиональные решения. Однако такие системы достаточно сложно настраивать для нетипичных требований корпоративной сети.

Серверам необходима возможность удаленного администрирования. Аппаратные или программные системы позволяют удаленно выполнять консольный доступ. Это позволяет освободить дополнительное пространство в машинном зале, а также дает возможность системным администраторам осуществлять работу из своего кабинета или дома. Системные администраторы могут проводить требуемое обслуживание без необходимости находиться непосредственно рядом с сервером.

Для повышения надежности серверы часто оснащаются дополнительными системами, предпочтительно в конфигурации $n + 1$. Наличие зеркалированного системного диска, резервных источников питания и других дополнительных компонентов повышает период работоспособного состояния системы. Возможность заменять неисправные компоненты во время работы системы уменьшает среднее время восстановления и перерывы в обслуживании. Хотя в прошлом подобная избыточность была роскошью, в современных условиях она зачастую является необходимостью.

Эта глава иллюстрирует наше утверждение о необходимости прежде всего разобраться с основами, чтобы впоследствии все шло своим ходом. Грамотное решение вопросов, рассмотренных в этой главе, играет большую роль для повышения надежности системы, а также упрощения обслуживания и восстановления. Эти вопросы необходимо решить в самом начале, а не откладывать на потом.

Задания

1. Какие серверы используются в вашем сетевом окружении? Оборудование какого количества разных поставщиков вы используете? Как вы думаете, это много? Каковы преимущества и недостатки повышения количества поставщиков? А уменьшения?
2. Опишите стратегию вашей компании при заключении контрактов на обслуживание и ремонт. Что можно сделать, чтобы снизить эту статью расходов? Что можно сделать, чтобы повысить качество обслуживания?

3. Каковы основные и менее значимые различия между узлами, которые вы используете в качестве серверов, и клиентскими рабочими станциями?
4. Для чего может понадобиться возможность «горячей» замены компонентов, если в системе нет избыточности $n + 1$?
5. Для чего может использоваться избыточность $n + 1$, если ни один компонент системы не поддерживает возможность «горячей» замены?
6. Какие критические узлы в вашей сети не обладают избыточностью $n + 1$ или не имеют компонентов с «горячей» заменой? Определите стоимость обновления самых критических узлов и внедрения на них избыточности $n + 1$.
7. Системному администратору понадобилось добавить диск в сервер из-за недостатка дискового пространства. Но он решил подождать до следующего профилактического перерыва и не устанавливать диск во время работы системы. Почему?
8. Какие службы в вашей сети было бы неплохо заменить одноцелевыми серверами (вне зависимости от того, доступна ли вам такая возможность)? Почему они являются подходящими кандидатами для замены?
9. Какие одноцелевые серверы используются в вашей сети? Какую именно работу по проектированию вам пришлось бы провести, если бы вы использовали для тех же целей универсальную машину?

Глава 5

Сервисы

Сервер – это оборудование. Сервис – это функция, предоставляемая сервером. Сервис может быть скомпонован на нескольких серверах, которые работают совместно друг с другом. В этой главе описывается создание сервиса, который отвечает требованиям пользователя, отличается надежностью и простотой обслуживания.

Предоставление сервиса подразумевает не только совмещение оборудования и программного обеспечения, но и обеспечение надежности сервиса, его масштабирование, а также мониторинг, обслуживание и поддержку. Сервис действительно становится сервисом только тогда, когда он отвечает этим основным требованиям.

Одной из основных обязанностей системного администратора является предоставление пользователям необходимых им сервисов. И это должно осуществляться постоянно. Нужды пользователей меняются по мере того, как меняются их должностные обязанности и развиваются технологии. В результате системный администратор вынужден тратить немало времени на разработку и установку новых сервисов. От того, насколько хорошо системный администратор настроит эти сервисы, будет зависеть количество времени и усилий, которое впоследствии необходимо будет тратить на поддержку этих сервисов, а также то, насколько довольны будут пользователи.

Любая типичная сеть обладает большим набором сервисов. Основные сервисы включают в себя DNS, электронную почту, сервисы аутентификации, подключения к сети и печати[1]. Эти сервисы являются самыми важными и в случае сбоев самыми заметными. Другими типичными сервисами являются различные методы удаленного доступа, сервис сетевого лицензирования, хранилища программ, сервис резервного копирования, доступ к Интернету, DHCP и файл-сервисы. Это всего лишь некоторые из общих сервисов, которые обычно предоставляют системные администраторы. Кроме того, существуют специализированные бизнес-сервисы, предназначенные для конкретных целей компании: бухгалтерских, производственных и других областей бизнеса.

Именно сервисы отличают структурированное компьютерное окружение, обслуживаемое системными администраторами, от окружения, состоящего из

---

[1] DNS, сеть и аутентификация – сервисы, от которых зависят многие другие сервисы. Электронная почта и печать могут казаться менее важными, но если откажет одна из них, вы поймете, что они являются центром работы всех сотрудников. Связь и печатные копии необходимы в работе любой компании.

одного или нескольких отдельных компьютеров. Дома и в небольших компаниях, как правило, установлено несколько отдельных машин, предоставляющих сервисы. Более крупные сети обычно связаны общими сервисами, которые упрощают связь и оптимизируют ресурсы. Когда домашний компьютер подключается к Интернету через провайдера интернет-услуг, он использует сервисы, предоставляемые интернет-провайдером и другими людьми, с которыми пользователь соединяется через Интернет. Офисные компьютеры используют те же сервисы и некоторые другие.

5.1. Основы

Создание исправного и надежного сервиса – ключевая задача системного администратора, которому при ее выполнении необходимо учитывать множество основных факторов. Самым важным таким фактором на всех этапах создания и развертывания являются потребности пользователей. Поговорите с пользователями и выясните, в чем они нуждаются и чего ожидают от данного конкретного сервиса[1]. Затем составьте список других требований, таких как административные требования, о которых знают только системные администраторы. Для вас ключевым словом должно быть *что*, а не *как*. Очень просто запутаться в реализации и забыть о целях и задачах.

Мы добились успеха с помощью открытых протоколов и открытых архитектур. Возможно, вы не всегда сможете этого достичь, но это стоит учитывать при разработке.

Сервисы необходимо создавать на машинах серверного класса, которые содержатся в соответствующих условиях и отличаются разумным уровнем надежности и быстродействия. За сервисом и машинами, от которых он зависит, необходимо установить мониторинг. При сбоях в работе должны генерироваться предупреждения или уведомления о неисправностях.

Большинство сервисов зависят от других сервисов. Понимание того, каким образом работает сервис, позволит вам точно определить, от каких сервисов он зависит. Например, почти все сервисы зависят от DNS. Если имена машин или имена доменов прописаны в конфигурации сервиса, значит, он зависит от DNS. Если в его log-файлах указываются имена узлов сети, которые используют сервис или к которым он обращается, значит, он использует DNS. Если люди, использующие сервис, пытаются через него связаться с другими машинами, значит, этот сервис использует DNS. Кроме того, практически каждый сервис зависит от сети, которая также является сервисом. DNS зависит от сети, поэтому все сервисы, зависящие от DNS, также зависят и от сети. Некоторые сервисы зависят от электронной почты, которая, в свою очередь, зависит от DNS и сети. Другие сервисы зависят от доступа к общим файлам на других компьютерах. Многие сервисы также зависят от сервиса аутентификации и авторизации, который позволяет отличить одного человека от другого, особенно в тех случаях, когда разные уровни доступа основаны на идентификации. Отказ в работе некоторых сервисов, таких как DNS, вызывает каскадные сбои всех других зависящих от них сервисов. При создании сервиса очень важно понимать, от каких сервисов он будет зависеть.

---

[1] Для некоторых сервисов, таких как служба имен и служба аутентификации, нет никаких требований пользователей, кроме того, что они должны работать стабильно, быстро и ненавязчиво.

Машины и программы, которые являются частью сервиса, должны зависеть от узлов и программ, созданных в соответствии с теми же или более высокими стандартами. Надежность сервиса соответствует надежности самого слабого звена в цепи сервисов, от которых он зависит. Сервис не должен неоправданно зависеть от узлов сети, которые не являются частью этого сервиса.

Доступ к серверным машинам должен быть ограничен для системных администраторов ради надежности и безопасности. Чем больше людей используют машину и чем больше программ и сервисов на ней запускается, тем выше шанс нарушения работоспособности. На машинах, на которых работают пользователи, должно быть установлено дополнительное ПО, так как пользователям нужен доступ к требуемым данным и другим сетевым сервисам.

Точно так же безопасность системы определяется уровнем безопасности ее самого слабого звена. Безопасность пользовательских систем не может быть выше самого слабого звена в безопасности всей инфраструктуры. Тот, кто сможет взломать сервер аутентификации, сможет и получить доступ к зависящей от него пользовательской информации. Тот, кто сможет взломать DNS-серверы, сможет перенаправить трафик от пользователя и получит потенциальный доступ к паролям. Если система безопасности зависит от DNS-сервера, который нетрудно взломать, такая система безопасности является уязвимой. Ограничение входа в систему и других видов доступа к машине в инфраструктуре безопасности снижает подобный риск.

Сервер должен быть максимально простым. Простота повышает надежность машин и упрощает исправление в случае возникновения проблем. Серверы должны отвечать минимальным требованиям к работе сервиса, и только системные администраторы должны иметь к ним доступ. Кроме того, системные администраторы должны получать к ним доступ только с целью обслуживания. Помимо этого, с точки зрения безопасности уязвимость серверов более критична, чем настольных компьютеров. Злоумышленник, который способен получить доступ с правами администратора к серверу, как правило, способен нанести больший урон, чем при доступе с правами администратора к настольному компьютеру. Чем меньше людей обладают доступом и чем меньше программ используется на этой машине, тем ниже риск того, что злоумышленник сможет получить к ней доступ, и тем выше шансы того, что злоумышленник будет обнаружен.

Системный администратор должен принять несколько решений при создании сервиса: оборудование какого поставщика необходимо приобрести, использовать ли один или несколько серверов для сложного сервиса, а также какой уровень избыточности необходимо предусмотреть в сервисе. Сервис должен быть максимально простым с минимальным количеством зависимостей – это позволит повысить его надежность и упростить поддержку и обслуживание. Еще один способ упростить поддержку и обслуживание сервиса – использовать стандартные оборудование, программное обеспечение и конфигурации, а также хранить документацию в стандартных местах. Кроме того, поддержку упрощает централизация сервисов, например наличие одного или двух крупных принт-серверов вместо сотен мелких, разбросанных по всей компании. И наконец, последний аспект внедрения любого нового сервиса – сделать его независимым от той конкретной машины, на которую он устанавливается, используя имена, связанные с сервисом, в конфигурации пользователей вместо, к примеру, реального имени узла. Если ваша операционная система не поддерживает эту функцию, сообщите поставщику ОС, что эта возможность является для вас очень важной,

и обдумайте возможность временно использовать другую операционную систему (более подробно этот вопрос обсуждается в главе 8). После того как сервис создан и протестирован, к нему необходимо постепенно подключать пользователей, параллельно тестируя и отлаживая его работу.

Пример: привязка сервисов к машине

В небольшой компании все сервисы запускаются на одной или двух центральных машинах. По мере роста компании эти машины могут стать перегруженными и некоторые сервисы придется перенести на другие машины. Таким образом, количество серверов увеличится и на каждом из них будет запущено меньше сервисов. Например, предположим, что центральная машина является почтовым сервером, почтовым релеем, принт-сервером и календарным сервером. Если все эти сервисы привязаны к настоящему имени машины, на каждой пользовательской машине в компании это имя будет указано в почтовом клиенте, настройках принтера, а также в планировщике событий. Если этот сервер сильно нагружен, обе почтовые функции переносятся на другую машину с другим именем и необходимо поменять настройки почты на всех остальных машинах в компании, что требует немалых усилий и вызывает перерыв в работе. Если на сервере снова возникает перегрузка и сервис печати перемещается на другую машину, снова потребуется перенастройка всех остальных машин в компании. С другой стороны, если бы каждый сервис был привязан к соответствующему глобальному псевдониму, например `smtp` для релея, `mail` для почтового сервера, `calendar` для календарного сервера и `print` для принт-сервера, достаточно было бы лишь заменить общий псевдоним, не прерывая при этом работу пользователей и не тратя излишнее время и силы (кроме как на создание самого сервиса).

5.1.1. Требования пользователей

Процесс создания нового сервиса всегда необходимо начинать с учета требований пользователей. Ведь сервис создается для пользователей. Если сервис не будет соответствовать их нуждам, на его создание будут лишь зря потрачены силы.

Для некоторых сервисов требований пользователей нет. DNS – один из таких сервисов. Другие сервисы, такие как электронная почта и сеть, более весомы для пользователей. Пользователям могут понадобиться определенные возможности их почтовых клиентов, и разные пользователи в различной степени загружают сеть в зависимости от выполняемой ими работы и настройки используемых систем. Другие сервисы в первую очередь ориентированы на пользователей, например система электронных заказов на закупку. Системные администраторы должны понимать, как пользователи будут применять сервис и какие их требования следует учесть при разработке сервиса.

Сбор требований пользователей подразумевает ответы на вопросы, каким образом пользователи намерены использовать сервис, какие возможности нужны и удобны для пользователей, насколько важным является для них этот сервис, какой уровень работоспособности и поддержки нужен пользователям для этого сервиса. Обеспечьте участие сотрудников в тестировании удобства использова-

ния демонстрационной версии сервиса, если это возможно. Если вы выберете систему, которая покажется людям слишком сложной в использовании, ваш проект окажется неудачным. Постарайтесь оценить, как много сотрудников будут пользоваться этим сервисом и какого уровня быстродействия они от него ожидают. Это поможет вам создать надежный и работоспособный сервис. Например, при создании почтовой системы постарайтесь оценить, сколько писем (входящих и исходящих) будет проходить через систему в самые загруженные дни, сколько дискового пространства понадобится каждому пользователю для их сохранения и т. д.

Кроме того, самое время сейчас разработать соглашение об уровне обслуживания для нового сервиса. В этом соглашении перечислены предоставляемые сервисы и уровень их поддержки. Как правило, в нем описаны проблемы, разбитые по категориям приоритетов. Для каждой категории указывается время ответных действий, возможно, по времени суток или дням недели, если в сети не предоставляется круглосуточная поддержка без выходных. Как правило, в соглашении об уровне обслуживания определяется процесс эскалации, который повышает серьезность проблемы, если она не решена в течение определенного времени, и привлекает внимание руководства, если проблема выходит из-под контроля. В случае когда пользователь платит за определенный сервис, в соглашении об уровне обслуживания описываются штрафы, накладываемые на поставщика, если его сервис не соответствует указанным стандартам. Это соглашение всегда обсуждается и утверждается обеими сторонами.

Процесс составления соглашения об уровне обслуживания – возможность для системных администраторов понять ожидания пользователей и соответственно их направлять, чтобы пользователи понимали, что выполнить возможно, а что нет и почему. Кроме того, это возможность распланировать требуемые для проекта ресурсы. Соглашение об уровне обслуживания должно описывать потребности пользователей и устанавливать реалистичные цели для системных администраторов в плане возможностей сервиса, работоспособности, быстродействия и поддержки. Это же соглашение должно содержать описание будущих потребностей и возможностей, чтобы все стороны понимали план развития. Соглашение об уровне обслуживания – документ, к которому могут обращаться системные администраторы в процессе разработки сервиса, чтобы убедиться, что они соответствуют ожиданиям как пользователей, так и системных администраторов и что все идет по графику.

Обсуждение соглашения об уровне обслуживания – совещательный процесс. Конечная его цель – найти компромисс между тем, чего в идеале хочет пользователь, тем, чего технически возможно добиться, тем, что позволяют финансы, и тем, что могут предоставить системные администраторы. Возможность, на разработку которой уйдут годы, нет смысла создавать для системы, если последнюю необходимо развернуть за полгода. Возможность, которая обойдется в миллион долларов, нет смысла создавать для проекта, чей бюджет составляет несколько тысяч долларов. Небольшая компания, в которой работают всего один или два системных администратора, не может позволить себе сервис поддержки, функционирующий круглыми сутками без выходных, чего бы там ни хотела сама компания. Никогда не стоит расстраиваться, если пользователь просит чего-то технически невыполнимого. Если бы пользователь знал о технологиях все, что знаете вы, он был бы системным администратором. Лучше помните, что это совещательный процесс и ваша роль в нем – все объяснить пользователю и вместе с ним придти к компромиссу.

Стартовые совещания

Хотя идея сделать все по электронной почте очень заманчива, мы считаем, что проведение хотя бы одного общего совещания в самом начале значительно упрощает ход дальнейших событий. Мы называем такие встречи стартовыми совещаниями. Проведение такого совещания на начальных стадиях процесса позволяет заложить основу успешного проекта.

Несмотря на то что личные встречи далеки от высоких технологий, они приводят к намного лучшим результатам. Электронную почту люди бегло просматривают или вообще игнорируют. Телефонные звонки не передают визуальные сигналы, облегчающие общение. На селекторных совещаниях люди зачастую отключают микрофон и просто не участвуют в обсуждении.

В стартовом совещании должны участвовать все ключевые персоны, имеющие отношение к процессу, – все **заинтересованные стороны**. Согласуйте цель нового сервиса, временные ограничения на его разработку, бюджет и обсудите основные вопросы. Все эти вопросы у вас решить не получится, но вы сможете их поставить. Нерешенные вопросы адресуйте участникам совещания.

Когда все придут к согласию, остальные встречи и совещания можно проводить по телефону или по электронной почте.

5.1.2. Эксплутационные требования

Системные администраторы должны учитывать и другие требования к новым сервисам, о которых пользователи могут не знать. Системным администраторам необходимо продумать административный интерфейс нового сервиса: будет ли он взаимодействовать с существующими сервисами и можно ли его интегрировать в центральные сервисы, такие как сервис аутентификации или каталогов.

Кроме того, системным администраторам необходимо учитывать масштабирование сервиса. Потребность в сервисе со временем может превысить изначально планируемый уровень и практически наверняка вырастет по мере роста самой компании. Системным администраторам необходимо продумать способ масштабирования действующего сервиса, не прерывая при этом его работу.

Сюда же относится и вопрос обновления сервиса. Каким будет процесс обновления при появлении новых версий? Будет ли он включать в себя перерыв в работе сервиса? Подразумевает ли он прямой доступ к каждому настольному компьютеру? Возможно ли провести обновление постепенно, протестировав его на нескольких добровольцах, прежде чем внедрять во всю сеть? Постарайтесь разработать сервис таким образом, чтобы обновление выполнялось просто, не прерывая работу сервиса, без прямого доступа к настольным компьютерам и постепенно.

Начиная с уровня надежности, ожидаемого пользователями и прогнозируемого системными администраторами как требования к будущей надежности системы, системные администраторы должны быть готовы составить перечень желательных функций, таких как кластеризация, вторичные или избыточные серверы

либо запуск на оборудовании или ОС с высокой отказоустойчивостью. Системным администраторам также потребуется продумать вопросы производительности сети в отношении сетевой инфраструктуры в месте работы сервиса и в месте расположения пользователей. Какой будет производительность сервиса, если часть пользователей будет работать удаленно, через медленное подключение с большими задержками? Есть ли способ заставить его из любого места работать одинаково хорошо либо близко к тому или для удаленных пользователей придется предусмотреть иные условия в соглашении об уровне обслуживания? Поставщики редко тестируют свою продукцию на подключениях с высокими задержками (подключениях с большим временем круговой задержки (Round-Trip Time, RTT)), и обычно все, от программистов до агентов по сбыту, в равной степени плохо представляют себе, насколько сложными могут быть проблемы. Тестирование на месте – зачастую единственный способ все проверить.

Пропускная способность или время ожидания

Термин **«пропускная способность»** означает количество данных, которое может быть передано в секунду. **Время ожидания** – это количество времени до момента, когда другая сторона примет данные. Подключение с большим временем ожидания, независимо от пропускной способности, отличается долгим временем передачи и подтверждения – между отправкой пакета и ответом о доставке. Некоторые приложения, например неинтерактивное (потоковое) видео, нечувствительны ко времени ожидания. Другие же сильно от него зависят.

Предположим, что для выполнения какой-то задачи требуется пять запросов к базе данных. Клиент посылает запрос и ожидает ответ. Это повторяется еще четыре раза. В сети Ethernet с малым временем ожидания эти пять запросов будут проходить настолько быстро, насколько сервер баз данных сможет их обрабатывать и возвращать результат. На всю задачу может потребоваться секунда. Но что будет, если этот сервер находится в Индии, а клиент выполняется на машине в Нью-Йорке? Предположим, что требуется полсекунды, прежде чем последний бит запроса дойдет до Индии. Скорость света превысить невозможно, а маршрутизаторы и прочее оборудование добавляют задержки. Теперь на ту же задачу требуется 5 с (по полсекунды на каждый запрос и ответ) плюс количество времени, которое требуется серверу на обработку запросов. Предположим, что общее время в этом случае составит 6 с. Это значительно медленнее, чем в Ethernet. Выполнение подобных задач тысячи и миллионы раз каждый день занимает значительное количество времени.

Допустим, для связи с Индией используется канал T1 (1,5 Мбит/с). Решит ли проблему расширение канала до T3 (45 Мбит/с)? Если время ожидания T3 такое же, как и T1, модернизация не улучшит ситуацию.

Решение в том, чтобы отправлять все пять запросов одновременно и ожидать прихода ответа по мере их обработки. Будет еще лучше, если удастся посылку пяти запросов заменить одной высокоуровневой операцией, которую сервер сможет выполнять локально. Например, разработчики SQL часто используют последовательности запросов для сбора данных

и вычислений по ним. Вместо этого стоит посылать более длинный SQL-запрос на сервер, собирающий данные, проводящий вычисления с ними и возвращающий только результат.

С математической точки зрения проблема заключается в следующем. Общее время на завершение операции (T) – это сумма интервалов времени, требуемых на завершение каждого запроса. Время, необходимое для завершения каждого запроса, состоит из трех интервалов: отправки запроса (S), вычисления результата (C) и получения ответа (R). Это можно выразить математически следующей формулой:

$$T = (S_1 + C_1 + R_1) + (S_2 + C_2 + R_2) + (S_3 + C_3 + R_3) + \cdots + (S_n + C_n + R_n)$$

В сетевом окружении с низким временем ожидания $S_n + R_n$ близко к нулю, что позволяет программистам этим пренебречь и, более того, свести формулу к виду

$$T = C_1 + C_2 + C_3 + C_n$$

что определенно не соответствует истине.

Программы, написанные исходя из предпосылки, что время ожидания равно или близко к нулю, показывают хорошие результаты в тестах в условиях локальной сети Ethernet, но ужасно работают в реальных условиях глобальной вычислительной сети (WAN) с высоким временем ожидания. Из-за этого программа может оказаться слишком медленной и стать непригодной к использованию. Большинство сетевых провайдеров «продают» пропускную способность, а не время ожидания. Следовательно, единственное, что могут предложить их работники службы продаж, – предоставить заказчику подключение с большей пропускной способностью, но, как мы только что продемонстрировали, увеличение пропускной способности не решает проблемы со временем ожидания. Мы видели много компаний, безрезультатно пытавшихся исправить такого рода проблемы, приобретая более широкополосные каналы.

Действенным решением может стать доработка программного обеспечения. Усовершенствование программ обычно предполагает переосмысление алгоритмов. В сетях с большим временем ожидания необходимо изменять алгоритмы таким образом, чтобы запросы и ответы не были жестко привязаны друг к другу. Один вариант решения (пакетные запросы) – отправлять все запросы одновременно, предпочтительно объединив их в малое количество пакетов, и ожидать прибытия ответа. Другой вариант (сквозные ответы) подразумевает отправку множества запросов таким образом, чтобы они не зависели от ожидания ответа. Программа должна быть способна отслеживать «сквозной поток» из n ответов с неподтвержденной передачей в любой момент.

Такие приложения, как потоковое видео и аудио, не настолько чувствительны ко времени ожидания, поскольку пакеты видео и аудио отправляются в одном направлении. Как только начинается вещание, задержка становится незаметна. Но в интерактивном обмене медиа-данными, например в голосовой связи между двумя лицами, время ожидания будет заметно как пауза между последними словами одного человека и ответом другого.

Даже если алгоритм отсылает запросы по одному и ожидает ответа, способ отправки может все изменить.

Пример: минимизация количества пакетов в сетях с большим временем ожидания

Глобальная фармацевтическая компания с центральным офисом в Нью-Джерси столкнулась с ужасными проблемами быстродействия приложения для работы с базой данных. Анализ показал, что SQL-запрос из 4000 байт отправлялся через трансатлантический канал в пятидесяти пакетах по 80 байт. Каждый пакет отправлялся только после того, как подтверждалось получение предыдущего. Только на подсоединение уходило 5 мин. Когда системные администраторы изменили конфигурацию модуля подключения к базе данных на отправку меньшего количества пакетов большего размера, проблема быстродействия исчезла. До этого разработчики пытались решить проблему с помощью дополнительного трансатлантического широкополосного канала, реализация которого заняла несколько месяцев и была очень дорогой, а результат оказался разочаровывающим, так как не дал ощутимого улучшения.

Каждый системный администратор и разработчик должен понимать, как время ожидания влияет на создаваемые сервисы. Системным администраторам также стоит выяснить, как они смогут вести мониторинг сервиса по показателям работоспособности и быстродействия. Возможность интеграции нового сервиса с существующими системами мониторинга – ключевое требование для выполнения соглашения об уровне обслуживания. Кроме того, системным администраторам и разработчикам следует выяснить, может ли система генерировать уведомления о неисправностях при обнаружении проблем в существующей системе регистрации неисправностей, если это потребуется.

Команде системных администраторов также нужно составить бюджет, который будет выделен на этот проект. Если системные администраторы не уверены, что смогут обеспечить ожидаемый пользователями уровень обслуживания в рамках текущего бюджета, это ограничение следует представить как часть обсуждения соглашения об уровне обслуживания. После утверждения соглашения об уровне обслуживания обеими группами системным администраторам нужно будет позаботиться о том, чтобы укладываться в рамки выделенного бюджета.

5.1.3. Открытая архитектура

Всегда, когда это возможно, новые сервисы следует строить, опираясь на архитектуру, которая использует **открытые** протоколы и форматы файлов. В частности, мы говорим о протоколах и форматах файлов, описание которых публично обсуждается, так что многие поставщики могут участвовать в написании этих стандартов и создавать интероперабельные продукты. Любой сервис с открытой архитектурой проще интегрировать с другими сервисами, которые следуют тем же стандартам.

Напротив, **закрытые** сервисы используют проприетарные протоколы и форматы файлов, которые способны взаимодействовать только с ограниченным

кругом решений, так как протоколы и форматы файлов могут изменяться без уведомления и требовать лицензирования у создателей протокола. Поставщики используют проприетарные протоколы, когда осваивают новую территорию или пытаются удержать свою долю рынка, препятствуя росту уровня конкуренции.

Иногда поставщики, использующие проприетарные протоколы, заключают эксплицитные лицензионные соглашения с другими поставщиками. Тем не менее обычно существует временной промежуток между выпуском новой версии у одного поставщика и выпуском совместимой версии у другого. Кроме того, отношения между двумя поставщиками могут нарушиться и они перестанут предоставлять программу сопряжения между двумя продуктами. Такая ситуация может стать настоящим кошмаром для тех, кто использует оба продукта и рассчитывает на их взаимодействие.

Протокол или продукт

Системным администраторам надо понимать разницу между протоколом и продуктом. Допустим, кто-то стандартизировал протокол Simple Mail Transport Protocol (SMTP) (Crocker 1982) для отправки электронной почты. SMTP – это не продукт, а документ на английском языке, в котором объясняется, как биты данных должны передаваться по проводам. Он отличается от продуктов, которые используют SMTP для передачи электронной почты с сервера на сервер. Путаница иногда возникает из-за того, что у компаний часто имеются внутренние стандарты, где перечисляются конкретные продукты, которые будут внедряться и поддерживаться. Это другое значение слова *«стандарт»*.

Нетрудно найти источник этой путаницы. До конца 1990-х годов, когда слово «Интернет» вошло в обиход домашних пользователей, многие люди имели дело только с протоколами, которые были привязаны к определенному продукту и не нуждались в коммуникациях с другими компаниями, так как у компаний не было возможности взаимодействовать так же свободно, как сейчас. Из-за этой ситуации распространилось мнение, что протокол – это то, что воплощено в конкретном программном пакете, а не существует самостоятельно как независимая концепция. Несмотря на то что с развитием Интернета больше людей стали узнавать о различии между протоколами и продуктами, многие поставщики попрежнему пользуются тем, что пользователи недостаточно осведомлены об открытых протоколах. Такие поставщики боятся возможной конкуренции и предпочитают бороться с конкурентами, замыкая пользователей на своих системах, затрудняющих миграцию к другим поставщикам. Эти поставщики изо всех сил стараются размывать различия между протоколом и продуктом.

Также остерегайтесь поставщиков, которые *дополняют и расширяют* стандарт, пытаясь препятствовать интероперабельности с конкурентами. Такие поставщики делают это, чтобы они могли заявить о поддержке стандарта, при этом не предоставляя своим пользователям преимуществ интероперабельности. Они не *ориентированы на нужды пользователей*. Широко известный пример подоб-

ного подхода – случай, когда компания Майкрософт внедряла систему аутентификации Kerberos, что было весьма хорошим решением, но расширила ее так, чтобы исключить возможность взаимодействия с системами Kerberos от других разработчиков. Все серверы должны были основаться на системах Майкрософт. Дополнения, сделанные Майскрософт, были бесплатны, но они заставляли заказчиков полностью отказаться от своей инфраструктуры обеспечения безопасности и заменить ее продуктами Майкрософт, если использовалась Kerberos.

С точки зрения бизнеса смысл использования открытых протоколов прост: это позволяет вам создать более качественные сервисы, потому что вы можете выбрать лучший сервер и лучший клиент, а не быть вынужденным, например, выбрать лучший клиент, а потом оказаться привязанным к менее оптимальному серверу. Люди хотят пользоваться приложением, которое соответствует их потребностям по функциональности и простоте использования. Системные администраторы хотят пользоваться приложением, которое упростит управление сервером. Эти требования зачастую противоречат друг другу. Обычно, если у пользователей или системных администраторов достаточно влияния, чтобы принять решение без согласования, другая сторона бывает удивлена решением. Если решение принимают системные администраторы, пользователи считают их фашистами. Если пользователи принимают решение, оно может стать источником многочисленных затруднений для администрирования, что впоследствии затруднит создание безупречного сервиса для пользователей.

Лучшим способом будет выбор протоколов, основанных на открытых стандартах и позволяющих каждой стороне выбрать свое собственное программное обеспечение. Такой подход позволяет отделить процесс выбора клиентского приложения от процесса выбора серверной платформы. Пользователи могут свободно выбрать программное обеспечение, наилучшим образом соответствующее их нуждам, склонностям и даже платформе. Системные администраторы могут независимо выбрать серверное решение, основываясь на своих потребностях по параметрам надежности, масштабируемости и управляемости. Системные администраторы смогут выбирать из конкурирующих серверных продуктов и не будут привязаны к потенциально трудно управляемому серверному программному обеспечению и платформе, необходимой для конкретного клиентского приложения. Во многих случаях системные администраторы смогут даже раздельно выбирать серверное оборудование и программное обеспечение, если поставщик программного обеспечения поддерживает различные аппаратные платформы.

Мы называем такую возможность разъединением выбора клиента и сервера. Открытые протоколы предоставляют свободную площадку для стимулирования конкуренции между поставщиками. Вы от этой конкуренции только выиграете.

Для сравнения следующая история иллюстрирует, что происходит, когда пользователи выбирают проприетарную систему электронной почты, которая не использует открытые протоколы, но соответствует нуждам клиентской стороны.

Опасность проприетарных почтовых программ

После длительного оценочного периода фармацевтическая компания из Нью-Джерси выбрала определенный проприетарный почтовый программный пакет для всех своих персональных компьютеров. Выбор основы-

вался на пользовательском интерфейсе и функциональности, без учета простоты управления сервером, надежности и масштабируемости. При масштабировании на большее количество пользователей система показала себя очень ненадежной. Система сохраняла все сообщения от всех пользователей в один большой файл, к которому у всех был доступ с правами на запись, что было кошмарно с точки зрения безопасности. Частые проблемы с повреждением данных привели к тому, что почтовую базу данных пришлось отправлять через Интернет поставщику для восстановления. Это означает, что потенциально уязвимая информация была открыта для посторонних лиц за пределами компании и что персонал компании не мог ожидать от электронной почты соблюдения конфиденциальности. Кроме того, это вызвало долгие простои системы электронной почты, так как ее невозможно было использовать, пока восстанавливали базу данных.

Так как программный пакет основывался не на открытых протоколах, служба поддержки системы не имела возможности выбрать конкурирующего поставщика, который мог бы предложить лучший, более безопасный и более надежный сервер. Из-за отсутствия конкуренции поставщик уделял вопросам управления сервером меньше внимания и игнорировал запросы по исправлению и улучшению, относящиеся к серверам. Если бы компания предпочла открытый протокол, а затем позволила пользователям и системным администраторам независимо выбрать программное решение для себя, это был бы наилучший вариант для всех.

Открытые протоколы и форматы файлов обычно статичны либо изменяются только с сохранением обратной совместимости и обладают широкой поддержкой, дающей максимальный выбор конечных продуктов и максимальные шансы получить надежный, интероперабельный продукт. Еще одно преимущество открытых систем в том, что вам не потребуются шлюзы для связи с остальным миром. Шлюзы – это «клей», соединяющий различные системы. Хотя шлюз может стать выходом из вашего положения, системы, основанные на общепринятых открытых протоколах, вообще не нуждаются в каких-либо шлюзах. Шлюзы – это дополнительные сервисы, которые требуют планирования мощностей, проектирования, мониторинга и всего остального, описанного в данной главе. Лучше уменьшить количество сервисов.

Шлюзы протоколов и снижение надежности

В колледже у Тома была проприетарная система электронной почты, не основанная на стандартных интернет-протоколах, таких как SMTP, а продававшаяся с программным пакетом для организации шлюза для приема и отправки почты через Интернет. В шлюзе использовался проприетарный протокол для связи с почтовым сервером и SMTP для связи с остальным миром. Этот шлюз был медленным, ненадежным и дорогим. Складывалось такое впечатление, что поставщик разрабатывал шлюз исходя из предположения, что через него будет проходить только незначительная часть почтового трафика. Шлюз был еще одним элементом,

которым надо было управлять, который надо было отлаживать, планировать для него мощности и т. д. У поставщика не было особых причин усовершенствовать шлюз, потому что он позволял пользователям связываться с системами, которые считались конкурирующими. Почтовая система много простаивала, и почти все простои случались из-за шлюза. Ни одной из этих проблем не возникло бы, если бы система использовала открытые протоколы, а не требовала шлюза.

История повторилась примерно десятилетие спустя, когда появился почтовый сервер Microsoft Exchange. В нем использовался нестандартный протокол и предлагались шлюзы для связи с другими сетями в Интернете. Эти шлюзы добавлялись к списку сервисов, которые системные администраторы должны были проектировать, конфигурировать, масштабировать, планировать для них мощности и т. д. Многие из широко известных ошибок в Exchange были связаны со шлюзом.

Эти примеры могут показаться устаревшими, так как сейчас никто не продает почтовые системы, неспособные нормально работать с Интернетом. Однако важно вспомнить эти уроки, когда в следующий раз вам попытаются продать систему управления календарем, сервис каталогов или иной продукт, который игнорирует интернет- и другие индустриальные стандарты, а взамен обещают прекрасные шлюзы за доплату или даже бесплатно. Использование стандартных протоколов подразумевает использование открытых стандартов, таких как Internet Engeniring Task Force (IETF) и Institute of Electrical and Electronic Engineers (IEEE), не зависящих от поставщика и не проприетарных. Проприетарные протоколы поставщиков приводят в будущем к серьезным проблемам. Поставщик, который предлагает шлюзы, скорее всего, не использует открытые стандарты. Если вы не уверены, прямо спросите, с какими открытыми стандартами взаимодействуют шлюзы.

5.1.4. Простота

При разработке нового сервиса прежде всего следует обращать внимание на простоту. Самое простое решение, удовлетворяющее всем требованиям, будет самым надежным, удобным в обслуживании, легко расширяемым и легко интегрируемым с другими системами. Чрезмерная сложность приводит к путанице, ошибкам и потенциальной трудности в использовании, а также может все замедлить. Сложные системы требуют больших расходов на их создание и обслуживание.

По мере своего роста система становится более сложной. Такова жизнь. Следовательно, если создавать ее как можно более простой, это позволит отсрочить день, когда система станет *слишком* сложной. Представим двух продавцов, предлагающих поставку систем. У одной системы 20 основных функций, а у другой – 200 дополнительных. Можно ожидать, что в более функциональном программном обеспечении будет больше ошибок, а у поставщика возникнет больше сложностей с поддержкой кода системы.

Иногда одно-два требования пользователей или системных администраторов могут значительно увеличить сложность системы. Если на стадии разработки

архитектуры вы столкнетесь с такими требованиями, лучше вернуться назад и провести повторную оценку важности требования. Объясните пользователям или системным администраторам, что эти требования можно удовлетворить, но только за счет снижения надежности, уровня поддержки и своевременности обслуживания. Затем попросите их заново оценить свои требования с этой точки зрения и решить, какие из них следует удовлетворить, а какими можно пренебречь.

Давайте вернемся к нашему примеру с предложением от двух продавцов. Иногда предложение с 20 основными функциями не включает в себя некоторые необходимые возможности и у вас может возникнуть желание отклонить предложение. С другой стороны, пользователи, которые понимают важность простоты, могут захотеть отказаться от некоторых возможностей ради большей надежности.

5.1.5. Отношения с поставщиком

При выборе аппаратного и программного обеспечения для сервиса у вас должна быть возможность побеседовать с техническими консультантами поставщиков, чтобы посоветоваться насчет выбора наилучшей конфигурации для вашего приложения. У поставщиков оборудования иногда бывают готовые конфигурации, оптимизированные для определенных приложений, таких как базы данных или веб-серверы. Если вы создаете типичный сервис, у вашего поставщика может найтись подходящая готовая конфигурация.

Если у вас оборудование от нескольких поставщиков серверов и у этих поставщиков есть подходящая продукция, вам следует использовать эту ситуацию с выгодой для себя. Пусть поставщики поборются за этот заказ. Так как у вас, вероятно, фиксированный бюджет, вам предоставляется возможность получить за те же деньги дополнительную функциональность, которую можно будет использовать для улучшения производительности, надежности или масштабируемости. Или вы можете добиться более выгодной цены и вложить излишки в улучшение сервиса каким-либо другим образом. Даже если вы знаете, какого поставщика выберете, не раскрывайте свой выбор до тех пор, пока не убедитесь, что добились максимально выгодных условий сделки.

При выборе поставщика, особенно программных продуктов, важно понимать, в каком направлении поставщик будет развивать продукт. Если вы крупный заказчик, у вас должна быть возможность участвовать в бета-тестировании и влиять на направление развития продукта путем согласования с руководителем проекта функций, которые могут быть для вас важны в будущем. В случае ключевых, центральных сервисов, таких как сервис аутентификации или каталогов, необходимо оставаться в русле направления развития продукта, иначе вы можете внезапно обнаружить, что поставщик перестал поддерживать вашу платформу. Ущерб от необходимости изменения центральной части инфраструктуры может быть очень велик. По возможности старайтесь налаживать постоянные отношения с поставщиками, которые в первую очередь разрабатывают продукты для платформы, используемой вами, а не с теми, кто портирует свою продукцию на эту платформу. Обычно в этом случае встречается меньше ошибок, в первую очередь добавляются новые функции и обеспечивается лучшая поддержка в продуктах, разрабатываемых для основной платформы. Меньше вероятность, что поставщик прекратит поддержку этой платформы.

5.1.6. Независимость от конкретной машины

У пользователей всегда должен быть доступ к сервису с использованием стандартного имени, основанного на назначении сервиса. Например, клиентские приложения должны находить свои общие календари на сервере `calendar`, почтовые клиенты – на POP-сервере (Myers and Rose 1996) с именем `pop`, IMAP-сервере (Crispin 1996) с именем `imap` и SMTP-сервере `mail`. Даже если некоторые из этих сервисов изначально размещаются на одной машине, доступ к ним должен предоставляться через функциональные имена, чтобы у вас была возможность масштабирования с помощью разделения сервиса на несколько машин без необходимости заново конфигурировать каждый клиент.

Основное имя машины не должно совпадать с названием функции. Например, у календарного сервера может быть основное имя `dopey`, а обращаться к нему будут как к `calendar`, но нельзя давать ему основное имя `calendar`, так как рано или поздно может потребоваться перенести функцию на другую машину. Перенос имени вместе с функцией более сложен, потому что все остальное, что привязано к основному имени (`calendar`) на первой машине, не должно перемещаться на новую машину. Управление присвоением имен и пространствами имен более подробно рассмотрено в главе 8.

Для сервисов, в которых привязка осуществляется к IP-адресам, а не к именам, обычно есть возможность выделить для машины, на которой запущен сервис, несколько виртуальных IP-адресов в дополнение к основному, настоящему IP-адресу и использовать для каждого сервиса свой виртуальный адрес. Тогда будет относительно просто перенести на другую машину виртуальный адрес вместе с сервисом.

При создании сервиса на машине продумайте, как вы будете впоследствии переносить его на другую машину. В какой-то момент кому-то придется ее переносить. По возможности максимально упростите работу этому человеку, спроектировав все как следует с самого начала.

5.1.7. Среда окружения

Надежному сервису требуется надежная среда окружения. Сервис влияет на эффективность работы ваших пользователей, напрямую либо косвенно, через другие машины и сервисы, зависящие от этого. Пользователи ожидают, что сервис будет доступен всегда, когда он им потребуется. Основная часть построения сервиса заключается в предоставлении обоснованно высокого уровня доступности, что подразумевает размещение всего оборудования, относящегося к сервису, в вычислительном центре, способном обеспечивать надежность.

Вычислительный центр обеспечивает надежное энергоснабжение, хорошее охлаждение, контролируемую влажность (что особенно важно в сухом или влажном климате), системы пожаротушения и безопасное место, где машины не могут быть случайно повреждены или отключены. Более подробно вычислительные центры рассматриваются в главе 6.

Есть и технические причины для обустройства вычислительного центра. Одна из причин размещения серверов в вычислительных центрах в том, что серверам часто требуется бóльшая скорость подключения к сети, чем клиентам, так как им необходимо связываться на приемлемой скорости с большим числом клиентов одновременно. Сервер часто бывает подключен к нескольким сетям, в том

числе и административным, с целью снижения трафика в основной сети. Высокоскоростное кабельное подключение и оборудование обычно требуют больших затрат на стадии начального развертывания, поэтому их лучше сначала устанавливать в ограниченном пространстве вычислительного центра, где их относительно недорого можно развернуть на большом количестве критически важных узлов. Все серверы, составляющие основу вашей сервиса, должны находиться в вычислительном центре, чтобы использовать преимущества высокоскоростной сети.

Ни один из компонентов сервиса не должен зависеть от каких-либо программ, выполняющихся на машинах, расположенных за пределами вычислительного центра. Сервис будет настолько надежным, насколько надежно самое слабое звено в цепи компонентов, необходимых для доступа к сервису. Компоненты на машине, находящейся в незащищенной среде, более подвержены сбоям и могут вызвать сбой всего сервиса. Если вы обнаружите зависимость от компонентов, работающих на машине за пределами вычислительного центра, найдите способ изменить ситуацию: переместите машину в вычислительный центр, продублируйте сервис на одной из машин в вычислительном центре или избавьтесь от зависимости от менее надежного сервера.

Зависимости NFS за пределами вычислительного центра

Протокол сетевой файловой системы NFS, обычно используемый в UNIX-системах, обладает возможностью приостанавливать работу клиентов во время отказа сервера до тех пор, пока он не будет восстановлен. Эта возможность полезна в ситуациях, когда лучше допустить простой, чем внести путаницу в клиентское программное обеспечение из-за отсутствия сервера или потерять данные из-за того, что сервер не отвечает.

Когда Том работал в Bell Labs, пользователь сконфигурировал свою настольную машину для работы в качестве NFS-сервера и начал предоставлять с него доступ к некоторым важным данным. Вскоре многие машины, в том числе некоторые весьма важные серверы вычислительного центра, монтировали дисковый раздел с его машины.

Потом пользователь отключил свою настольную машину и ушел в отпуск. Все машины, пытавшиеся получить доступ к данным, остановили работу, ожидая, когда настольная машина снова включится.

Именно по этой причине серверы обычно не монтируют файловые системы NFS с других серверов. В приведенном примере серверы надо было сконфигурировать так, чтобы они монтировали тома NFS только с машин, непосредственно управляемых командой системных администраторов. А в этом случае системным администраторам пришлось решать, попросить ли охрану открыть дверь офиса того работника, чтобы запустить его машину, или перезапускать все клиентские машины, в том числе несколько очень важных машин, которые не следовало перезагружать без особых причин.

В случае фундаментальных сервисов, таких как DNS-серверы, нужно особенно стараться избегать зависимостей от других систем.

Неразрешимые взаимные зависимости

Начинающая интернет-компания столкнулась с проблемой нехватки места на дисках и в целях экономии экспортировала часть свободного места на дисках настольных компьютеров под управлением UNIX через NFS. В результате этот диск был смонтирован на всех серверах, поскольку на нем размещался один из общих компонентов. После тотального сбоя в электросети, продолжавшегося дольше, чем работа источников бесперебойного питания, сеть компании больше не смогла работать. Рабочая станция не могла завершить загрузку без работающего DNS-сервера, а DNS-серверу для завершения загрузки требовался доступ к разделу NFS. Вскоре после этого компания наняла системного администратора.

5.1.8. Ограничение доступа

Представьте ситуацию: пользователь зашел в компьютерный зал, сел за клавиатуру и монитор критически важного сервера и вышел в сеть только для того, чтобы проверить почту. После этого он выключил машину, как обычный настольный компьютер. И теперь никто не сможет получить доступ к главной бухгалтерской базе данных. Возможно, вы сами сталкивались с чем-то подобным.

Ограничение прямого доступа к серверам – одна из составляющих сервиса. Доступ к машине, как консольный, так и с помощью других способов удаленного доступа, должен быть разрешен только для системных администраторов, ответственных за работу сервиса. Это ограничение важно, так как взаимодействующие с машиной пользователи могут ей дать нагрузку выше допустимой. Пользователь может вызвать сбой машины, перезагрузить ее или выключить. Хуже всего, если кто-то имеет доступ через консоль, что дает возможность получить привилегированный доступ. Например, по крайней мере одна из Windows-систем электронной почты позволяет лицу, подключившемуся через консоль, читать все электронные письма в системе.

Чем больше людей подключаются напрямую к машине, тем выше вероятность сбоя. Даже операционные системы, известные своей ненадежностью, могут месяцами стабильно работать, предоставляя сетевые сервисы, если с ними не взаимодействуют пользователи.

Человек, привыкший пользоваться конкретным сервером для нересурсоемких задач, таких как проверка почты, может случайно запустить другие программы, которые сильно нагрузят центральный процессор, память и систему ввода-вывода. Сам не понимая этого, человек может навредить сервису. Например, допустим, что сервер предоставляет сервис через NFS и пользователи начали сталкиваться с проблемами производительности NFS. Правильным действием будет подать заявку группе системных администраторов, чтобы они устранили проблемы с производительностью. Тем не менее пользователю будет легче и быстрее просто запустить обработку непосредственно на сервере. В этом случае приложение получает доступ к данным как к локальному диску, без каких-либо сетевых задержек. Человек, который имеет возможность воспользоваться сервером, скорее всего, так и поступит, не принимая во внимание вред для системы. Чем больше пользователей начнут запускать приложения на NFS-серве-

ре, тем сильнее снизится производительность сервиса NFS, она станет более нестабильной и менее надежной, и в результате все больше людей будут переносить выполнение задач непосредственно на сервер. Естественно, такая ситуация никому не выгодна. Гораздо лучше разобраться в сложившейся ситуации и начать исправлять источник проблемы, как только о ней сообщит первый пользователь.

Мы рекомендуем с самого начала ограничить доступ к серверам для всех, кроме системных администраторов.

5.1.9. Надежность

Наряду с вопросами среды окружения и доступа есть еще несколько моментов в отношении надежности, которые следует учитывать при планировании сервиса. В главе 4 мы объясняли, как создать более надежный отдельный сервер. Надежность серверов как компонентов сервиса – еще один аспект повышения надежности сервиса в целом.

Если у вас есть избыточное оборудование, используйте его по возможности эффективно. Например, если в системе два блока питания, подключите их к разным электрическим сетям и разным розеткам. Если у вас есть избыточные машины, по возможности используйте раздельное подключение к питанию и к сети, например к разным коммутаторам. В конце концов, если сервис должен быть доступен из разных сетей, подумайте о размещении избыточных систем в другой сети, чтобы использовать их как запасные в случае критического сбоя в основной сети.

Все компоненты каждого сервиса, кроме избыточных элементов, должны быть плотно взаимосвязаны, использовать одни и те же источники питания и сетевую инфраструктуру, чтобы сервис в целом, насколько это возможно, зависел от наименьшего числа компонентов. Рассеивание неизбыточных компонентов по многочисленным частям инфраструктуры просто приведет к тому, что у сервиса будет больше вероятных точек неисправностей, каждая из которых может вызвать отказ всего сервиса. Например, предположим, что развернут сервис удаленного доступа и часть этого сервиса – новая, более безопасная система аутентификации и авторизации. Система конструктивно состоит из трех компонентов: модуля удаленных подключений, сервера, проверяющего, что подключающиеся – те, за кого себя выдают (аутентификация), и сервера, который определяет, к каким сегментам им разрешен доступ (авторизация). Если три компонента получают питание от разных источников, выход из строя любого источника питания вызовет отказ всего сервиса. Каждый из них – вероятная точка сбоя. Если они питаются от одного источника, сбой других источников питания на них не повлияет. Аналогично, если они подключены к одному сетевому коммутатору, только выход из строя этого коммутатора вызовет отказ сервиса. С другой стороны, если они разбросаны по трем сетям с множеством различных коммутаторов и маршрутизаторов, участвующих в связи между компонентами, гораздо больше компонентов могут выйти из строя и вызвать отказ сервиса.

Наиболее эффективный способ добиться максимальной надежности сервиса – сделать его настолько простым, насколько это возможно. Найдите самое простое решение, которое соответствует всем требованиям. При оценке надежности создаваемого вами сервиса разбейте его на составные части и изучите зависимости и степень надежности каждой из них, пока не добьетесь набора серверов

и сервисов, которые ни от чего больше не зависят. Например, многие сервисы зависят от сервиса имен, такого как DNS. Насколько надежен ваш сервис имен? Зависят ли ваши серверы имен от других серверов и сервисов? Также в число распространенных центральных сервисов входят сервисы аутентификации и каталогов.

Наверняка одним из компонентов вашей системы является сеть. Когда вы создаете централизованный сервис с удаленным доступом к нему, особенно важно учитывать в расчетах топологию сети. Будет ли сервис доступен для удаленных сетей при отказе связи с главной сетью? Имеет ли смысл в таких случаях предоставление доступа для удаленных сетей? Каковы расходы на это? Есть ли проблемы с восстановлением синхронизации? Например, сервис имен должен оставаться доступным для обеих сторон при затрудненной связи, так как многое из того, от чего зависят люди в удаленной сети, находится только на машинах этой сети. Но люди не смогут ничего сделать, если им не обеспечить разрешение имен. Даже если база данных их сервера имен не получает обновлений, устаревшая база данных по-прежнему будет полезна. Если у вас организован централизованный сервис аутентификации удаленного доступа с системами удаленного доступа в других офисах, возможно, у этих систем удаленного доступа должна оставаться возможность аутентификации людей, подключающихся к ним, даже при отказе связи с центральным сервером. И в том и в другом случае в программном обеспечении должна быть заложена возможность предоставления вторичных серверов в удаленных офисах и возобновления синхронизации баз данных после восстановления подключения. Однако, если вы создаете большую базу данных или файл-сервер, обеспечить доступ удаленных офисов к сервису в случае отказа связи практически нереально.

При **частичном отказе** по-прежнему предоставляется частичная функциональность. Например, при отказе DNS-сервера пользователи продолжат работу, хотя иногда несколько медленнее или с потерей отдельных функций.

При **полном отказе**, с другой стороны, нарушается работа всех сервисов, из-за чего останавливается вся работа. Лучше группировать пользователей, сервисы и серверы таким образом, чтобы полный отказ сервиса нарушал работу только отдельных групп пользователей, а не всех сразу. Интересный момент в работе компьютеров – то, что в случае отказа критически важной функции, такой как NFS, зачастую становится невозможной любая работа. Таким образом, 90% функциональности могут быть равны 0% функциональности. Ограничьте 10-процентный отказ отдельной частью сети.

Например, отказ NFS-сервера останавливает работу всех активно подключенных клиентских приложений. Предположим, что у нас три группы пользователей и три NFS-сервера. Если данные пользователей распределяются по файловым серверам случайным образом, отказ одного файлового сервера повлияет на всех пользователей. С другой стороны, если каждая группа пользователей ограничена отдельным файловым сервером, в худшем случае только одна треть пользователей не сможет продолжать работу во время простоя.

Группировка кабелей питания

Ту же методику можно применить к подключению оборудования. Начинающий системный администратор очень гордился тем, как аккуратно он подключил новую группу серверов. В каждом сервере было три ком-

понента: центральный процессор, внешние жесткие диски и монитор. Одна линия питания обеспечивала все процессоры, другая – все жесткие диски, и третья – все мониторы. Каждый кабель был аккуратно проложен и закреплен скобами – выглядело это очень хорошо. Наставник похвалил его за аккуратную работу, но, зная, что серверы еще не эксплуатируются, воспользовался случаем и отключил линию питания всех дисков. Все серверы вышли из строя. Системный администратор запомнил этот урок: лучше подключать отдельную линию электропитания ко всем компонентам машины. Выход из строя любой из линий электропитания вызовет отказ одной трети устройств. В обоих случаях отключится одна треть компонентов, но в последнем случае только одна треть сервиса будет недоступна.

Сценарии входа в систему в Windows

Еще один пример надежности группировки относится к проектированию сценариев входа в систему в MS Windows. Все, что требуется сценарию, должно быть на том же сервере, что и сценарий. Соответственно, сценарий не нуждается в проверке работоспособности сервера. Если пользователи используют сценарии входа в систему от разных серверов, следует продублировать на всех серверах то, к чему у сценария должен быть доступ, а не создавать множество зависимостей.

5.1.10. Один сервер или несколько

Независимые сервисы, или демоны, всегда должны находиться на отдельных машинах, если позволяет уровень финансирования и количество персонала. Тем не менее, если создаваемый вами сервис объединен более чем с одним новым приложением или демоном, связь с которыми осуществляется через сеть, вам придется подумать, размещать ли все компоненты на одной машине или разделить их между несколькими машинами.

Этот выбор может быть обусловлен соображениями безопасности, производительности или масштабируемости. Например, если вы создаете веб-сайт с базой данных, вам придется разместить базу данных на отдельной машине, чтобы вы могли настроить доступ к базе данных, защитить ее от несанкционированного доступа из Интернета и расширить внешний интерфейс вашего сервиса за счет подключения дополнительных веб-серверов, не затрагивая машину с базой данных.

В других случаях один из компонентов с самого начала предназначен только для одного приложения, но впоследствии может использоваться и другими приложениями. Допустим, вам нужно подготовить календарный сервис, использующий LDAP-сервер каталогов (Yeong, Howes and Kille 1995), и это первый сервис с использованием LDAP. Должны ли календарный сервер и сервер каталогов размещаться на одной или на разных машинах? Если такой сервис, как LDAP, может быть впоследствии использован другими приложениями, он должен размещаться на выделенной машине, а не на общей, чтобы календарный

сервис мог обновляться и дополняться независимо от значительно более важного сервиса LDAP.

Иногда два приложения или демона могут быть полностью взаимосвязаны и никогда не использоваться отдельно. В этой ситуации при прочих равных условиях имеет смысл размещать их на одной машине, чтобы сервис зависел только от одной машины, а не от двух.

5.1.11. Централизация и стандарты

Еще один элемент построения сервиса – централизация инструментария, приложений и сервисов, необходимых вашим пользователям. Централизация подразумевает, что инструментарий, приложения и сервис управляются в первую очередь центральной группой системных администраторов на едином центральном наборе серверов, а не многочисленными корпоративными группами, дублирующими работу друг друга и закупающими собственные серверы. Поддержку этих сервисов предоставляет центральная служба поддержки. Централизация сервисов и создание их стандартными способами упрощает поддержку и снижает затраты на обучение персонала.

Чтобы предоставлять должную поддержку любых сервисов, на которую рассчитывают пользователи, команда системных администраторов в целом должна хорошо в них разбираться. Это означает, что каждый сервис должен быть правильно интегрирован в работу службы поддержки и по возможности везде использовать стандартное оборудование вашего поставщика. Сервис должен разрабатываться и документироваться неизменным способом, чтобы системные администраторы, отвечающие на звонки в службу поддержки, знали, где что находится, и, соответственно, могли быстрее реагировать. Поддержка нескольких копий одного сервиса может быть более сложной. Придется предоставить работникам службы поддержки способ определять, например, к какому серверу печати подключен конкретный пользователь, обратившийся с заявкой.

Общая централизация не отменяет централизации на уровне региональных или организационных подразделений, в особенности если в каждом регионе или организации есть своя служба поддержки. Некоторые сервисы, такие как электронная почта, аутентификация и сети, являются частями инфраструктуры и должны быть централизованными. В крупных компаниях эти сервисы могут быть созданы вокруг центрального ядра, обменивающегося информацией с распределенными региональными или организационными системами. Для других, таких как файловые серверы и процессорные фермы, более естественной будет централизация на уровне подразделений.

5.1.12. Производительность

Никому не нравятся медленные сервисы, даже если они обладают весьма впечатляющими возможностями. С точки зрения пользователя, в любом сервисе важны два фактора: работает ли он[1] и если да, то насколько быстро. При разработке сервиса вам придется уделить внимание характеристикам его производительности, даже если потребуется преодолеть массу других сложных техничес-

[1] В понятие «*работает*» входит надежность, функциональность и пользовательский интерфейс.

ких задач. Если вы решите все сложные проблемы, но сервис получится медленным, его пользователи не оценят ваши усилия.

По мере роста скоростей процессоров, сетевого и видеооборудования возрастают ожидания в отношении производительности. Приемлемая производительность сегодня не может быть такой же, как полгода или год назад. Помните об этом при разработке системы. Следует стремиться к тому, чтобы в течение нескольких лет вам не потребовалась модернизация. Вам хватит и других забот. Вам нужна машина, которая не обесценится слишком быстро.

Для создания сервиса с достойной производительностью вы должны понимать, как он устроен, и, возможно, найти способы эффективно разделить его между несколькими машинами. С самого начала вы также должны учитывать, как будет масштабироваться производительность начальной системы по мере роста нагрузки и ожиданий от нее.

Во время **тестирования нагрузки** вы создаете искусственную нагрузку на сервис и следите за ее реакцией. Например, сгенерируйте 100 обращений в секунду к веб-серверу и измеряйте время ожидания или общее время на обработку отдельного запроса. Затем сгенерируйте 200 обращений в секунду и посмотрите, как это скажется на поведении сервиса. Увеличивайте количество обращений до тех пор, пока не увидите, какую нагрузку может выдержать сервис, прежде чем время отклика станет неприемлемым.

Если ваше тестирование показывает, что система работает нормально с несколькими пользователями одновременно, то сколько ресурсов (оперативной памяти, систем ввода-вывода и т. д.) потребуется, когда сервис будет введен в строй и его станут использовать сотни или тысячи пользователей одновременно? Ваш поставщик, скорее всего, поможет вам с приблизительной оценкой, но по возможности постарайтесь проводить свои тесты. Не стоит ожидать безупречной точности от прогнозов поставщика на тему того, как ваша организация будет использовать его продукцию.

Плохое планирование мощностей – плохое первое впечатление

Всегда приобретайте серверы с достаточно большим запасом мощности, которые справятся с пиковой нагрузкой и растущим числом пользователей. Новая система электронных квитанций, развернутая в одной сети, была моментально перегружена большим количеством одновременно обращающихся к ней пользователей. Пользователи, испытавшие систему, сочли ее невероятно медленной и ненадежной и вернулись к старому бумажному методу. В этой ситуации сложилось плохое первое впечатление о сервисе. Было отправлено сообщение, в котором говорилось, что был проведен анализ причин и что системе требуется больше оперативной памяти, которую быстро предоставят. Даже когда была доставлена новая оперативная память, пользователи не приняли новую систему, поскольку все «знали», что она слишком медленная и ненадежная. Они предпочли не менять систему, в работоспособности которой были уверены.

Эта система могла сэкономить миллионы долларов в год, но руководство решило сэкономить на приобретении дополнительной оперативной па-

мяти для системы. Финансовая группа рассчитывала на то, что новая система приобретет широкую популярность и станет в будущем основой многочисленных приложений, но производительность изначально была недостаточной и не оставалось запаса для роста. Новый сервис был широко разрекламирован внутри финансовой группы, так что для них не должно быть ничего удивительного в том, что число пользователей росло не постепенно, а большое количество людей попыталось воспользоваться сервисом в первый же день. В результате финансовая группа решила резко внедрить новый сервис, вместо того чтобы постепенно развертывать его в подразделениях компании (более подробно с разных сторон эта тема будет рассмотрена в разделе 19.1.6). На этом опыте финансовая группа многому научилась в области внедрения новых электронных сервисов. Что более важно, группа на собственном опыте убедилась, что пользователи «обжегшись на молоке, дуют на воду». Очень сложно заставить пользователей принять сервис, который однажды их уже подвел.

При выборе машин для запуска сервиса учитывайте особенности работы сервиса. Есть ли в нем процессы, часто обращающиеся к диску? Если есть, выбирайте для этих процессов серверы с быстрой дисковой системой ввода-вывода и быстрыми дисками. Для дальнейшей оптимизации определите, какая операция чаще требуется при обращении к диску: чтение или запись? Если сервис держит в памяти большие таблицы с данными, ищите серверы с большим количеством быстрой памяти и большим кэшем. Если сетевой сервис обменивается большим количеством данных с клиентами или между серверами сервиса, приобретите побольше высокоскоростных сетевых интерфейсов и изыскивайте способы распределения трафика между интерфейсами. Это можно сделать с помощью отдельной сети для связи между серверами, или выделенных сетевых интерфейсов для ключевых клиентских сетей, или используя технологию, позволяющую клиенту прозрачно подключаться к ближайшему сетевому интерфейсу. Также обратите внимание на возможности кластеризации и устройства, позволяющие создавать свободно связанные кластеры либо машины, на которых запущены одинаковые сервисы, представляемые как единое целое.

Производительность сервиса для удаленных сетей тоже может вызвать затруднения из-за подключения с низкой пропускной способностью и высоким временем ожидания (в разделе 5.1.2 приведены рекомендации по поводу времени ожидания). Если сервис генерирует большое количество сетевого трафика, то вам придется находить нестандартные решения для достижения достаточной производительности при удаленных подключениях к нему, особенно если сервис разрабатывался без учета возможности размещения одного-двух серверов в каждой удаленной сети. В некоторых случаях для достижения приемлемой производительности достаточно будет интеллектуальных механизмов управления очередью или качества сервиса (QoS). В других случаях вам может потребоваться найти способы уменьшения сетевого трафика.

Производительность в удаленных сетях

Крупная компания заказала сторонним компаниям часть функций поддержки пользователей, в том числе поддержку оборудования. Компании было нужно предоставить людям в нескольких отделениях по всему миру интерактивный доступ к системе поддержки пользователей и пользовательскому сервису заказа запасных компонентов. В обоих сервисах был графический интерфейс, работающий на клиентском компьютере и обращающийся к серверам. До этого и клиенты, и серверы находились в одной филиальной сети, но теперь появились очень удаленные подключения.

Одно из приложений передавало на клиентский дисплей огромные растровые изображения вместо небольших объемов данных, которые затем могла отображать клиентская программа. Например, отправлялось растровое изображение того, как должно выглядеть окно, вместо кратких инструкций о размещении кнопки здесь, текстовой строки там и т. д. Эта функция серверного программного обеспечения делала обычную клиент–серверную конфигурацию совершенно бесполезной на медленных каналах. Разработчики сервиса обнаружили, что можно запускать клиентское приложение на машине в той же сети, что и сервер, и удаленно отображать результаты, передаваемые через глобальную сеть на настольный компьютер конечного пользователя, улучшив тем самым интерактивную производительность для конечного пользователя. Поэтому они закупили несколько машин серверного класса для работы в роли клиентских машин в центральной сети. Реальные клиенты подключались к этим машинам, которые отображали клиентам результаты через глобальную сеть, достигая приемлемой производительности.

Проблемы производительности на глобальных каналах и решение, позволившее достичь приемлемой производительности, были найдены во время систематического тестирования ранних прототипов проекта. Если бы эти проблемы были обнаружены в последний момент, внедрение проекта значительно задержалось бы, так как потребовалось бы полностью перепроектировать всю систему, в том числе системы безопасности. Если бы это было обнаружено после начала обслуживания конечных пользователей сервиса, проект наверняка провалился бы.

5.1.13. Мониторинг

Сервис не готов и не имеет права называться сервисом до тех пор, пока не налажен мониторинг производительности, проблем, работоспособности и не внедрены механизмы планирования мощностей (мониторинг – тема главы 22).

Служба поддержки или оперативная группа поддержки должна автоматически получать оповещения о проблемах сервиса, чтобы начать их исправлять до того, как они затронут слишком большое количество людей. Если пользователь постоянно обнаруживает крупные проблемы с сервисом и должен звонить, чтобы

сообщить о них, прежде чем кто-либо начнет разбираться с проблемой, это производит впечатление очень низкого стандарта обслуживания. Пользователи не должны чувствовать, что проблемы системы волнуют только их. С другой стороны, проблемы, которые вы обнаружили и устранили до того, как их заметили, похожи на звук упавших в лесу деревьев, который некому было услышать. Например, если на выходных произошел отказ системы, вы были вовремя оповещены и успели все исправить до утра понедельника, то ваши пользователи даже не поинтересуются, было ли что-то не так (в этом случае можно сообщить о решении проблемы по электронной почте, что повысит доверие к вам, раздел 31.2).

Аналогично, группа системных администраторов должна вести упреждающий мониторинг сервиса с точки зрения планирования мощностей. В зависимости от типа сервиса, в планирование мощностей может включаться пропускная способность сети, производительность сервера, скорость транзакций, лицензии и доступность физических устройств. Кроме того, системные администраторы должны обоснованно прогнозировать и планировать возможности роста сервиса. Чтобы делать это эффективно, мониторинг использования должен быть неотъемлемой частью сервиса.

5.1.14. Разворачивание сервиса

То, как среди пользователей будет внедряться новый сервис, так же важно, как и то, как система разрабатывалась. От внедрения и от первых впечатлений пользователей зависит, как в дальнейшем будет восприниматься сервис. Так что постарайтесь, чтобы первые впечатления были положительными.

В числе ключевых моментов создания хорошего впечатления – готовность документации, ознакомленная с новым сервисом и хорошо подготовленная служба поддержки и проработанные процедуры поддержки. Нет ничего хуже, чем столкнуться с проблемой в новом приложении и, обратившись за помощью, обнаружить, что никто ничего не знает.

Процесс внедрения также включает в себя создание и тестирование механизма установки нового программного обеспечения или необходимых настроек конфигурации на каждый настольный компьютер. Используйте методы внедрения нового программного обеспечения на настольных компьютерах (раздел 3.1.2), в том числе методику постепенного развертывания «одна, несколько, много», где все начинается со специально отобранных тестовых групп, численность которых постепенно увеличивается. В идеале сервису не должно требоваться новое программное обеспечение или конфигурирование настольных компьютеров, потому что это более удобно для пользователей и снижает необходимость обслуживания, но зачастую установка новых клиентских программ на настольные компьютеры необходима.

5.2. Тонкости

Помимо того что создаваемый вами сервис должен быть надежным, отслеживаемым, простым в обслуживании и поддержке, соответствующим всем основным вашим требованиям и требованиям пользователей, необходимо учитывать и некоторые другие аспекты. Если это возможно, для каждого сервиса стоит использовать выделенные машины. Это значительно упрощает обслуживание

и поддержку сервисов. В крупных компаниях использование выделенных машин – одна из основ. Для небольших компаний стоимость установки выделенных машин может быть чрезмерно высокой.

Еще один идеал, к которому стоит стремиться при создании сервисов, – добиться для них полной избыточности. Некоторые сервисы являются настолько важными, что полная избыточность для них – это необходимость, не зависящая от размера компании. По мере роста компании вы должны стремиться к полной избыточности и других сервисов.

5.2.1. Выделенные машины

В идеале сервис необходимо создавать на выделенных машинах. В крупных сетях такая структура может быть оправдана на основе требований к сервисам. Однако в небольших сетях целесообразность такого шага будет значительно менее очевидной. Наличие выделенных машин для каждого сервиса повышает надежность сервисов, упрощает отладку при возникновении каких-либо проблем с надежностью, снижает масштаб простоев, а также намного упрощает модернизацию и планирование мощностей.

В растущих корпоративных сетях, как правило, выделяется одна центральная административная машина, являющаяся ядром всех критически важных сервисов. Она предоставляет сервисы имен, аутентификации, печати, электронной почты и т. д. В результате из-за увеличения нагрузки эту машину приходится разделять, а сервисы – распределять по нескольким серверам. Зачастую к тому времени, как системным администраторам удается добиться финансирования для дополнительных административных машин, эта машина уже настолько загружена сервисами и зависимостями, что разделить ее очень сложно.

Сложнее всего при распределении сервисов с одной машины на несколько разобраться с зависимостями IP-адресов. Некоторые сервисы подразумевают жестко запрограммированные на всех пользователей IP-адреса. В конфигурации многих сетевых продуктов, таких как брандмауэры и маршрутизаторы, IP-адреса жестко запрограммированы в их конфигурации.

Разделение центральной машины

Synopsys, будучи еще небольшой компанией, начинала с типичной конфигурации одной центральной административной машины. Она играла роль NIS-мастера (Network Information Service,), DNS-мастера, сервера времени, принт-сервера, консольного сервера, почтового сервера, SOCKS-релея, сервера аутентификации аппаратных ключей, загрузочного сервера, административного узла NetApp, файлового сервера, CAP-сервера (Columbia Appletalk Protocol) и т. д. Кроме того, во всем машинном зале только у этой машины имелись клавиатура и монитор, поэтому именно ее были вынуждены использовать системные администраторы, если им нужно было работать в зале. По мере того как компания росла, появились новые системные администраторы, которые использовали ПО консольного сервера для доступа к консолям других узлов. Время от времени один из новых системных администраторов случайно вводил команду `halt` на центральном сервере, вместо того чтобы использовать соответст-

вующую команду для отправки сообщения `halt` через ПО консольного сервера. Так как все зависело от этой конкретной машины, подобные несчастные случаи разом останавливали работу всей компании.

Пришло время разделить функциональность машины на несколько серверов. Причиной этому стали не только случайные ошибки, но и все нарастающие перегруженность и нестабильность машины. На данный момент на центральной машине было запущено столько сервисов, что одно только выяснение, какие это сервисы, само по себе составляло непростую задачу.

Основные NIS- и DNS-сервисы были перенесены на три машины с множеством сетевых интерфейсов, в результате чего к каждой сети было подключено две таких машины. Другие сервисы были перенесены на дополнительные машины. При этом каждая новая машина стала основной машиной для одного сервиса и вторичной для другого. Перенос некоторых сервисов было достаточно просто осуществить, так как они были связаны с именами сервисов. Перенести другие сервисы было сложнее, так как они были привязаны к IP-адресам. В некоторых случаях на машинах в других отделах компании была задана зависимость от реального имени узла, а не от имени сервиса.

Спустя несколько лет первая центральная машина все еще существовала, хотя ее важность и перегруженность были значительно снижены по мере того, как системные администраторы продолжали отслеживание зависимостей, которые удаленные отделения компании нестандартным образом встроили в свои локальные инфраструктурные серверы и настольные компьютеры.

Разделение узла, имеющего вселенскую важность, на несколько разных узлов – очень сложная задача. И чем дольше такой узел существует, чем больше сервисов на нем создается, тем сложнее становится такая задача. В этом случае может помочь использование имен, основанных на названиях сервисов, однако их необходимо стандартизировать и внедрить эти стандарты во все отделения компании.

5.2.2. Полная избыточность

Наличие дублирующего сервера или набора серверов, которые готовы принять на себя роль основных серверов в случае сбоя, называется **полной избыточностью**. В случае сбоя переход роли основного сервиса к вторичному может проводиться несколькими способами: потребуется вмешательство человека, переход может быть автоматическим при сбое основного сервера или основной и вторичный серверы разделят нагрузку до отказа одного из них, после чего оставшийся сервер возьмет на себя всю рабочую нагрузку.

Тип используемой вами избыточности будет зависеть от самого сервиса. Некоторые сервисы, такие как веб-серверы и вычислительные фермы, прекрасно запускаются на крупных фермах клонированных машин. Другие сервисы, такие как огромные базы данных, – наоборот. Последние требуют более тесно связанной системы преодоления отказа. Программное обеспечение, которое вы исполь-

зуете для предоставления сервиса, может потребовать избыточности в виде постоянно подключенного пассивного подчиненного сервера, который реагирует на запросы только в случае отказа основного сервера. В любом случае механизм избыточности должен обеспечивать синхронизацию данных и поддерживать их целостность.

В крупных фермах клонированных серверов и в других случаях, когда избыточные серверы постоянно работают параллельно с основными, избыточные машины можно использовать для распределения нагрузки и увеличения быстродействия при безотказной работе. Если вы используете этот подход, будьте осторожны и не позволяйте нагрузке достигнуть точки, при которой производительность стала бы неприемлемой в случае отказа одного из серверов. Добавьте еще несколько серверов параллельно существующим, прежде чем такая точка будет достигнута.

Некоторые сервисы являются неотъемлемой частью ежеминутного функционирования сети, поэтому их полная избыточность обеспечивается на самых ранних стадиях создания этой сети. Другие сервисы в этом отношении игнорируются до тех пор, пока сеть не достигнет очень крупных размеров или не произойдет серьезный, заметный сбой такого сервиса.

Для сервисов имен и аутентификации, как правило, полная избыточность создается в первую очередь, частично из-за того, что программное обеспечение разработано для вторичных серверов, и частично из-за их критической важности. Для других критических сервисов, таких как электронная почта, печать и сеть, избыточность создается гораздо позже, так как полную избыточность для таких сервисов создать сложнее и дороже.

Как и в случае с любыми другими аспектами, определите, полная избыточность каких сервисов принесет вашим сотрудникам наибольшую пользу, а затем начните именно с этих сервисов.

Пример: разработка надежного почтового сервиса

Боб Фландрена (Bob Flandrena) разработал интересный способ избыточности для входящей и исходящей электронной почты в Bell Labs. Почта, поступающая из Интернета, загружалась на группу машин, защищенных брандмауэром, а затем переправлялась на соответствующий внутренний почтовый сервер. Если брандмауэр не работал, внешняя машина создавала очередь почтовых сообщений. На этой внешней машине было создано крупное хранилище, способное вместить почту за пару дней. Ведение журналов, спам-контроль и различные вопросы безопасности, таким образом, решались на небольшом количестве внутренних узлов, которые гарантированно просматривали все входящие письма.

Внутренние почтовые серверы направляли письма друг другу. Однако их конфигурация была упрощена благодаря тому факту, что более сложные решения маршрутизации принимались двумя почтовыми узлами, защищенными брандмауэром. Эти узлы отличались более сложной конфигурацией и могли определить, нужно ли направлять почту в Интернет.

Исходящие письма (отправляемые в Интернет) почтовые узлы отправляли на два избыточных узла, находящихся за пределами брандмауэра

и выделенных для повторных попыток отправки почты на внешние доменные имена. Интернет был ненадежным, и повторные попытки работы с почтой стали тяжелым бременем. На почтовых узлах было создано хранилище достаточно большого объема на случай отсутствия доступа к внешним релеям. Такое же хранилище было создано на внешних машинах на случай неудачных попыток отправить почту в течение долгого времени.

Настройки брандмауэра позволяли пропускать только трафик с исходящей почтой (SMTP) с почтовых узлов на внешние релеи. Для входящей почты были разрешены только соответствующие пути. Все эти узлы включали в себя одно и то же оборудование и программное обеспечение с незначительными различиями в конфигурации. В наличии всегда имелся дополнительный набор оборудования, чтобы в случае отказа узла его можно было быстро заменить.

Система работала медленнее при отказе одного из узлов, но, пока функционировал брандмауэр, функционировала и почта. При отказе брандмауэра помещение входящей и исходящей почты в хранилище могло быть остановлено только в том случае, если бы все избыточные системы одновременно дали сбой.

Эта система отлично поддавалась масштабированию. Проводился независимый мониторинг каждого потенциально узкого места. Если оно начинало перегружаться, простое добавление узлов и соответствующие записи DNS MX повышали пропускную способность. Конструкция системы была простой, четкой, надежной и легкой в поддержке.

Единственными точками, которые могли дать сбой, были узлы доставки почты внутри компании. Однако отказ одного из них влиял только на определенный отдел компании. А добиться этого было сложнее всего.

Еще одно преимущество подобной избыточности – **упрощение модернизации**. Она позволяла провести постепенную модернизацию. Все узлы по одному отключаются, обновляются, тестируются и заново подключаются. Простой одного узла не нарушает работу всего сервиса, хотя и может сказаться на его быстродействии.

5.2.3. Потоковый анализ для масштабирования

Если вы представляете себе отдельные компоненты типичной транзакции в сервисе, вы сможете масштабировать сервис более точно и эффективно. Опыт Страты в создании масштабируемых интернет-сервисов для интернет- и ASP-провайдеров позволил ей создать потоковую модель для отдельных транзакций и объединить их в электронные таблицы, чтобы получить общую потоковую картину. На самом деле все это намного проще, чем представляется на первый взгляд.

Потоковая модель – просто список транзакций и их зависимостей со всей информацией, которую можно получить об использовании ресурсов по каждой транзакции. Эта информация может включать в себя объем памяти, используемой на сервере этой транзакции; размер и количество пакетов, используемых

в транзакции; количество открытых сокетов, используемых для обслуживания транзакции, и т. д.

При моделировании отдельной служебной транзакции с помощью потоковой модели включаются все детали, необходимые для проведения транзакции, даже такие, как поиск интернет-имен через DNS, чтобы получить истинную картину транзакции. Даже внешние аспекты, на которые вы не можете влиять, такие как поведение корневых DNS-серверов, могут воздействовать на то, что вы пытаетесь моделировать. Если узкое место транзакции обнаруживается, например, на стадии поиска имен, вы можете запустить внутренний кэширующий сервер имен, сэкономив тем самым часть времени на внешний поиск. В сетях, где сохраняют и анализируют отчеты веб-сервисов или других видов внешнего доступа, постоянно так делают, и это ускоряет ведение отчетов. Еще больше можно ускорить этот процесс, просто регистрируя IP-адреса внешних узлов и проводя поиск имен на стадии последующей обработки для анализа.

Приятный момент в работе сервисов заключается в том, что они обычно основаны на транзакциях. Даже передача файлов состоит из множества транзакций чтения и записи блоков по сети. Главное, о чем следует помнить при создании потоковой модели, – транзакции сервисов практически всегда зависят от транзакций инфраструктуры. При исследовании проблем с масштабированием сервиса постоянно выясняется, что узкое место сервиса – где-то в инфраструктуре.

Когда потоковая модель точно изображает сервис, вы можете локализовать проблемы производительности и масштабируемости, увидев, какая часть модели потоков данных является слабым звеном, провести мониторинг этого участка в реальных или искусственно созданных условиях и посмотреть, как он функционирует или дает сбой. Например, если ваша база данных способна обрабатывать 100 запросов в секунду и вы знаете, что каждый доступ к домашней странице вашего сайта требует трех запросов из базы данных, вы можете прогнозировать, что ваш сайт будет работать только при нагрузке не более 33 переходов в секунду. Зато теперь вы знаете, что можно увеличить производительность базы данных до 200 запросов в секунду (возможно, продублировав ее на втором сервере и разделив запросы между ними) и сайт сможет обрабатывать вдвое больше переходов в секунду при условии, что не помешают другие узкие места.

Ресурсы сервера тоже могут стать проблемой. Предположим, что сервер предоставляет доступ к электронной почте по протоколу IMAP. Возможно, вам известно из непосредственных наблюдений или из документации поставщика, что каждому пользователю, подключающемуся к серверу, требуется около 300 Кб оперативной памяти. Просмотрев отчеты, вы можете понять типичное распределение использования сервера: какая часть от общего числа посетителей сервера использует его одновременно в разное время суток.

Знание количества людей, использующих сервис, – только часть процесса. Чтобы проанализировать ресурсы, вам также придется выяснить, загружает ли процесс IMAP в память сервера файловые индексы, или что-то другое, или даже все содержимое почтового ящика. Если так, вам нужно узнать средний размер загружаемых данных, который может быть вычислен как среднее арифметическое размера пользовательских файловых индексов, как средняя линия или медиана участка кривой размера файлов, на котором находится большинство файловых индексов, или даже путем учета только тех файловых индексов, которые используются в период максимальной нагрузки и проведения тех же

вычислений с ними. Выберите тот способ, который кажется более подходящим для вашего приложения. Можно использовать систему мониторинга для проверки вашего прогноза. Таким образом можно обнаружить неожиданные моменты, например что средний объем почтового ящика растет быстрее, чем ожидалось. Это может отразиться на размере файловых индексов и, следовательно, на производительности.

Наконец вернитесь назад и проделайте такой же анализ на всех этапах движения потока данных. Если настольный компьютер пользователя делает внутренние запросы для поиска имен, чтобы найти почтовый сервер, вместо того чтобы кэшировать информацию о том, где его можно найти, следует это включить в анализ потока данных как нагрузку на сервер имен. Может быть, сотрудник использует веб-почту, тогда он использует ресурсы веб-сервера, программное обеспечение которого затем создает IMAP-подключение к почтовому серверу. В таком случае возможно выполнение не менее двух запросов на поиск имен за одну транзакцию, так как пользовательский настольный компьютер сначала ищет веб-сервер, а тот, в свою очередь, ищет IMAP-сервер. Если веб-сервер проводит локальную аутентификацию и передает подтверждение на IMAP-сервер, возникает дополнительный поиск имени сервера каталогов, а затем транзакция с каталогами.

Потоковая модель работает на всех уровнях масштабирования. Вы можете успешно спроектировать модернизацию сервера для отдела с тридцатью сотрудниками или кластеры мультимедийного сервиса для трех миллионов пользователей одновременно. Чтобы получить точные цифры, которые вам нужны для крупномасштабного планирования, можно использовать анализ трафика тестовой установки, а также информацию от поставщика, отслеживание системы и т. д.

Пример анализа потоковой модели

Когда-то Страта управляла большим количеством настольных компьютеров, получающих доступ к группе файловых серверов по сети. Изучалась претензия по поводу медленного открытия файлов, но сеть не была перегружена, как не было и необычного количества повторных передач или задержек в файлах статистики файловых серверов на узлах, предоставляющих файлы. Дальнейшее расследование показало, что при открытии файлов все настольные компьютеры использовали один сервер каталогов для получения информации о размещении файлов на серверах и что именно сервер каталогов был перегружен. Никто не догадывался, что, хотя сервер каталогов может легко справиться с количеством пользователей, чьи настольные компьютеры к нему обращались, но каждый пользователь генерировал десятки, а то и сотни запросов на открытие файлов при выполнении крупных задач. Когда было вычислено количество запросов от каждого пользователя и примерное количество одновременно обращающихся пользователей, стало видно, что для достижения хорошей производительности необходим дополнительный сервер каталогов.

5.3. Заключение

Разработка и создание сервисов – важная часть работы каждого системного администратора. От того, насколько хорошо системный администратор выполнит эту часть работы, зависит то, насколько легко будет обслуживать и поддерживать каждый сервис, насколько он будет надежным, производительным, соответствующим требованиям пользователей и в конечном счете насколько довольны будут пользователи работой команды системных администраторов.

Вы создаете сервис для улучшения обслуживания ваших пользователей, непосредственно, за счет предоставления необходимого им сервиса, или опосредованно, за счет улучшения эффективности работы команды системных администраторов. Всегда помните о потребностях пользователей. В конечном итоге это главная причина создания сервисов.

Системный администратор может сделать многое для улучшения обслуживания, например создать выделенные серверы, упростить управление, вести мониторинг серверов и сервисов, следовать стандартам компании и централизовать сервисы на нескольких машинах. В число условий создания лучшего сервиса входит ваша способность видеть дальше начальных требований будущих проектов по модернизации и обслуживанию. Создание сервиса, максимально независимого от машин, на которых он выполняется, – основной способ упростить обслуживание и модернизацию.

Сервисы должны быть настолько надежны, насколько это требуется пользователям. Спустя некоторое время в более крупных компаниях вы должны быть готовы сделать большее количество сервисов полностью избыточными, чтобы при сбое любого из компонентов и его замене сервис не прекращал работу. Распределите приоритеты в том порядке, который обеспечит для сервисов полную избыточность, основываясь на потребностях ваших пользователей. Только наработав достаточный опыт с конкретными системами, вы сможете понять, какие из них наиболее важны.

Последняя, но, возможно, наиболее заметная часть создания нового сервиса – постепенное развертывание сервиса с минимальными помехами в работе пользователей. Мнение пользователей о сервисе формируется в основном во время процесса внедрения, так что очень важно провести его правильно.

Задания

1. Составьте список сервисов, которые вы могли бы реализовать в ваших условиях. Какое аппаратное и программное обеспечение потребуется для создания каждого из них? Перечислите их зависимости.
2. Выберите сервис, который вы разрабатываете или можете прогнозировать необходимость его разработки в будущем. Что вам понадобится, чтобы построить его в соответствии с рекомендациями данной главы? Как вы будете внедрять сервис среди пользователей?
3. Какие сервисы зависят от машин, находящихся за пределами машинного зала? Как вы можете избавиться от этой зависимости?
4. Мониторинг каких сервисов вы ведете? Как вы можете расширить охват мониторинга, чтобы он отслеживал работу сервиса, а не машин? Отправля-

ет ли ваша система мониторинга заявки на обслуживание или оповещения персоналу? Если нет, насколько сложно будет добавить такую функциональность?

5. Есть ли у вас машины, на которых запущено несколько сервисов? Если да, то как вы сможете разделить их, чтобы каждый сервис выполнялся на отдельной машине? Как пользователи перенесут этот процесс? Поможет это или повредит сервису?
6. Как у вас осуществляется планирование мощностей? Достаточно удовлетворительно или вы собираетесь усовершенствовать этот процесс?
7. Каким из ваших сервисов обеспечена полная избыточность? Каким образом обеспечивается избыточность? Есть ли другие сервисы, которым тоже следует обеспечить избыточность?
8. Перечитайте раздел о пропускной способности и времени ожидания (раздел 5.1.2). На что похожи математические формулы для двух предложенных решений: пакетных и сквозных запросов?

Глава 6

Вычислительные центры

Эта глава посвящена созданию **вычислительного центра** – места, в котором находятся машины, предоставляющие общие ресурсы. Однако вычислительный центр – не просто комната с серверами. Как правило, вычислительный центр оснащен системами охлаждения, регулировки влажности, электропитания и противопожарными системами. Все эти системы – часть вашего вычислительного центра. По теории вы должны собрать все наиболее важные компоненты в одном месте, а затем следить, чтобы это место было достаточно надежным.

Эти помещения соответствуют разным условиям и немного отличаются друг от друга. Зачастую вычислительные центры – это отдельные здания, построенные специально для вычислительных и сетевых операций. *Машинный*, или *компьютерный*, *зал* – менее внушительное помещение, возможно, переоборудованное из обычного офисного. Самые маленькие помещения подобного типа часто шутливо называют *компьютерными каморками*.

Строить вычислительный центр дорого, а сделать это правильно – еще дороже. Вы должны быть готовы к тому, что руководство будет против таких затрат и потребует их обоснования. Будьте готовы обосновать сегодняшние дополнительные затраты, показав, как это сэкономит время и деньги в следующие годы. Некоторые истории в этой главе помогут вам.

В небольших сетях сложно будет доказать полезность многих рекомендаций из этой главы. Однако, если ваша мелкая сеть собирается расти, используйте эту главу как план к вычислительному центру, который понадобится вашей компании, когда она вырастет. Планируйте усовершенствование вычислительного центра по мере того, как компания будет расти и сможет позволить себе вкладывать больше средств в повышенную надежность. А пока делайте то, что можете выполнить со сравнительно малыми вложениями, например приведите в порядок стойки и кабели, и изыскивайте возможности улучшения.

Многие организации предпочитают арендовать место в **колокейшн-центрах** – вычислительных центрах, место в которых для нуждающихся в этой услуге компаний сдает в аренду компания, предоставляющая данную услугу. Такая возможность может быть очень экономичной, особенно с учетом опыта компании в таких эзотерических вопросах, как энергоснабжение и охлаждение. В этом случае данная глава поможет вам с пониманием беседовать на тему вычислительных центров и задавать верные вопросы.

Из-за того что оборудование вычислительного центра, как правило, входит в общую инфраструктуру, его трудно модернизировать или фундаментально изменять вычислительный центр без назначения хотя бы одного профилакти-

ческого перерыва на обслуживание (в главе 20 есть советы, как это сделать). Так что это решение хорошо подходит только на первое время, пока вы лишь начинаете создание собственного вычислительного центра. Разумеется, по мере смены технологий требования к информационному центру будут меняться, но вашей целью должен быть прогноз потребностей на 8–10 лет вперед. Если вы думаете, что 10 лет – это много, вспомните о том, что срок существования большинства вычислительных центров – 30 лет. На самом деле 10 лет – это пессимистический прогноз, подразумевающий полное обновление дважды за время существования здания.

На заре компьютерной эры компьютеры были огромными и их обслуживали несколько специалистов. Сам их размер требовал, чтобы компьютеры размещались в специальной среде вычислительного центра. Большие ЭВМ требовали особого охлаждения и энергоснабжения и, следовательно, вынуждены были находиться в специальной среде вычислительного центра. Мини-ЭВМ меньше грелись и были менее требовательны к энергоснабжению, но тоже размещались в специализированных компьютерных залах. Суперкомпьютеры, как правило, нуждаются в водяном охлаждении, особо требовательны к энергоснабжению и обычно размещаются в вычислительных центрах со специально усиленным и укрепленным фальшполом. Первые настольные компьютеры, такие как Apple II и персональные компьютеры под управлением DOS, не использовались в качестве серверов, а размещались на рабочих столах без специального энергоснабжения или охлаждения. Эти компьютеры были радикально новым инструментом, противоположным большим ЭВМ, и их пользователи гордились тем, что могут работать вне вычислительных центров. Рабочие станции UNIX с самого начала использовались и как настольные компьютеры, и как серверы. Здесь граница между тем, что должно находиться в вычислительном центре, а что на столе или под столом в любом помещении, стала менее очевидной и определялась уже функциями и требованиями к доступности для пользователей, а не типом машины. Круг замкнулся: миру персональных компьютеров потребовались надежные системы, доступные круглосуточно без выходных, и персональные компьютеры начали снова размещать в вычислительных центрах, хотя ранее это были альтернативные варианты.

6.1. Основы

На первый взгляд может показаться, что создать вычислительный центр довольно просто. Нужен только большой зал со столами, стойками или сетчатыми стеллажами – и все! На самом деле основы создания хорошего, надежного вычислительного центра, который позволит системным администраторам работать эффективнее, значительно сложнее. Для начала вам понадобится выбрать качественные стойки и сетевые кабели, подготовить питание, которое будет подаваться к оборудованию; потребуется серьезное охлаждение и нужно будет продумать систему пожаротушения. Кроме того, вы должны основательно спланировать устойчивость помещения к стихийным бедствиям. Правильная организация зала подразумевает продуманную разводку кабелей, службу консолей, пометку ярлыками, наличие инструментов, запасных частей, рабочих мест и мест парковки для передвижных устройств. Также вам понадобится проработать механизмы безопасности вычислительного центра и продумать способы транспортировки оборудования в зал и из зала.

6.1.1. Размещение

Во-первых, вам нужно решить, где будет размещаться вычислительный центр. Если это будет центральный узел для офисов по всему миру или в пределах географического региона, то сначала придется выбрать город и здание в этом городе. Когда здание выбрано, необходимо выбрать подходящее место внутри здания. На всех этих этапах при принятии решения следует принимать во внимание стихийные бедствия, типичные для этого региона.

Обычно системные администраторы не могут повлиять на выбор города и здания. Тем не менее, если вычислительный центр обслуживает весь мир или значительный регион и при этом расположен в местности, где часты землетрясения, потопы, ураганы, грозы, торнадо, град или иные стихийные бедствия, способные повредить информационному центру или вызвать перебои с энергоснабжением и связью, вы должны быть подготовлены к подобным случайностям. Кроме того, вы должны быть готовы к тому, что чей-то экскаватор случайно повредит ваши линии энергоснабжения и связи, независимо от того, насколько хорошо вы защититесь от стихийных бедствий (см. произведение неизвестного автора «The backhoe, natural enemy of the network administrator» (Экскаватор, природный враг администратора сетей), *www.23.com/backhoe/*). Подготовка к перебоям в энергоснабжении будет рассмотрена в разделе 6.1.4. Против перебоев со связью вы можете внедрить технологии резервных подключений на случай, если основные каналы выйдут из строя. Эти меры предосторожности могут быть такими же простыми, как различная маршрутизация линий (когда избыточные подключения идут по разным каналам к одному провайдеру), или такими же сложными, как спутниковые резервные подключения. Также вы можете поставить вопрос о создании второй сети, полностью дублирующей все службы вычислительного центра, когда основная сеть выходит из строя. Такой подход обходится дорого и может быть оправдан только в случае, если временный отказ вычислительного центра угрожает компании сопоставимыми убытками (глава 10).

Размещение и политические границы

Иногда сеть, расположенная в нескольких милях от другой, значительно лучше из-за того, что она расположена в другом штате или округе. Например, одной компании, сдававшей в аренду места в новом вычислительном центре в конце 1990-х годов, требовалось много вычислительных центров для обеспечения избыточности. Одним из решений компании было не арендовать помещения в округах, принимавших участие в предложенном в Калифорнии плане прекращения регулирования энергетической отрасли. Это зачастую означало, что одно из одинаковых помещений, находящихся в нескольких милях друг от друга, признавалось непригодным. Те, кто не придерживается нормативных актов, не заметили бы разницы.

Когда план прекращения регулирования привел к известным проблемам с энергоснабжением в Калифорнии в 2000–2001 годах, то, что раньше казалось паранойей, обернулось предотвращением значительных перебоев в энергоснабжении.

Когда приходит время выбирать помещение для вычислительного центра внутри здания, команда системных администраторов должна в этом участвовать. На основании требований, выведенных из содержания этой главы, вы должны обсудить размеры необходимого вам помещения. Также вы должны быть готовы предоставить отделу недвижимости требования, которые помогут им выбрать подходящее место. Как минимум, вы должны быть уверены, что пол достаточно прочный, чтобы выдержать вес оборудования. Однако есть и другие факторы, которые необходимо учитывать.

Если в регионе часто случаются наводнения, по возможности надо избегать размещения вычислительного центра в подвале или даже на первом этаже. Также вам надо учитывать, как это отразится на размещении вспомогательной инфраструктуры вычислительного центра: таких систем, как источники бесперебойного питания, автоматы включения резерва (ATS), генераторы и системы охлаждения. Если эти вспомогательные системы откажут, то и вычислительный центр тоже. Не забывайте, что вычислительный центр – не просто зал, в котором стоят серверы.

Пример: бункеры – самые защищенные вычислительные центры

Если вам нужно защищенное здание, вы не ошибетесь, последовав примеру вооруженных сил США. Федеральное ведомство предоставляет страховку служащим вооруженных сил США и членам их семей. Большинство работающих там людей – бывшие военные, и их вычислительный центр – прочнейшее здание, какое только можно представить, – военный бункер. Люди, которым довелось там побывать, рассказывают, что иногда трудно было не хихикать, но они оценили усилия по защите. Это здание способно выдержать любую погоду, стихийные бедствия и, скорее всего, террористические атаки и артиллерийский обстрел. Многие поставщики сейчас предоставляют место в колокейшн-центрах, защищенных, как бункеры.

HavenCo

Но излишнее увлечение безопасностью тоже чревато проблемами. Например, компания HavenCo приобрела морской форт времен Второй Мировой войны, похожий на нефтяную буровую платформу, и разместила там вычислительный центр. Компания годами мучилась с проблемами логистики (например, все оборудование и запасные части приходилось транспортировать на рыболовном траулере) и с кадровыми проблемами, так как мало кто соглашался жить в бетонной башне в семи милях от берега. С бизнесом у компании тоже все обстояло плохо, так как большинство пользователей предпочитали обслуживание традиционных вычислительных центров. В результате в конце июля 2006 года компания понесла огромный ущерб, когда загорелось хранилище топлива для генератора. Когда писались эти строки, на сайте компании сообщалось, что HavenCo реконструируется и ищет новых инвесторов.

При размещении вычислительных центров в сейсмически опасных регионах надо учитывать несколько факторов. Вы должны выбирать стойки, которые в достаточной степени устойчивы к вибрации, и удостовериться, что оборудование хорошо закреплено в стойке и не выпадет при землетрясении. Вам следует установить соответствующие сейсмостойкие конструкции, усиливающие, но не слишком жесткие. Если у вас настелен фальшпол, вы должны убедиться, что он достаточно прочный и соответствует строительным нормам. Продумайте прокладку кабелей питания и сетевых кабелей в вычислительном центре. Смогут ли они выдержать нагрузку на растяжение и сжатие или могут оборваться?

Существует несколько уровней сейсмической готовности вычислительных центров. Хороший консультант по информационным центрам должен быть готов согласовать с вами возможности и затраты, чтобы вы могли решить, что соответствует требованиям вашей компании. Как показывает опыт, хороший продавец стоек тоже может рассказать вам о большом количестве конструктивных решений и требований к безопасности, а также порекомендовать хороших инженеров по охлаждению и лучшие компании, занимающиеся системами питания и кабелями. Хороший продавец стоек может свести вас со всеми специалистами, которые вам понадобятся при проектировании вычислительного центра.

В грозоопасных регионах потребуется особая грозовая защита. Проконсультироваться по этому вопросу можно у архитекторов.

Грозовая защита

В одном холме в Нью-Джерси были значительные залежи железной руды. На вершине холма стояло огромное здание, кровля которого была целиком сделана из меди. Так как и холм, и крыша были подвержены частым ударам молний, здание было оборудовано очень серьезной грозовой защитой. Однако в каждом необъяснимом перебое, случавшемся в здании, системные администраторы спешили обвинить железную руду и медную кровлю, даже если не было дождей. Всякое бывает!

Избыточные центры

Особо крупные организации, предоставляющие веб-сервисы, развертывают многочисленные избыточные вычислительные центры. У одной из таких компаний было множество вычислительных центров по всему миру. Каждая из служб, или проектов компании, разделялась между разными информационными центрами, бравшими на себя часть рабочей нагрузки. Достаточно популярным проектам во время наибольшей нагрузки для обслуживания требовались мощности четырех вычислительных центров. Более популярным проектам для достижения достаточной мощности требовалось восемь вычислительных центров. Компания придерживалась такой политики: в любое время для всех служб должно быть доступно столько вычислительных центров, чтобы любые два из них могли отключиться и при этом мощностей оставшихся хватало бы для обеспечения служб. Такая избыточность $n + 2$ позволяла отключить один

из центров для профилактических работ, и, если при этом неожиданно отключался еще один, обслуживание не приостанавливалось.

6.1.2. Доступ

Местные законы в некоторой степени определяют доступ в ваш вычислительный центр и, например, могут требовать наличия как минимум двух выходов или пандусов для инвалидных колясок, если у вас настелен фальшпол. Помимо этих соображений, вы должны продумать, как будете перемещать стойки и оборудование в зал. Некоторые элементы оборудования могут быть шире стандартных дверных проемов, так что вам могут понадобиться более широкие двери. Если у вас двойные двери, убедитесь, что между ними нет стояка. Также стоит предусмотреть проходы между стойками, достаточные для транспортировки оборудования на места. Может понадобиться усилить некоторые зоны пола и проходы к ним, чтобы пол выдержал особо тяжелое оборудование. Также вам надо предусмотреть свободный доступ от погрузочной платформы на всем пути до вычислительного центра. Не забывайте, что обычно оборудование доставляется в таре, габариты которой превышают размер самого оборудования. Мы видели, как на погрузочной платформе оборудование приходилось вынимать из упаковки, чтобы его можно было отвезти в лифт и к месту назначения.

Погрузочная платформа

В одной из молодых компаний Силиконовой долины не было погрузочной платформы. Однажды к ним пришла большая партия серверов, которые пришлось оставить на улице возле здания, потому что не было возможности выгрузить их с грузовика прямо в здание. Часть серверов была на поддонах, которые приходилось разбирать и по частям переносить ко входу в здание. Другие, достаточно мелкие части отвозили в здание по пандусу для инвалидных колясок. Но некоторые части были настолько большими, что ни один из этих способов не подходил и их перевозили по стальному пандусу в гараж; там их втискивали в небольшой подъемник и поднимали на уровень этажа, где находился компьютерный зал. К счастью, дело было летом в Калифорнии и во время этого длительного процесса не начался дождь.

6.1.3. Безопасность

Вычислительный центр должен быть физически защищен настолько, насколько это возможно сделать, не препятствуя работе системных администраторов. Доступ должен предоставляться только тем, чьи обязанности того требуют: техникам по обслуживанию аппаратуры, операторам резервных копий на стримерах, сетевым администраторам, специалистам по материальной части и технике безопасности, а также ограниченному числу руководителей. Ответственный за пожарную безопасность и, в некоторых случаях, аварийные бригады, приписанные к этой зоне, должны назначаться из тех, у кого уже есть доступ.

Ограничение доступа в вычислительный центр повышает надежность и безотказность размещенного там оборудования и увеличивает вероятность, что

стандарты прокладки кабелей и монтажа в стойки будут соблюдаться. К серверам, по определению, предъявляются высокие требования по безотказной работе, и следовательно, все изменения должны вноситься группой системных администраторов в соответствии с установленными правилами и процедурами, направленными на выполнение либо превышение обязательств по уровню обслуживания. Сотрудники, не входящие в число системных администраторов, не имеют таких обязательств и не обучены ключевым процессам группы системных администраторов. Поскольку эти сотрудники посвящают меньше времени обслуживанию инфраструктурного оборудования, они скорее могут допустить ошибки, которые способны вызвать дорогостоящий простой. Если кому-то из ваших пользователей нужен физический доступ к машинам в вычислительном центре, они не могут считаться высоконадежными или инфраструктурными машинами и поэтому должны быть перемещены в лабораторные условия, где пользователи смогут получить к ним доступ. Либо можно использовать технологии удаленного доступа, такие как KVM-коммутаторы.

Запирать вычислительный центр на ключ – неидеальный способ, так как ключи неудобны, их слишком легко скопировать и сложно отследить их местонахождение. Лучше подумайте о внедрении систем бесконтактных пропусков, они более удобны и автоматически регистрируют входящих. В вычислительных центрах с особо высокими требованиями к безопасности, например в банках или медицинских центрах, иногда совмещают использование ключей и бесконтактных пропусков, либо требуют одновременного присутствия двух людей с пропусками, чтобы никто не находился в зале без присмотра, либо используют датчики движения, чтобы убедиться, что зал действительно пуст, когда это отмечено в записях регистрации пропусков.

При проектировании вычислительного центра учитывайте высоту считывателя бесконтактных пропусков. Если считыватель карт находится на нужной высоте, пропуск можно повесить на цепочку или носить в заднем кармане и подносить к считывателю карт без помощи рук. Стильные системные администраторы делают это с изяществом Элвиса. Остальные выглядят просто глупо.

Биометрические замки приносят много беспокойства. Этично ли устанавливать систему безопасности, которую можно обойти, отрезав палец у авторизованного сотрудника? Если данные очень ценные, биометрические замки могут поставить жизнь авторизованных сотрудников под угрозу. Большинство биометрических систем безопасности дополнительно проверяют наличие пульса или температуру, чтобы удостовериться, что палец принадлежит живому человеку. Другие системы требуют введения PIN-кода или распознавания голоса в дополнение к биометрическому сканированию. Если вы установите такую систему безопасности, мы рекомендуем выбирать ту, которая проверяет, что сотрудник все еще жив. Но даже в таком случае существуют этические проблемы, связанные с тем, что сотрудник при увольнении не может изменить свои отпечатки пальцев, голос или ДНК. Биометрическая информация – это **неотменяемый ключ**. И наконец, что не менее важно, люди с ограниченными физическими возможностями не всегда могут воспользоваться такими системами.

Недавно эффективность биометрических систем была поставлена под сомнение. Цутому Мацумото (Tsutomu Matsumoto), японский специалист в области криптографии, доказал, что лучшие системы сканирования отпечатков пальцев можно надежно обмануть, приложив немного изобретательности и потратив подручных материалов на 10 долларов: из обычного желатина он сделал поддельный палец (SPIE 2002).

Также для безопасности зала важны правила для посетителей. Можно ли посетителей оставлять одних? Что делать в случае, если для установки или ремонта на несколько часов привлекают работников поставщика? Придется ли системным администраторам нянчиться с ними все это время?

Я плачу вам не за то, чтобы вы смотрели, как люди красят!

В одном вычислительном центре нужно было покрасить стены. Была выбрана компания, которая заявляла, что у них есть опыт работы в вычислительных центрах.

Системные администраторы предложили выйти подежурить и присмотреть, чтобы маляры ничего не сломали и не повредили. Их руководитель ответил: «Я не собираюсь платить вам за то, чтобы вы целый день смотрели, как люди красят!» – и сказал, чтобы маляров оставили одних выполнять свою работу.

Можете представить себе результат.

Восстановление повреждений обошлось дороже, чем недельная зарплата.

6.1.4. Электричество и охлаждение

Энергоснабжение и охлаждение вычислительного центра непосредственно взаимосвязаны. Оборудование работает от электричества, охлаждение борется с теплом, выделяемым аппаратурой при ее работе. При слишком высокой температуре оборудование может работать с ошибками или даже сгореть.

Как правило, на каждый ватт, потребляемый вашим оборудованием, вам придется потратить по меньшей мере 1 ватт на охлаждение. Тепло, выделяемое оборудованием, потребляющим 10 кВт, потребует системы охлаждения на 10 кВт (на самом деле скорее 11 или 12 кВт, учитывая неэффективность системы). Это законы термодинамики. Значит, половина вашего счета за электричество идет на охлаждение, а половина – на питание оборудования. Кроме того, это означает, что аппаратура, которая потребляет меньше электроэнергии, экономит ее вдвое больше за счет меньшей потребности в охлаждении.

Вы можете направить воздушные потоки в вычислительном центре двумя основными способами. Первый способ – это использование фальшпола в качестве воздухопровода для холодного воздуха. Вентиляционная система нагнетает холодный воздух и создает достаточное давление, чтобы воздух поступал через отверстия в фальшполе. Вентиляционные отверстия размещаются так, чтобы воздух из них шел снизу в оборудование, выводя тепло наверх и наружу. Этот способ работает за счет того, что горячий воздух поднимается вверх. Многие считают, что под фальшполом проще прокладывать кабели. Но кабели перекрывают поток воздуха, и их нельзя прокладывать под полом, используемым для охлаждения. Если у вас фальшпол, часть архитектуры охлаждения, кабели и источники питания придется размещать над стойками. Вам нужно будет постоянно напоминать сотрудникам, что кабели и другие элементы, препятствующие потоку воздуха, нельзя размещать под полом.

Другой способ – подавать холодный воздух со стороны потолка и обдувать машины сверху вниз. Так как горячий воздух поднимается вверх, потребуется дополнительная работа для нагнетания холодного воздуха вниз. Используя такую систему, вы можете также прокладывать кабели над стойками либо использовать фальшпол исключительно для кабелей.

При принятии решения о необходимом количестве энергоснабжения и охлаждения вы должны стремиться достигнуть максимальной мощности электропитания одновременно с максимальной мощностью охлаждения, используя все доступное вам пространство.

Правила охлаждения

В 2001 году распространенной практикой для типичного, не слишком перегруженного офисного компьютерного зала было охлаждение из расчета 5 т (60 050 БТЕ) на каждые 5000 квадратных футов вычислительного центра.

Не забывайте, что оборудование имеет тенденцию уменьшаться в габаритах и спустя несколько лет для той же площади может потребоваться больше мощности и больше охлаждения. По мере того как популярность завоевывают вместительные фермы блейд-серверов, старые правила становятся неприменимы.

Еще один компонент кондиционирования – контроль влажности. В вычислительном центре нужно регулировать влажность воздуха, так как высокая влажность приводит к образованию конденсата и выходу оборудования из строя, а при низкой влажности возникают статические разряды, которые также могут повредить оборудование. В идеале влажность воздуха должна быть от 45 до 55%. Системы энергоснабжения, отопления[1], вентиляции и кондиционирования громоздки, их сложно заменять, и почти наверняка для этого потребуется перерыв. Поэтому старайтесь планировать эти системы хотя бы на 8–10 лет вперед.

Электропитание вычислительного центра должно быть сглаженным, или **стабилизированным**, чтобы защитить оборудование от скачков и спадов напряжения, обычных в электрической сети. Стабилизированное резервное питание также подразумевает устойчивую синусоидальную форму и постоянную величину напряжения. Для этого потребуется как минимум один источник бесперебойного питания, обеспечивающий достаточное электроснабжение со стабильным напряжением для всего вычислительного центра. Обычно источник бесперебойного питания подает напряжение с блоков батарей, непрерывно подзаряжаемых от входящей линии питания, когда напряжение в сети достаточно стабильно. Затем питание с ИБП подается на распределительные щиты в вычислительном центре и других местах, нуждающихся в защите питания. ИБП с модульными блоками батарей изображен на рис. 6.1.

---

[1] Иногда информационным центрам нужно отопление. Говорят, компьютеры на Южном полюсе, на станции Амундсена–Скотта, не нуждаются в отоплении. Однако на зимних Олимпийских играх в 1998 году в Нагано на вершинах горнолыжных трасс для компьютеров приходилось использовать электрообогреватели, поскольку ночью все выключалось (Guth and Radosevich 1998).

Рис. 6.1. *Модульный ИБП в корпорации GNAC*

Системы бесперебойного питания должны иметь возможность оповещать персонал о сбоях или иных проблемах. Небольшие источники бесперебойного питания при истощении батарей должны уметь посылать серверам оповещения о необходимости выключения.

При приобретении источников бесперебойного питания наиболее важно учитывать следующее: как показывают исследования, перебои в электросети обычно либо очень короткие (исчисляемые секундами), либо очень длинные (полдня и дольше). Большинство перебоев с напряжением длятся не более 10 с. С точки зрения статистики, если электричества нет более 10 мин, наиболее вероятно, что его не будет весь день и вы можете отпустить сотрудников домой.

Следовательно, приобретение ИБП, который обеспечивает резервное питание значительно дольше часа, с точки зрения статистики будет пустой тратой денег. Если электричества нет в течение часа, скорее всего, его не будет до конца дня или около того, а ИБП с таким запасом емкости стоит слишком дорого. Если в вашем соглашении об уровне обслуживания требуется устойчивость к перебоям в электросети длительностью более часа, вашему информационному центру потребуется генератор.

Таким образом, можно проектировать систему резервного питания либо в расчете на час работы, либо намного дольше. Если вы приобретете ИБП с емкостью, достаточной на час работы, он обеспечит питание во время частых коротких перебоев и даст вам время для выключения всех систем во время редких длительных перебоев. Такое решение менее дорогостоящее, так как источнику бесперебойного питания не придется питать систему охлаждения, поскольку обычно один час вычислительный центр может продержаться без охлаждения. Как следует из написанного выше об охлаждении и энергоснабжении, питание системы охлаждения от ИБП потребует удвоить его емкость, что примерно вдвое увеличит его стоимость.

Вычислительные центры, предоставляющие службы круглосуточно без выходных, требуют более сложных систем бесперебойного питания. Небольшие ИБП,

рассчитанные на короткое время работы, комбинируются с генератором и АВР, переключающимся между ними. Такой тип систем бесперебойного питания поможет пережить многочасовые перебои. ИБП справится с частыми короткими перебоями и даст вам время для включения генератора. Служба аварийной дозаправки должна быть готова позволить зданию неограниченное время получать электричество от генератора. На рис. 6.2 и 6.3 показаны топливный резервуар и генератор соответственно.

Рис. 6.2. *Бак емкостью 1000 галлонов для заправки генераторов в корпорации GNAC*

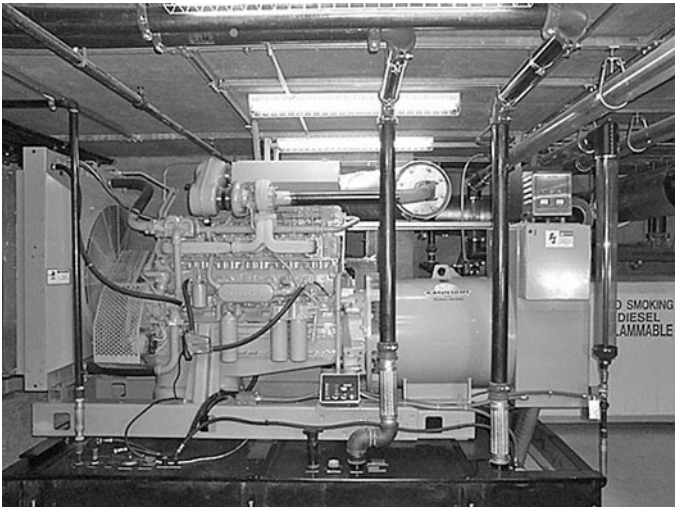

Рис. 6.3. *Избыточные генераторы в корпорации GNAC, каждый с собственным баком на 200 галлонов, заправляемым из главного бака на 1000 галлонов*

Автомат включения резерва – это устройство, управляющее переключением питания ИБП от сети или генератора. АВР отслеживает напряжение в сети и, если оно находится в пределах нормы, подключает к сети ИБП. Если АВР фиксирует перебои в сети, то питание ИБП отключается, включается генератор и, когда генератор начинает вырабатывать стабильное напряжение, ИБП переключается на него. Когда напряжение в сети возвращается в норму, АВР снова переключает ИБП на питание от сети и выключает генератор. Обычно АВР оснащается также и ручным переключателем, так что вы можете в случае необходимости принудительно переключить ИБП на питание от сети или генератора. Панель управления АВР изображена на рис. 6.4.

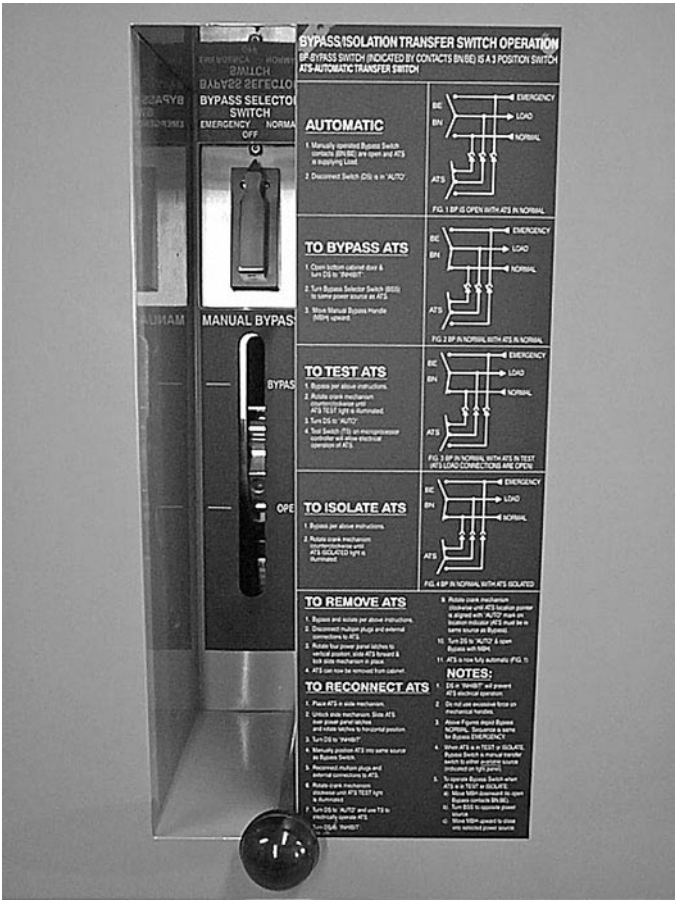

Рис. 6.4. *Переключатель обхода АВР в корпорации GNAC*

Всегда устанавливайте переключатель, позволяющий включить питание в обход ИБП в случае его отказа. Все питание вычислительного центра идет через ИБП. Следовательно, если он откажет, то на время ремонта вам понадобится переключиться на другой источник питания. Переключатель должен быть отдельным от ИБП и находиться на разумном расстоянии от него. ИБП работает

на батареях, и в случае их воспламенения вам вряд ли захочется заходить в зал ИБП, чтобы включить обход. ИБП может оснащаться собственным переключателем обхода, но этого недостаточно, особенно в случае пожара.

При приобретении источника бесперебойного питания следует учитывать его обслуживание и требования к окружению. ИБП может требовать периодической профилактики, и уж точно вам придется заменять батареи примерно раз в три года. Также может потребоваться охлаждение и контроль влажности, что может предопределить место размещения ИБП в здании. Кроме того, выясните, может ли ИБП принудительно переводиться из режима быстрой в режим постепенной зарядки батарей. ИБП, быстро заряжающий батареи, создает значительную нагрузку на остальную систему энергоснабжения, что может вызвать отключение электричества. При медленной зарядке дополнительная нагрузка на электросеть значительно ниже.

Генераторы должны проходить тщательную профилактику, ежемесячные испытания и периодически дозаправляться. В противном случае в тех немногих ситуациях, когда они понадобятся, генераторы не будут работать и вы зря потратите деньги.

Пример: отказ системы отопления, вентиляции и кондиционирования

Небольшая биотехнологическая молодая компания со штатом примерно в 50 сотрудников создавала свой первый вычислительный центр сразу после переезда в большое здание, где они планировали оставаться по крайней мере 10 лет. В штате компании не было старшего системного администратора. Менеджер технического отдела не понимал, насколько много тепла может вырабатывать вычислительный центр, и решил сэкономить, приобретя менее мощные системы отопления, вентиляции и кондиционирования, чем рекомендованные подрядчиками, оборудовавшими вычислительный центр. Вместо этого компания купила компоненты, рекомендованные продавцом систем отопления, вентиляции и кондиционирования, который явно не был знаком с планированием вычислительных центров.

Спустя несколько лет вычислительный центр был полон оборудования, а системы отопления, вентиляции и кондиционирования выходили из строя каждые несколько месяцев. Каждый раз, когда это случалось, системные администраторы выключали наименее необходимые машины, брали огромные ведра со льдом (его в лабораториях было в достатке) и вентиляторы и до конца дня пытались сохранить наиболее критичные элементы вычислительного центра в рабочем состоянии. Затем системные администраторы выключали все на ночь. В течение следующих 2–3 недель случалось множество отказов оборудования, в основном дисков. Затем все входило в норму до следующего сбоя систем отопления, вентиляции и кондиционирования. Техники по вентиляции и кондиционированию сказали системным администраторам, что проблема в неспособности системы охлаждения справиться с тем количеством тепла, которое выделял вычислительный центр.

Проблема не решилась, пока не были установлены дополнительные мощности охлаждения.

Если в вычислительном центре есть генератор, то системы отопления, вентиляции и кондиционирования тоже должны иметь резервное питание. Иначе системы будут перегреваться.

Для выявления горячих точек полезно распределить по информационному центру и подключить к системам мониторинга датчики температуры. Другой вариант, быстрый и дешевый, – перемещать по залу цифровые термометры, записывающие показания о высокой и низкой температуре. Если вы достаточно чувствительны к температуре, можете определить места перегрева рукой. Горячие точки, которые не обдуваются воздухом, особенно опасны, так как они нагреваются быстрее. После выявления горячих точек проблема сводится к перемещению оборудования или замене системы отопления, вентиляции и кондиционирования. Если горячие точки остались незамеченными, они могут стать причиной отказа оборудования. Некоторые поставщики аппаратного обеспечения предоставляют способ мониторинга температуры в одной или нескольких точках внутри их оборудования. Если есть такая возможность, надо ее использовать, потому что она обеспечивает бóльшую зону наблюдения, чем при размещении термодатчиков в помещении.

Системы отопления, вентиляции и кондиционирования часто выходят из строя незаметно и иногда возобновляют работу так же незаметно. Так как сбои систем отопления, вентиляции и кондиционирования повышают вероятность сбоев другого оборудования, важно вовремя заметить их сбой. Если в самих системах не предусмотрен механизм автоматического оповещения службы поддержки, следует включить температурные датчики в конфигурацию систем мониторинга сети.

Мониторинг температуры в зале как датчик присутствия

Вести мониторинг температуры в зале нужно не только для выявления аварийных ситуаций, таких как сбои систем отопления, вентиляции и кондиционирования или пожары, но и для предотвращения развития порочной практики. Например, один руководитель был озабочен тем, что системные администраторы иногда не закрывают дверь машинного зала. Он заметил, что, когда он входит в зал, там температура близка к обычной комнатной и кондиционеры работают на полную мощность, пытаясь компенсировать эффект открытой двери.

На собрании персонала его все уверяли, что никто не забывает закрывать дверь. Он настроил Cricket, программу мониторинга, работающую через SNMP, для сбора данных о температуре с маршрутизаторов в этом и других машинных залах. На следующем собрании он продемонстрировал графики, показавшие, что температура в течение рабочего дня повышается на 10°, но остается нормальной по выходным и праздникам. Еще более наглядно проблему демонстрировало то, что в других машинных залах не было такого разброса температур. На следующем собрании он продемонстрировал графики, показывающие, что проблема исчезла, и поблагодарил всех за то, что они не забывают закрывать дверь.

В дополнение к подключению систем отопления, вентиляции и кондиционирования к генератору может быть полезно подключить и другие цепи здания

к резервному питанию от генератора. Эти цепи должны быть устойчивы к коротким перебоям и скачкам напряжения. Подходящий кандидат – освещение, особенно в помещениях службы поддержки и эксплуатационного отдела. Группам, которые должны работать во время перебоев, таким как служба поддержки, погрузки и разгрузки или центр обслуживания пользователей, может быть полезно иметь резервное питание освещения и электросети от генератора и небольших настольных ИБП. Во всех помещениях должно быть по крайней мере аварийное освещение, включающееся автоматически при отключении электроэнергии, даже если это не предусмотрено региональными строительными нормами. Если вы можете позволить себе такую роскошь, как отключение электросети всего здания, может быть полезно попробовать провести такое испытание и посмотреть, что еще вам может понадобиться подключить к аварийному питанию. Если невозможно провести полное испытание, представьте себе все, что вам потребуется сделать при отключении электроэнергии, и отметьте, какие из необходимых для вас элементов окажутся недоступны.

Важность освещения

В одной компании не было подведено аварийное питание к освещению генераторного зала. Это упущение было обнаружено, когда случился сбой электроснабжения и пришлось заправлять дизельный генератор в темноте.

Максимальная нагрузка – это не просто суммарное потребление оборудования вычислительного центра. Все компоненты электрической системы, а также выключатели и автоматические предохранители между ними должны иметь запас мощности, достаточный, чтобы выдержать максимальную нагрузку вычислительного центра, системы отопления, вентиляции и кондиционирования, работающих с максимальной производительностью, и нагрузку ИБП, заряжающих батареи.

Дополнительные мощности

Небольшая компания переехала в новые помещения. Они предусмотрительно выделили для вычислительного центра большую площадь, зная, что через несколько лет он заметно вырастет. У компании пока не было достаточно средств на организацию полных мощностей электроснабжения и кондиционирования, которые им в конечном счете могли понадобиться, и поэтому была установлена временная система, которую должны были заменить через год или два на полноценную систему.

Для добавления дополнительных электрических мощностей нужно подключиться к новому выделенному трансформатору местной энергетической компании, что подразумевает отключение электричества в здании. Также потребуются новые генераторы, новые АВР, новые системы бесперебойного питания и новые распределительные электрощиты в вычислительном центре.

Местная энергетическая компания переключала на новый трансформатор только в рабочее время в рабочие дни. По заверениям энергетической компании, переключение должно было занять полчаса, но системные администраторы компании предполагали, что на это уйдет не меньше двух часов. У системных администраторов уже были ИБП, АВР и генератор, поэтому планировалось на время отключения воспользоваться питанием от генератора. Тем не менее, в связи с тем что генератор надежно работал под нагрузкой не более нескольких минут, системные администраторы приняли мудрое решение взять на день напрокат второй генератор, на случай если первый выйдет из строя.

Когда привезли второй генератор, системные администраторы заранее провели кабели от него к АВР, чтобы они были под рукой, если их понадобится подключить. Они также на всякий случай вызвали в этот день своих подрядчиков, выполняющих работы с электрооборудованием.

Когда настал этот день, системные администраторы вручную переключили оборудование на питание от генератора за пару минут до того, как энергетическая компания отключила электричество в здании. Генератор работал хорошо в течение десяти минут, а затем отключился. Бросились в бой подрядчики-электрики, отключили от АВР кабели неисправного генератора, быстро подключили кабели второго генератора, запустили его, дождались, когда напряжение стабилизируется, и в завершение переключили АВР на питание от генератора. Все это время один человек дежурил возле ИБП в вычислительном центре, а другой – вместе с подрядчиками. Они поддерживали друг с другом связь по сотовому телефону. Сотрудник в вычислительном центре передавал обратный отсчет оставшегося до разрядки ИБП времени людям, работающим внизу, а они, в свою очередь, информировали его о ходе работы.

Как в лучших приключенческих фильмах, трагедия случилась в самый последний момент. Питание АВР от генератора было включено, когда дисплей ИБП показывал, что осталось две секунды. Однако впечатление, что бедствие удалось предотвратить, длилось недолго. ИБП «не понравилось» питание, которое он получал от нового генератора, поэтому он полностью израсходовал остатки батарей и переключился в режим обхода, направив напряжение с генератора непосредственно в вычислительный центр.

В спешке трехфазные силовые кабели от генератора неправильно подключили к АВР, потому что АВР был закреплен на стене вверх ногами. Поэтому, несмотря на тщательную подготовку к мероприятию, в этот день все равно произошел короткий скачок напряжения, когда оборудование переключилось на питание от сети, поскольку во время перехода в ИБП была истощена батарея.

Однако и на этом проблемы не закончились. Еще одно отключение произошло из-за предохранителя временной электросистемы, рассчитанного на меньшую нагрузку и не справившегося с зарядкой батарей ИБП вместе с питанием вычислительного центра. Когда вычислительный центр был переключен обратно на питание от сети и все работало стабильно, системные администраторы начали заряжать батареи ИБП. Спустя несколько минут термический предохранитель перегрелся и отключился. Источник

бесперебойного питания снова исчерпал заряд батарей и за несколько секунд до того, как предохранитель остыл достаточно для включения, вычислительный центр во второй раз остался без электричества.

Для завершения модернизации электросистемы требовалось еще переключиться на новые источники бесперебойного питания, АВР, генераторы и распределительные щиты. Все эти оставшиеся компоненты до переключения пару недель тщательно тестировались с блоками нагрузки. Было выявлено много неисправностей, и переключение прошло безупречно.

Даже если вы устанавливаете систему, которая наверняка будет временной, вы все равно должны проверять каждый компонент с тем же вниманием к деталям, как если бы это была постоянная система. Ни один из компонентов не должен быть недостаточно мощным. Ни один из компонентов не должен быть установлен нестандартным образом. Иначе, независимо от того, насколько хорошо вы будете готовиться к каждой случайности, система преподнесет вам неожиданные сюрпризы, когда вы меньше всего этого ожидаете.

Малогабаритные варианты охлаждения

В небольших компаниях часто имеется только компьютерный шкаф с одним сервером и пара небольших сетевых устройств. Зачастую для столь малого количества оборудования достаточно обычного охлаждения помещения. Однако, если охлаждение отключается на выходные, то первые же летние трехдневные выходные приведут к перегреву. Или компания дорастет до четырех-пяти серверов и комната будет перегреваться все время.

В такой ситуации **точечные кулеры** могут обеспечить до 10 000 БТЕ охлаждения, при этом им требуется только стандартная розетка на 110 В и воздуховод до ближайшего окна на улицу. Современные модели могут выбрасывать образующийся конденсат отработанным воздухом, устраняя необходимость каждый день освобождать емкость для сбора конденсата. В некоторых зданиях можно направить воздуховод за потолочные перекрытия, откуда потом отработанный воздух выведет вентиляционная система здания.

Малогабаритные устройства стоят всего 300 долларов. Для маленького компьютерного шкафа или телекоммуникационного зала это настолько мало, что можно приобрести еще одно на замену. Часто для покупки за такую цену даже не требуется согласование с руководством.

Для более крупных залов с пятью-десятью стойками оборудования можно взять напрокат передвижные блоки охлаждения за умеренную цену. Иногда год аренды стоит меньше, чем расходы на установку и создание постоянной системы.

Эти передвижные системы можно привезти в компьютерный зал и настроить за полдня. Небольшой молодой компании имеет смысл арендовать пятитонную систему (65 050 БТЕ) на год или два и заменить ее, когда потребности вырастут, а компания будет достаточно большой, чтобы позволить себе постоянное решение.

Цена систем охлаждения может показаться возмутительной, если до этого вы приобретали только потребительские (или домашние) устройства охлаждения. Промышленные или офисные системы – это совершенно другие устройства. Домашние устройства должны работать несколько часов в день в летнее время. Промышленные устройства работают круглосуточно без выходных в течение всего года. Так как они должны работать безостановочно, они проектируются по-другому и оснащаются более надежными двигателями и компонентами, что повышает их цену.

Обеспечив свой вычислительный центр стабилизированным питанием, вы должны подвести питание к стойкам. Хороший способ сделать это – проложить подвесную шину питания, что даст вам возможность подвести к каждой стойке разные напряжения, если у вас есть оборудование, требующее нестандартного питания, что встречается среди оборудования высшего класса. Кроме того, подвесной монтаж снижает риск контакта с водой на полу или под фальшполом, например, от утечки из кондиционера или из водопроводных труб. Электрические розетки можно разместить подальше от источников протечек и закрыть чем-нибудь от брызг. При наличии фальшпола нужно установить под ним датчики воды. Строительный подрядчик, скорее всего, поможет вам найти впадины, где вода будет скапливаться в первую очередь. Кроме того, следует разместить датчики под кондиционером.

Подвесная шина также дает большую гибкость в количестве питания для каждой стойки, так как у стоек может быть разная потребность в питании, а между стойками дополнительные кабели питания лучше не прокладывать. Оборудование, получающее питание из соседней стойки, может быть непреднамеренно обесточено, если кто-то, работающий с соседней стойкой, не знает о зависимости другой стойки. Опыт показывает, что лучше по возможности размещать все в пределах одной стойки.

Блок распределения питания внешне похож на электрический удлинитель, но в его внутренней разводке к разным розеткам подведено питание от разных цепей. Распределительный блок снижает шанс перегрузки, тогда как обычный удлинитель – нет.

На рис. 6.5 и 6.6 показаны примеры подвесных шин питания и распределительных блоков соответственно. Также на рис. 6.5 можно увидеть, как выглядит аккуратная инфраструктура сетевых кабелей.

Некоторые блоки распределения питания обладают функцией **удаленного управления питанием**, то есть дают возможность удаленно управлять каждым отдельным разъемом питания. Возможность включить или выключить конкретный разъем позволит не ходить в вычислительный центр, когда машине не хватает обычной перезагрузки. Такие распределительные блоки очень дороги, и сложно оправдать их использование для всего оборудования. Часто использование такого типа блоков распределения ограничено сетевым оборудованием, используемым для внешних подключений к информационному центру, и оборудованием, необходимым для удаленного управления другим оборудованием.

Распределительные блоки с удаленным управлением питанием

Блоки распределения питания с удаленным управлением питанием также распространены в местах, где нет людей, или в офисах с недостаточным

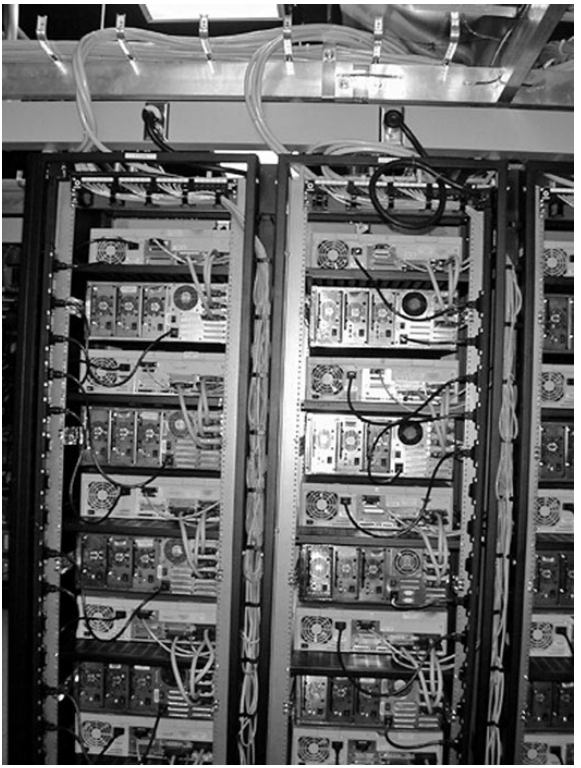

Рис. 6.5. *Стойки с узлами сети в корпорации GNAC с патч-панелью наверху и консолями, подключенными к патч-панелям. Сетевые и консольные кабели различаются по цвету*

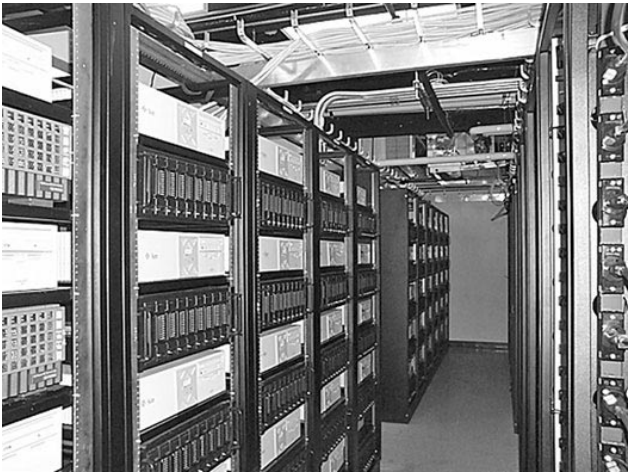

Рис. 6.6. *Вычислительный центр корпорации GNAC с предварительно проложенными подвесными сетевыми и электрическими кабелями*

количеством техников, например в небольших торговых офисах. Некоторые распределительные блоки могут управляться тоновыми сигналами с телефона. Возможность удаленно включить и выключить узел существенно сокращает время, необходимое для того, чтобы вернуть в строй недоступный сервер.

Питание должно правильно распределяться внутри стойки с помощью распределительного блока питания. Если в вычислительном центре есть разные источники питания, обеспечивающие защищенное или незащищенное питание или питание от двух раздельных систем бесперебойного питания и генераторов, они должны быть однозначно идентифицируемыми по цвету розеток распределительного блока. Существует множество вариантов распределительных блоков, в том числе для вертикального и горизонтального монтажа в стойке. Если позволяют габариты стоек и оборудования, лучше использовать вертикальные. Подробнее об этом рассказано в разделе 6.1.7.

В любом случае проверьте, где находится выключатель питания распределительного блока и насколько легко его случайно задеть и выключить. В некоторых блоках распределения питания выключатель закрыт небольшим кожухом, который нужно открыть, чтобы получить доступ к выключателю. Будет плохо, если кто-то случайно отключит питание всей стойки.

Распределительные блоки вверх ногами

Технический руководитель компании Synopsys всегда монтировал горизонтальные распределительные блоки в стойках вверх ногами. Это было обусловлено тем, что на блоках распределения питания был большой выключатель, нажатие на который обесточивало распределительный блок. Он решил, что можно легко прислониться к распределительному блоку и выключить его. Однако если блок перевернуть, то менее вероятно, что кто-то случайно переключит выключатель вверх.

Один из блоков распределения питания не был смонтирован вверх ногами новым системным администратором, которому не сказали об этой методике и который не читал документацию. Спустя несколько месяцев другой системный администратор случайно задел этот распределительный блок и нажал на выключатель, обесточив несколько важных серверов. После этого все решили, что лучше сразу предупреждать всех новых системных администраторов об этой особенности.

6.1.5. Системы пожаротушения

Настоятельно рекомендуется установить в вычислительном центре систему пожаротушения, даже если этого не требуют местные законодательные акты. Блоки питания, батареи ИБП и диски могут случайно перегореть или загореться. При проблемах с электропроводкой может возникнуть искра, которая подожжет находящиеся поблизости материалы.

Как правило, местные законодательные акты не только требуют наличия системы пожаротушения, но и четко оговаривают, какие системы можно использовать, а какие нельзя. Этот список постоянно меняется по мере того, как выясняются новые изъяны систем, в частности опасность, которую они представляют для людей в помещении при своей активации. Если у вас есть выбор, подумайте, какой опасности могут подвергаться люди, работающие в помещении; насколько вредное воздействие система оказывает на окружающую среду; какой ущерб она может нанести оборудованию, не подверженному пожару; а также насколько хорошо система справляется с возгоранием электроаппаратуры.

Еще один фактор, который необходимо учесть, – стоит ли связать активацию системы пожаротушения с переключателем, отключающим питание в компьютерном зале. Например, если вы собираетесь облить водой все оборудование, необходимо сначала отключить питание. Подобный жесткий метод отключения оборудования может вызывать серьезные сбои в дальнейшей работе аппаратуры, но не настолько серьезные, как обливание водой работающего оборудования.

Выясните, позволит ли выбранная вами система пожаротушения работать остальному оборудованию. Если нет, можно ли локализовать пожаротушение в пределах нескольких стоек? В некоторых системах предусмотрен блок предварительной активации, который сообщает сотрудникам о небольшом локальном облаке дыма перед активацией системы пожаротушения. Это дает сотрудникам время на отключение задымившегося устройства, прежде чем начнется пожар и система пожаротушения активируется в полном масштабе.

Помимо технологии вашей системы пожаротушения, вам необходимо установить несколько важных процедурных компонентов. Если ваша система пожаротушения связана с оперативным центром, необходимо проинструктировать сотрудников этого центра, что они должны делать в случае тревоги. Если в помещении круглосуточно дежурят люди, которые не разбираются в компьютерах, для них необходимо провести инструктаж, как следует реагировать на пожарную тревогу. После активации системы пожаротушения вам, скорее всего, придется какое-то время обойтись без нее, так как системе нужно время на дозаправку. Если пожар вновь разгорится после активации системы пожаротушения, вы рискуете потерять все здание. Вам необходима четкая процедура, которая позволит максимально снизить риск повторного возгорания, а также отследить и эффективно ликвидировать его в случае возникновения.

6.1.6. Стойки

Оборудование в вычислительном центре, как правило, крепится в стойки. На первый взгляд стойки играют не такую уж важную роль. Это всего лишь металлический прокат и болты. Однако на самом деле стойки играют настолько важную роль, что определяют практически все остальные аспекты вычислительного центра. Для вычислительного центра стойки – то же самое, что позвоночник для вашего организма. Позвоночник определяет общую форму, влияя на все остальные аспекты. Каждый вид стоек предназначен для определенной цели. Некоторые больше подходят для серверов, а другие – для сетевого оборудования.

Стойки позволяют организовать оборудование. Грамотная организация позволяет разместить в помещении большее количество компьютеров. Повышенная плотность достигается благодаря вертикальному размещению оборудования

в стойках. Если бы машины размещались на полу или столах, вычислительные центры занимали бы гораздо бóльшую площадь. Когда машины стоят буквально друг на друге, сложно работать на нижней машине, не затронув при этом верхнюю.

Стойки – часть системы охлаждения. Воздушные потоки в помещении в основном определяются расположением стоек. Внутри самой стойки хороший воздушный поток позволяет должным образом охлаждать компьютеры. Стойки с плохой проходимостью воздуха осложняют охлаждение оборудования.

Стойки – часть кабельной инфраструктуры. Возможность создать грамотную, управляемую кабельную систему в основном зависит от того, позволяют ли стойки как следует проложить кабели. Неряшливая проводка не только ужасно выглядит, но и является неэффективной. Без стоек не будет возможности управления кабелями: кабели разных машин будут путаться и постоянно оказываться на полу, где на них могут наступить. Это может привести к повреждению кабелей и их случайному отключению. Найти поврежденный кабель может быть очень сложно, а иногда и невозможно, не потянув при этом другие кабели с риском повредить или отключить их.

Стойки – часть инфраструктуры питания. Блоки распределения питания, как правило, расположены внутри стоек. Без стоек снабжение питанием станет бессистемным и повысится риск возникновения пожара из-за множества удлинителей. В результате возникнет жуткая неразбериха, которая станет настоящим кошмаром для службы поддержки. Стойки позволяют разделить кабели питания и сетевые кабели, что снижает количество сетевых проблем.

Тип стоек и их расположение повлияют на количество и вид используемого пространства.

Отличный продавец стоек

Когда Том занимался созданием компьютерного зала в Lumeta, продавец стоек, с которым Том работал, практически спроектировал весь зал, включая систему охлаждения, питания и кабелей. Продавец объяснил, что, если что-то произойдет с охлаждением, техник в первую очередь все свалит на стойки. То же самое касается распределения питания и укладки кабелей. Он решил, что поскольку люди могут обвинить его в отказе систем охлаждения, питания и кабелей, то он должен убедиться в том, чтобы они были спроектированы как положено. И хотя это не входило в обязанности продавца стоек и сам он не получал за это никакой компенсации, он помог оценить другие проекты и планы компьютерного зала. Том был определенно рад получить дополнительные услуги в придачу к стойкам!

Выбор стоек – не такое простое дело, как может показаться на первый взгляд. Необходимо учитывать множество факторов. Основные – это количество вертикальных штанг (две или четыре), высота, ширина и глубина стойки. Кроме того, стоит учесть вентиляцию воздуха в стойке, прочность стойки, наличие отверстий с резьбой, а также возможность установки вертикальных рельс и полок. Кроме того, проверьте, понадобятся ли вам передние, задние или боковые панели стоек, а также продумайте возможности управления кабелями.

6.1.6.1. Обзор стоек

Стойки часто называют *19-дюймовыми стойками* из-за того, что изначально они использовались в мире телекоммуникаций и их ширина составляла 19 дюймов. Вертикальные перекладины, к которым крепится оборудование, называются *рельсами*. Как правило, две или четыре рельсы располагаются на расстоянии 17,75 дюймов (45 см) друг от друга. Вместе с их собственной толщиной это обычно составляет ровно 19 дюймов[1]. У современных стоек есть по бокам дополнительные крепежи для кабелей, которые увеличивают ширину стоек.

Отверстия в стойках располагаются группами по три: над первым отверстием на расстоянии 0,5 дюйма (12,7 мм) расположено второе; выше, через 0,625 дюйма (15,875 мм), идет следующее отверстие; и через 0,625 дюйма (15,875 мм) – еще одно. Далее образец расположения повторяется.

Вертикальное расстояние между двумя крайними отверстиями из трех называется *рэк-юнитом*, или U (от англ. unit). 1U равен 1,75 дюйма (4,5 см). Высота оборудования измеряется в рэк-юнитах, или U. Дисковый массив может иметь высоту 4U, крупный сервер – 8U, 16U или даже больше. Высота небольших серверов, как правило, составляет 2U, если у них много дисков, и 1U, если нет. Устройство высотой 1U из-за его формы часто называют «*коробкой от пиццы*». Высота стандартной полноразмерной стойки составляет 42U.

У системных администраторов-новичков могут возникать проблемы, но, если установить устройство, начиная с первого отверстия в группе из трех, все остальные устройства ниже и выше первого встанут в стойку идеально. Другими словами, отверстие, которое кажется первым, на самом деле является третьим в предыдущей группе отверстий. Если начать установку оборудования с неверного отверстия, все остальные устройства не встанут должным образом и придется оставить между ними промежуток, начав установку следующего устройства с первого отверстия в очередной группе.

На хороших стойках имеются отметки, обозначающие первые отверстия в каждой группе из трех отверстий. Кроме того, на хороших стойках все отверстия пронумерованы. Если вам нужно найти пару одному из отверстий на другой стороне, достаточно просто отыскать отверстие с тем же номером. Без такой нумерации даже самый толковый системный администратор почувствует себя идиотом, подняв оборудование на стойку и выяснив, что вроде бы правильное отверстие вовсе таковым не является. И как это ни удивительно, нумерация отверстий появилась не так давно (если вам этот абзац показался странным, спросите об этом у системного администратора постарше).

У более старых стоек оборудование крепится болтами к круглым отверстиям с резьбой. Иногда эти отверстия загрязняются, резьба срывается и данную часть стойки дальше использовать невозможно. У стоек разных производителей отверстия могут быть разного диаметра, и иногда на поиск подходящих болтов уходит немало усилий. У стоек с отверстиями без резьбы эти проблемы решаются простым наличием болта и гайки. Если резьба вдруг сорвется, достаточно заменить болт и гайку.

В современных стойках болты не используются, а отверстия квадратные. На устройствах предусмотрены зацепы, которые проходят в квадратное отверстие по диагонали. Устройство устанавливается в стойку, и его удерживает сила тяжести. Крупногабаритное оборудование закрепляется дополнительными винтами. Более старое оборудование можно установить в такие стойки с помо-

[1] См. *http://en.wikipedia.org/wiki/19-inch_rack*.

щью **монтажных гаек** – металлических квадратов с резьбовым отверстием. Монтажная гайка вставляется в квадратное отверстие, и оборудование крепится к ней болтами. Когда болт туго затянут, гайка блокируется в отверстии. Если резьба монтажной гайки загрязняется или срывается, гайку можно просто заменить. Так как вы покупаете болты и монтажные гайки одновременно, вы точно знаете, что они друг другу подходят. Однако будьте осторожны при замене гаек, чтобы не повредить свои пальцы (возможно, вам стоит приобрести **инструмент для установки и изъятия монтажных гаек** за 40 долларов). Новое оборудование можно закрепить в старых стойках с резьбовыми отверстиями с помощью наборов специальных инструментов. Такие наборы, как правило, дорого стоят.

6.1.6.2. Вертикальные штанги

Рельсы по углам стойки называют *вертикальными штангами*. Стойки могут быть двухштанговыми (или однорамными) и четырехштанговыми (или двухрамными).

Однорамные стойки, как правило, используются для сетевого и телекоммуникационного оборудования, для которого обычно предусмотрена возможность центрального крепления, а также крепления на лицевой и/или задней панели. Однако часто проще и безопаснее установить крупногабаритное сетевое и телекоммуникационное оборудование в двухрамную стойку, которая лучше защищает аппаратуру от случайных толчков, способных ослабить или повредить кабели. Кроме того, двухрамные стойки, как правило, лучше приспособлены для горизонтальной укладки кабелей.

Бóльшая часть серверного оборудования предусматривает крепление только на лицевой панели, хотя некоторые серверы имеют возможность центрального крепления или крепления на задней панели. При креплении лицевых панелей в однорамных стойках аппаратура будет выпирать с задней стороны и устройства различной глубины будут выдаваться на разное расстояние. Это может представлять опасность как для людей, проходящих за стойкой, так и для оборудования. Полноразмерные полки для однорамных стоек крепятся по центру, как правило, в виде двух половинных полок: одна – за переднюю панель и одна – за заднюю. Установка оборудования с креплением на лицевой панели и полок (или оборудования с центральным креплением) означает, что полезная глубина такой стойки больше глубины двухрамной стойки, где все выравнивается по лицевой панели.

Однорамные стойки дешевле двухрамных, поэтому они используются во многих компаниях. Однако с двухрамными стойками работать приятнее.

Если в вашей компании решили приобрести однорамные стойки, при их установке удостоверьтесь, что между рядами достаточно свободного места. Проходы должны быть достаточно широкими, чтобы вместить полторы глубины оборудования плюс пространство для прохода людей. Минимальная ширина проходов, как правило, указана в правилах пожарной безопасности. Машины не могут выступать в это пространство. Причина, по которой пространство между рядами рассчитывается исходя из полуторной глубины оборудования плюс минимальная ширина прохода, – возможная установка крупной машины с передним креплением в один юнит и оборудования с центральным креплением или полки в стойке позади нее.

У стоек могут быть дополнительные ножки, которые выступают в проход. Они предотвращают падение стойки при выдвижении серверов.

Пример: недостаточно широкие проходы

Одна компания арендовала часть помещения с сетчатым ограждением и несколько стоек в вычислительном центре, сделав свой выбор на основе стоимости стоечной площади. Между однорамными стойками были слишком узкие проходы. Когда в оба ряда установили оборудование, получить доступ к аппаратуре в заднем ряду стало невозможно. Более того, кабели с заднего ряда оказались настолько близко к ограждению, что просто-напросто торчали из него (из-за чего наличие сетчатого ограждения вообще теряло смысл). Системные администраторы, вынужденные трудиться в таких условиях, возненавидели свою работу, но иного выхода не было. В контракте была оговорена площадь огороженной части помещения и количество стоек. Системным администраторам нужно было более тщательно все измерить и просчитать прежде, чем подписывать контракт.

6.1.6.3. Высота

Высота стойки может влиять на надежность, если стойка высокая и системному администратору приходится тянуться к машине через другое оборудование. Кроме того, высокие стойки могут просто не уместиться в помещении, если к потолку что-нибудь прикреплено (например, шины питания, системы охлаждения или противопожарные системы) или над ними будет недостаточно места для циркуляции воздуха либо нормальной работы противопожарной системы. Может быть опасно выдвигать полки в верхней части стойки. С другой стороны, высокие стойки позволяют более эффективно использовать пространство в вычислительном центре.

6.1.6.4. Ширина

Большинство оборудования подходит для 19-дюймовых стоек, но телекоммуникационное оборудование, как правило, устанавливается в стойки, совместимые с системой построения сетевого оборудования (NEBS, Network Equipment Building System). У таких стоек расстояние между штангами составляет 21 дюйм (53,3 см). Однако обычно NEBS-оборудование поставляется с собственной стойкой, поэтому достаточно отвести место для стойки и не беспокоиться о покупке самой стойки. В зависимости от типа вашего оборудования вам необходимо создать план помещения, распределив пространство соответствующим образом. На плане могут быть предусмотрены места для стоек разной или одинаковой ширины.

Если у нас есть выбор, мы предпочитаем более широкие стойки. Дополнительная ширина упрощает размещение кабелей.

6.1.6.5. Глубина

Двухрамные стойки могут быть различной глубины из-за различных габаритов оборудования. Стоит выбирать стойки, глубина которых позволяет целиком разместить в них аппаратуру, чтобы все кабели были защищены от случайных задеваний и при необходимости можно было бы использовать в стойке горизонтальную укладку кабелей. Если машины будут выступать в проходах, появится

угроза безопасности. Кроме того, если из-за выступающих устройств ширина прохода окажется слишком малой, это может стать нарушением местных правил техники безопасности. К тому же, если все оборудование полностью умещается в стойках, это выглядит не только аккуратно, но и профессионально. Однако, если глубина стоек слишком большая, можно очень быстро занять всю площадь в помещении и при этом не разместить все нужное оборудование. При наличии свободного пространства идея установить дополнительное оборудование с задней стороны стоек может быть очень соблазнительной. Однако при этом доступ к кабелям или задним панелям других машин будет затруднен. Будет сложно обслуживать другие машины, установленные в той же стойке. В результате плохой циркуляции воздуха оборудование может перегреваться.

Пытаясь сделать 1U-серверы все более и более функциональными, поставщики увеличивают их глубину. Некоторые серверы могут в принципе не уместиться в старые стойки из-за недостаточной глубины последних.

Неудачное использование пустого пространства

У одной компании в вычислительном центре не хватало места, пока строился дополнительный вычислительный центр. Однако системные администраторы должны были устанавливать машины. Системные администраторы поняли, что во многих старых отдельных машинах есть неиспользуемое пространство, в которое можно установить дополнительные платы и диски. Системные администраторы начали устанавливать более компактные машины в работающие старые машины, кропотливо наклеивая ярлыки на большие машины и перечисляя на них все оборудование внутри. Такая практика была достаточно необычной и значительно усложнила поиск машин, если системные администраторы забывали, что крупные машины использовались в качестве дополнительных стоек. Однако единственной реальной проблемой стал тот факт, что они потребляли больше электроэнергии на квадратный фут, чем могли дать ИБП, так как в вычислительном центре было слишком много машин. В идеале нужно было подготовить новый вычислительный центр до того, как возникла подобная ситуация.

6.1.6.6. Циркуляция воздуха

Тепло отводится от оборудования благодаря циркуляции воздуха. В некоторых стойках предусмотрены встроенные вентиляторы, позволяющие усилить поток воздуха. Если хотите приобрести такие стойки, обдумайте способ, с помощью которого воздух будет в них попадать. Может потребоваться фальшпол с перфорацией, чтобы воздух подавался в стойку снизу. Если вы выбрали более простую стойку, не оснащенную собственной системой циркуляции воздуха, вам, возможно, не стоит устанавливать дверцы для передней, задней или боковых панелей, чтобы они не препятствовали потоку воздуха, охлаждающему оборудование в стойке. Благодаря дверцам и боковым панелям вычислительный центр будет выглядеть аккуратнее, однако многие ошибки подключения кабелей будут скрыты и проложить аккуратную проводку в стойках будет сложнее,

если стойки уже не поставляются с готовой проводкой (раздел 6.1.7). Аккуратная проводка возможна, как показано на рис. 6.5 и 6.7, но она потребует поддержания порядка.

Стойки с дверцами

Том предпочитает стойки с дверцами. Если дверца не закрывается, значит, что-то сделано неправильно. Системный администратор не отойдет от стойки, если с нее свисают провода, после того как он произвел какие-то изменения. Однако, так как стойки с дверцами сложнее охлаждать, Том использует их только в случае, если охлаждение вообще не требуется, например в качестве стоек только для сетевых патч-панелей.

Кристина предпочитает стойки без дверец. Она с одного взгляда может определить, все ли правильно было сделано, и в случае необходимости исправляет ошибки до того, как ситуация выйдет из-под контроля.

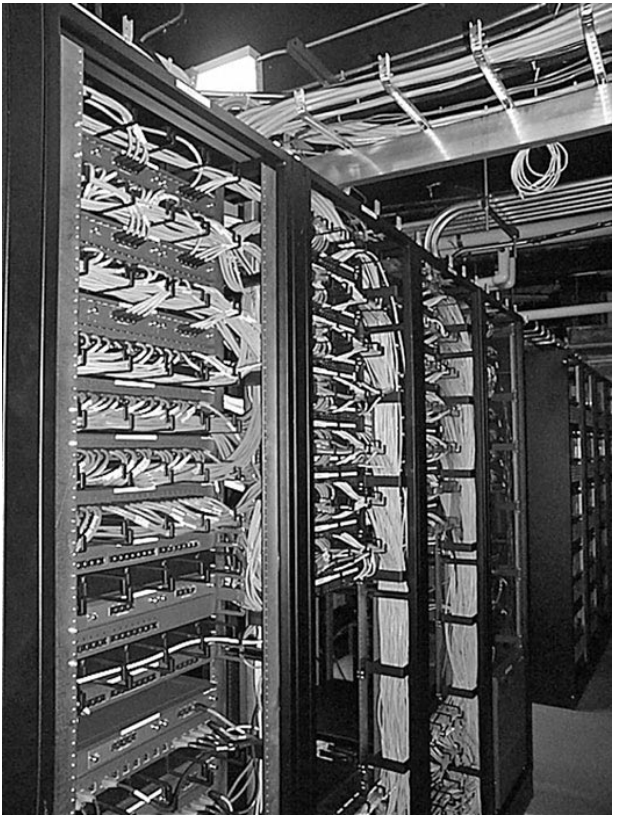

Рис. 6.7. *Сетевые стойки в корпорации GNAC. В одной стойке установлены патч-панели, а в соседней – сетевые устройства*

6.1.6.7. Укладка кабеля

При приобретении стойки всегда продумывайте укладку кабелей. В общем, рекомендуется сразу приобрести инструменты для укладки кабелей. Чтобы определить, что именно вам необходимо, продумайте, каким образом вы собираетесь прокладывать проводку в своем вычислительном центре (подробности в разделе 6.1.7). Обдумайте возможность горизонтальной и вертикальной укладки кабелей. Кабели, должным образом уложенные между стойками и внутри них, позволят работать эффективно, не затрагивая при этом другое оборудование. Распутывание кабелей – достаточно непростое дело. Кроме того, оно всегда сопровождается отключением аппаратуры. Если вы не обеспечите должное управление кабелями, люди начнут подключать оборудование, как им заблагорассудится. В результате выяснится, что не получится вытащить неисправное устройство из стойки, чтобы заменить его, не отключив при этом три других критически важных устройства, которые не имеют ничего общего с нужной вам машиной.

Горизонтальная укладка кабелей по рельсам стойки может быть открытой или закрытой. При открытой укладке используются крупные разрезные кольца, за которыми проходят кабели. Кабели через определенные отрезки укладываются в кольца, которые помогают удержать кабели на месте. При закрытой укладке кабели располагаются в закрывающихся коробах. Крышка короба снимается, кабели размещаются внутри, и крышка вновь закрывается. Открытая укладка может показаться менее аккуратной, если не поддерживать ее в должном виде, но при закрытой укладке в коробах часто прячут огромные петли, если кабель оказался слишком длинным. Если же короба полностью забиты, установить крышку может быть сложно или невозможно и ее просто не устанавливают. В результате такая укладка становится еще более неряшливой, чем открытая. Кроме того, с закрытой укладкой работать очень утомительно. Ощутимых преимуществ она не дает, а проблем с ней предостаточно.

В некоторых стойках предусмотрена вертикальная укладка кабелей в углубления между стойками. В других стойках углубления расположены с внутренней стороны на задних штангах. В третьих стойках крепежи сделаны на задних штангах с внешней стороны. Если крепежи для кабелей находятся между стойками, кабели будут занимать больше ценного пространства. Если направляющие крепятся с задней стороны стоек, кабели будут выступать в проходы, что, во-первых, делает их более уязвимыми, а во-вторых, может быть нарушением техники безопасности. Если кабели укладываются внутри стойки, стойки должны быть достаточно глубокими, чтобы в них умещалось самое крупногабаритное оборудование плюс кабели. И, где бы ни устанавливались крепежи для кабелей, они могут быть открытыми или закрытыми.

Крепежи для кабелей также могут быть различной ширины. В вычислительных центрах, как правило, используются крепежи разной ширины в зависимости от назначения стоек. В стойках, в которых установлено много коммутационных панелей, сетевого и консольного оборудования, будет и много кабелей. Для таких стоек требуются более широкие и глубокие кабельные крепежи, чем для стоек, в которых установлена пара узлов с несколькими сетевыми и консольными подключениями. Если в стойке много кабелей, потребуется горизонтальная укладка, хорошо распределенная между аппаратурой и различными коммутационными панелями. Недостаток места для укладки кабелей грозит не только лишней тратой нервов, но и спонтанными решениями, которые очень сложно контролировать. Это затруднит доступ к кабелям, и системные администраторы могут повредить кабели, пытаясь затолкнуть их в крепежи. Лучше переоценить, чем недооценить требования к пространству.

6.1.6.8. Прочность

Стойки должны быть достаточно прочными, чтобы выдержать вес устанавливаемого в них оборудования. Как уже говорилось ранее, в сейсмоопасных регионах могут быть повышенные требования к прочности стоек.

6.1.6.9. Окружающая среда

Если ваши стойки будут установлены в удаленных районах, учитывайте факторы окружающей среды в этих районах. Например, в Китае повсеместное использование угля приводит к загрязнению воздуха серой. Сера приводит к высокой влажности воздуха, что, в свою очередь, способствует появлению ржавчины на стойках. Чтобы предотвратить ржавчину, можно использовать специальное покрытие.

6.1.6.10. Полки

Малогабаритное оборудование, не предназначенное для установки в стойку, можно разместить на полке. Есть специальные полки, устанавливаемые в стойки.

Тщательно продумайте, как полки и различное оборудование будут установлены в стойке, а также каким образом, если это вообще возможно, следует объединить разную аппаратуру в одной стойке. Продумайте, можно ли установить полки в стойки, в которых вертикальные рельсы передвигаются вперед или назад. Зачастую крупное оборудование для стоек требует определенного расстояния между вертикальными рельсами, чтобы можно было прикрепить аппаратуру со всех четырех углов. В некоторых случаях положение этих рельсов может помешать установить другое оборудование, которое требует другого расстояния между рельсами. Что еще хуже, для полок может потребоваться определенное положение рельсов, несовместимое с другим оборудованием. Удостоверьтесь, что выбранные вами стойки позволяют устанавливать полки при разных положениях вертикальных рельсов. Возможно, вам также стоит приобрести дополнительные вертикальные рельсы, чтобы в одну стойку можно было установить пару устройств разной глубины.

6.1.6.11. Дополнительная площадь

Подсчитайте количество крупного, свободно стоящего оборудования, которое занимает площадь, сопоставимую со стойкой или больше, и при этом не может быть установлено в стойку. Если вы оставите место для такого оборудования, это повлияет на количество заказываемых вами стоек и на план проводки в вычислительном центре.

6.1.7. Проводка

В вычислительном центре держать проводку в порядке достаточно сложно. Однако при планировании центра у вас есть несколько способов, с помощью которых вы облегчите системным администраторам задачу по поддержке проводки в приличном состоянии.

Скрыть беспорядок – не значит устранить его. Если беспорядка не видно, это не значит, что он не отразится на работе системных администраторов. Фальшпол поможет скрыть неряшливые кабели, которые будут путаться как попало. Вы-

таскивая тот или иной кабель из-под пола, вы обнаружите, что он запутался среди прочих кабелей. Возможно, и вытащить его будет не так просто. Это приведет к тому, что кабели будут просто оставлять на месте, чтобы разобраться с ними «позже, когда будет время».

Кабели под фальшполом

В одной компании в самом старом вычислительном центре был фальшпол. Под ним проходила проводка, и старые кабели оттуда вообще не убирали. Они просто накапливались там слой за слоем. В компанию пришел новый системный администратор, который вскоре решил в свое свободное время вытащить из-под пола все неиспользуемые кабели. В некоторых местах было так много кабелей, что новые с трудом туда помещались. За три месяца он вытащил из-под пола две мили кабелей.

Лучшее, что вы можете сделать, – это заранее максимально подготовить проводку на стойках. Выберите в вычислительном центре отделение, в котором будет установлено только сетевое оборудование. Например, задний ряд. Затем на верх каждой стойки установите патч-панель с хорошо читающимся ярлыком. К панели с запасом подключите кабели. Сделайте хорошо читающийся ярлык для стоек.

На ярлыках стоек должен быть указан ряд и позиция стойки в ряду. Ярлыки разместите на стенах достаточно высоко, чтобы их было видно с любой точки и стойки можно было легко найти. На рис. 6.8 и 6.9 показаны примеры таких ярлыков для стоек и коммутационных панелей.

Подключите патч-панель стойки к патч-панели в вашем сетевом ряду, на которую наклеен соответствующий ярлык и указан номер стойки. Если вы используете консольные серверы, установите один из них в верхнюю часть каждой стойки, если это позволяет их размер. Если же серверы слишком крупные, установите патч-панели для консолей в каждую стойку, которая соединена с консольным сервером, установленным рядом. Либо можете увеличить количество кабелей, подключенных к заднему ряду центра, и разместить консольные серверы с сетевым оборудованием. Подобный пример изображен на рис. 6.10.

Рис. 6.8. *Нумерация на верхней части стен в вычислительном центре в компании Synopsys, которая используется для идентификации стоек и упрощает их поиск*

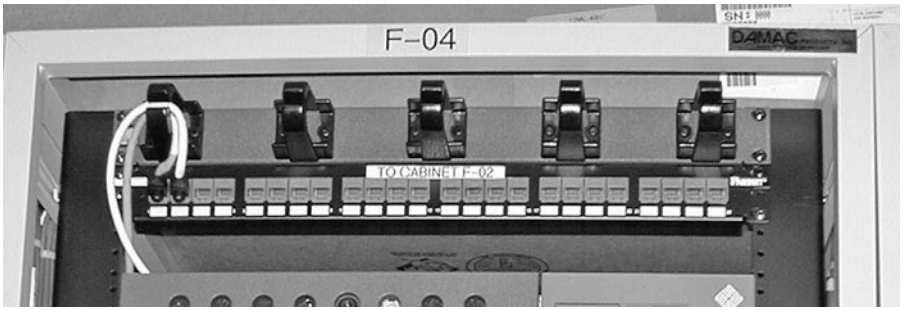

Рис. 6.9. *На верхней части стоек в компании Synopsys наклеены ярлыки и установлены патч-панели, где указана стойка, в которой они находятся*

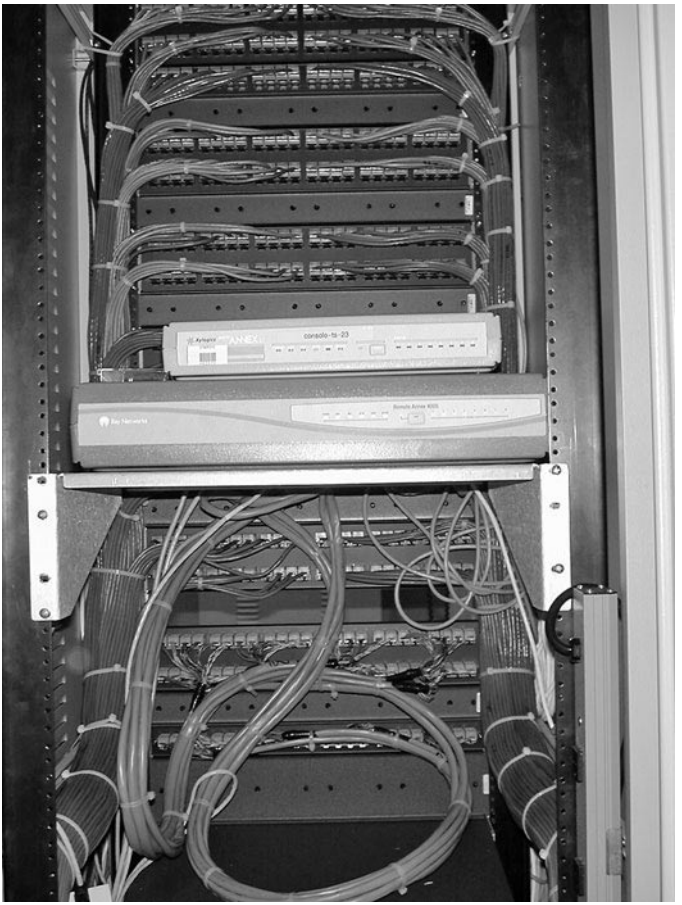

Рис. 6.10. *В компании Synopsys последовательные консольные концентраторы хранятся в сетевых стойках, а особые кабели используются для прямого их подключения к патч-панели*

В некоторых корпоративных сетях используют сетевые кабели разных цветов. По крайней мере, кабели разного назначения (категория 5, категория 6) и кабели с разной разводкой (прямой, кроссоверный) должны быть разных цветов. В некоторых сетях по цветам разделяют разные подсети. Мы рекомендуем использовать красный цвет для сетей, которые подключены к Интернету без брандмауэра.

Советы по патч-кабелям

Короткие сетевые кабели, которые используются для соединения машины с сетью, а также соединения двух патч-панелей или патч-панели с машиной, называются **патч-кабелями**. Как правило, длина таких кабелей составляет 1, 2 или 3 м.

Если вы разные цвета присваиваете разным типам сети или категориям кабеля, ту же систему цветов стоит использовать для патч-кабелей. Некоторые предпочитают изготавливать собственные патч-кабели. Для этого необходимо приобрести соответствующие компоненты и **устройство для обжима**. Себестоимость самодельных кабелей невысокая, что является основной причиной их изготовления. Однако время от времени из-за самодельных кабелей возникают ошибки сети и простой в работе. По мере того как скорость работы сетей увеличивается, допустимое отклонение уменьшается. Сделать кабель категории 5, который соответствовал бы всем требованиям сертификации, очень сложно. Кабель категории 6 может не пройти сертификацию из-за малейших деталей. Например, каждая витая пара должна содержать определенное количество витков на метр, а каждый виток в определенной степени снижает наводки. Чтобы к каждому концу прикрепить коннектор RJ-45, необходимо развить каждую пару. Однако, если развить пару больше чем на несколько дюймов, наводки могут вырасти настолько, что кабель не пройдет сертификацию. Требования действительно высокие. Захотите ли вы потратить уйму времени на изготовление и переделывание кабелей, прежде чем они пройдут сертификацию?

При оптовом приобретении стоимость патч-кабелей становится вполне разумной. Мы не рекомендуем изготавливать их самостоятельно.

И еще. Люди часто интересуются, почему каждый новый патч-кабель перевязан двумя стяжками. Так почему же? Дело не только в том, чтобы кабели не запутались при транспортировке. И не в том, чтобы разозлить вас, когда вы пытаетесь быстро распаковать большое количество кабелей. Причина в том, что это позволяет аккуратно организовать подключенные кабели. Распаковав кабель, развяжите стяжки и подключите кабель. Затем используйте те же самые стяжки, чтобы закрепить кабель на стойке или на рельсе. Благодаря этому ваши кабели всегда будут выглядеть аккуратно.

Все сетевые и консольные кабели для серверов, размещенных в стойке, должны располагаться в этой же стойке, не считая тех, что были проведены заранее. Удостоверьтесь, что внутри стойки достаточно места для кабелей. Приобретите кабели различной длины, чтобы всегда было можно подобрать нужный вариант. Всегда должна быть возможность использовать кабель, длина которого после прохода кабеля через все крепления позволяет чуть выдвинуть машину вперед

на случай сейсмических событий. При этом кабель не должен быть слишком длинным, чтобы не образовывались большие свисающие петли. Если узлы сети установлены на выдвижных полках, удостоверьтесь, что длина кабелей позволяет выдвинуть полку, не нарушив при этом функциональность машины. Кабели никогда нельзя пропускать в стойке по диагонали, иначе впоследствии они будут мешать производить работы в стойке. Чтобы вашим сотрудникам было проще делать все правильно, обеспечьте наличие на складе полного ассортимента кабелей разной длины. В противном случае вам придется впоследствии разбираться либо с кабелями, разбросанными по полу, либо с паутиной кабелей, переплетающихся за стойками.

Укладка кабелей в сетевом ряду потребует немало крепежа и сил, но, по крайней мере, вся работа производится в одной зоне. Кроме того, вы сможете оптимизировать эту зону, если сети являются общими для большинства или всех машин, например выделенная сеть для резервного копирования, административная сеть или подключения к последовательной консоли. Если вы знаете, что какая-то часть кабелей со стойки будет подключена к определенным пунктам, то можете подготовить все эти кабели заранее, что снизит энтропию вашей системы кабелей. Либо, если вы сможете сконфигурировать ваше сетевое оборудование, чтобы оно назначило определенный порт той или иной сети, вы будете иметь возможность заранее подготовить все кабели. На рис. 6.11 отображен набор патч-панелей.

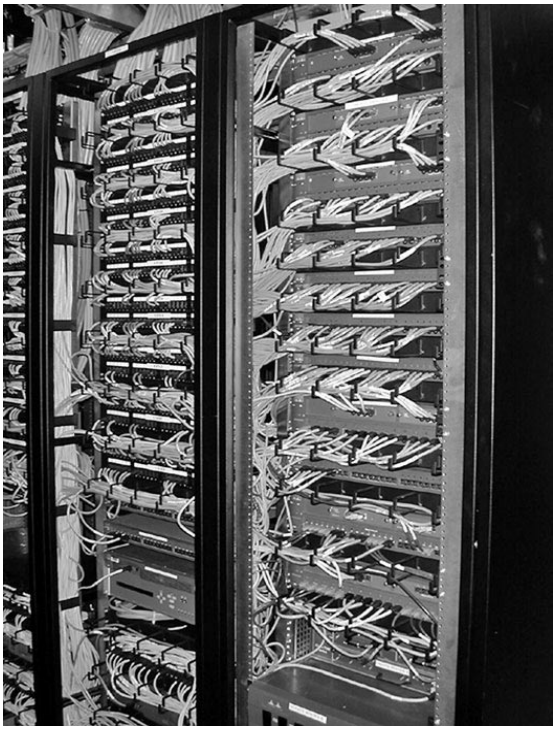

Рис. 6.11. *Сетевые стойки в корпорации GNAC (патч-панели подключены к подвесным кабелям, а те – к заранее подготовленным кабелям патч-панелей на верхней части каждой стойки с узлами сети)*

Однако хотим вас предостеречь от избыточной предварительной укладки кабелей в сетевых стойках. При отказе оборудования действовать необходимо точно, и, возможно, понадобится быстро переключить много кабелей к другому оборудованию, пока вы ищете замену неисправному. Кроме того, необходимо учитывать исключения из правил, которые обязательно проявятся. Не стоит загонять себя в угол, не оставляя никакой свободы выбора в системе кабелей.

Пример: результат хорошей проводки

Предварительная укладка кабелей для десятка сетевых подключений к каждой стойке может показаться дорогостоящим решением, но оно быстро окупается. Однажды Том контролировал работу двух машинных залов в двух разных зданиях. Только в одном из залов была сделана предварительная укладка кабелей. Во втором зале на установку каждой новой машины уходил целый день. Укладка сетевых и консольных кабелей занимала несколько часов, а порой и целый день. С годами из-за частых работ напольное покрытие стало шатким и небезопасным. Сложность и опасность работы в зале заставили системных администраторов постоянно откладывать выполнение различных задач. Стало сложно выделить 2–3 свободных часа на установку, особенно потому, что для этого требовалось два человека. В результате установка новых узлов сети могла откладываться на неделю. А успешная установка узла становилась настоящим праздником.

Во втором вычислительном центре, напротив, к каждой стойке было заранее подведено по десятку кабелей категории 5, подключенных к патч-панели, установленной рядом с сетевым оборудованием. Установка нового узла в этом центре занимала менее 15 мин. Работы по установке не откладывались и не становились из ряда вон выходящим событием. Стоимость предварительной укладки кабелей более чем компенсируется производительностью, которую она обеспечивает.

Связки кабелей

В компьютерном зале, в котором не проведена предварительная укладка кабелей, вам придется прокладывать кабель при каждой установке новой машины. Обдумайте вариант создания связки из 6 или 12 кабелей и укладки всей связки сразу. На это уйдет чуть больше времени, чем на укладку одного кабеля, но зато при установке следующей машины будет возможность использовать свободные, уже проложенные кабели. Мы рекомендуем проложить связку кабелей от сетевой стойки или ряда к стойке, в которой много пустого пространства.

Чтобы сделать связку, выполните следующее.

1. Возьмите 12 кабелей одного типа и длины. Распакуйте их, но оставьте стяжки.
2. Наклейте ярлыки на оба конца каждого кабеля. Например, на оба конца первого кабеля наклейте ярлыки A-1. На оба конца второго кабеля – ярлыки A-2. Продолжайте это, пока ярлыки не будут наклеены на все концы всех кабелей (чтобы все упростить, на следующую связку наклейте ярлыки от B-1 до B-12). Очень важно накле-

ить все ярлыки до перехода к следующему этапу. Попытки аккуратно наклеить все ярлыки после того, как все кабели проложены, могут занять несколько часов.

3. Найдите длинный свободный коридор или зал.
4. Удалите стяжки с одного кабеля, но не выкидывайте их. Проложите кабель по коридору.
5. Повторите эту процедуру со всеми остальными кабелями.
6. С помощью стяжек, оставшихся от кабелей, свяжите все кабели вместе. Связывайте их примерно через каждый фут. С каждого конца связки оставьте один-два свободных метра.
7. Вот и все!

Основными аргументами против предварительной укладки кабелей являются уменьшение свободного пространства в стойке и стоимость. Однако повышение надежности, производительности и управляемости благодаря отсутствию запутанных проводов как на полу, так и за стойками является огромным.

Далеко не везде можно предварительно уложить кабели в стойках. Например, в колокейшн-центрах, в стойках которых будет установлено оборудование пользователей, невозможно предугадать, какая именно аппаратура будет установлена и какие стойки должны быть соединены между собой или с сетевым оборудованием центра.

Еще один прием по оптимизации системы кабелей – наличие на боковых панелях стоек вертикальных блоков распределения питания с множеством розеток. Приобретите два коротких кабеля питания разной длины (например, 30 и 60 см) и подключите каждое устройство к ближайшей розетке. Как ясно из рис. 6.12, это позволит предотвратить использование длинных кабелей питания, которые могут путаться с кабелями передачи данных и вдобавок к беспорядку создавать помехи.

Разделение кабелей питания и кабелей передачи данных

В компании, где Кристина работала консультантом, системный администратор получила заявку о проблеме с сетью. Пользователь, подавший заявку, обнаружил, что передача данных между двумя узлами осуществлялась очень медленно. Системный администратор удостоверилась, что проблема действительно существует, и провела несколько тестов. Она выяснила, что сетевой интерфейс одной из машин регистрировал множество ошибок, и отправилась в вычислительный центр, чтобы проверить кабели. Она убедилась, что все подключено правильно и замена кабелей не требуется. Однако при проверке системный администратор заметила, что кабель питания машины, которую она в спешке установила чуть ранее в тот же день, пересекался с сетевым кабелем, подключенным к интерфейсу, у которого и возникли проблемы. Все остальные кабели питания были аккуратно отделены от сетевых кабелей и уложены в соответствующие крепежи. Она вспомнила слова Кристины о том, что сетевые кабели и кабели передачи данных необходимо держать отдельно

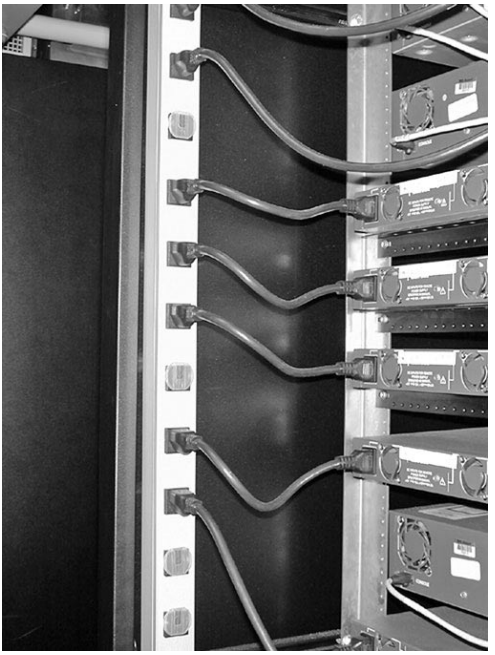

Рис. 6.12. *Вертикальные блоки распределения питания в корпорации GNAC с короткими кабелями питания, которые не только удобны, но и позволяют грамотно организовать проводку*

из-за возможных электромагнитных наводок. Поэтому она не пожалела пары минут на то, чтобы провести кабель питания через соответствующие крепежи вместе с остальными кабелями питания. При дальнейших тестах оказалось, что сетевые проблемы исчезли.

6.1.8. Маркировка

Грамотная маркировка и ярлыки необходимы для безотказной работы вычислительного центра. Все устройства должны иметь ярлыки как на лицевой, так и на задней панели. На этих ярлыках должно присутствовать полное имя устройства, которое указано в корпоративном пространстве имен (глава 8) и в системе консольного сервера (раздел 6.1.10).

Если к машине имеется несколько подключений одного вида и с первого взгляда неясно, какое из них для какой цели используется (например, несколько сетевых интерфейсов, принадлежащих разным сетям), необходимо наклеить ярлыки как на интерфейсы, так и на кабели. Здесь же полезно использовать сетевые кабели разных цветов, например, распределив цвета по разным доменам[1]. Например,

[1] В крупных компаниях достаточно сложно подобрать разные цвета для каждой сети.

у брандмауэра может быть три сетевых интерфейса: для внутренней защищенной сети, для внешней незащищенной сети и для служебной сети, доступ к которой от ненадежных сетей осуществляется через брандмауэр. Рядом с интерфейсами должны быть как минимум надписи «*внутр*», «*внешн*» и «*служ*». На кабелях должны иметься ярлыки с соответствующими надписями. При решении той или иной проблемы вы легко сможете определить, что, допустим, у внешней сети не горит индикатор соединения. А если вам необходимо снять устройство со стойки, чтобы решить аппаратную проблему, то при повторной его установке вам не придется думать, какой кабель куда подключается.

Если на сетевом устройстве много портов, приклеивать ярлык у каждого из них непрактично. Однако стоит прикрепить ярлыки к оборудованию, на котором разные порты связаны с сетями или виртуальными локальными сетями. Например, на таком ярлыке может быть следующая надпись: «192.168.1/24: платы 1–3; 192.168.15/24: платы 4, 5, 8; 192.168.27/24: платы 6, 7».

Для сетевого оборудования, подключаемого к глобальной вычислительной сети (ГВС), на ярлыке должно быть указано имя другой стороны подключения и идентификационный номер поставщика подключения. Этот ярлык должен быть на устройстве, на котором находятся индикаторы ошибок данного подключения. Например, модуль обслуживания канала и данных (CSU/DSU, Channel Service Unit/Data Service Unit) для линии T1 должен иметь ярлык вида «T1 до офиса в Сан-Диего» или «Подключение 512K к ГВС с протоколом Frame Relay». Кроме того, на этом ярлыке должен быть указан идентификатор сети поставщика T1 и его телефонный номер. Указание телефонного номера позволит сэкономить время на его поиски при сбое в работе.

Сетевое оборудование, как правило, предоставляет средства для маркировки портов в программном обеспечении. Средства программной маркировки должны использоваться в полной мере, предоставляя как минимум ту же информацию, что и обычные ярлыки. Сетевое оборудование становится малогабаритным и более интегрированным, поэтому подробную информацию на обычных ярлыках становится уместить все сложнее. Из-за этого программная маркировка является самым удобным способом хранения информации, которая необходима при отладке.

Использование вместе стандартных ярлыков и программной маркировки обеспечивает наличие нескольких источников «знания». Важно удостовериться, что оба эти средства синхронизированы и предоставляют одну и ту же информацию. Назначьте кого-нибудь ответственным за обеспечение идентичной информации на стандартных и программных ярлыках, проверку корректности информации и устранение несоответствий. Нет ничего хуже, чем несколько несоответствующих источников информации, когда вы пытаетесь исправить проблему. Для обновления ярлыков требуется усердие, время и силы. Но это экономит массу времени при отказе оборудования, когда необходимо отреагировать максимально быстро. Кроме того, это может предотвратить случайные ошибки, если кто-то подключает кабель не туда, куда следует.

Наклеивание ярлыков на оба конца всех кабелей – работа достаточно утомительная, особенно если приходится использовать старые кабели и удалять имеющиеся на них ярлыки, прежде чем наклеить новые. Кроме того, к сожалению, приклеивать ярлыки к кабелям сложно из-за того, что не все ярлыки долго держатся на изоляции. Хорошая альтернатива – приобрести кабели с уже готовыми ярлыками, на которых указан тип и длина кабеля, а также уникальный цифровой код на обоих концах кабеля. Ваш поставщик кабелей должен предоставить вам эту услугу, включая систему отслеживания уникальных ко-

дов. Таким образом, у вас будет простой способ найти второй конец кабеля (если вы примерно знаете, где он находится), вместо того чтобы искать его вручную. Даже если вам придется искать его вручную, вы будете иметь уверенность, что нашли верный кабель, до того, как отсоедините его. Для этого достаточно лишь сверить цифры. Альтернативный способ – найти стяжки с плоскими концами, на которые можно наклеить ярлык. Их можно навесить на каждый конец кабеля, и ярлыки на таких стяжках менять довольно просто.

Если вы наклеиваете ярлыки на кабели вручную, делайте это до укладки кабелей. Это стоит повторить: сначала ярлык, потом укладка. В противном случае вы полдня проведете, играя в угадайку, пока будете наклеивать ярлыки на уже проложенные кабели. Это мы знаем по собственному опыту.

Политика внедрения стандартов маркировки

В Eircom очень жесткая политика маркировки. Серверы должны иметь ярлыки на лицевой и задней панелях. На конце каждого кабеля питания должно быть указано имя машины, к которой этот кабель подключен. На сетевых кабелях ярлыков нет, но они все строго разделяются по цветам. Политика маркировки кратко и четко описана в памятке, висящей на стене вычислительного центра (рис. 6.13). Проводятся периодические проверки ярлыков, любой сервер или кабель питания без ярлыка убирается. Эта политика четко оговаривает, что ответственность за любые возникшие проблемы несет сотрудник, установивший машину или подключивший кабель питания без ярлыка, а не человек, отключивший машину. Однако, так как проверки проводятся очень часто, машины, не соответствующие стандартам маркировки, как правило, отключаются до того, как впервые запускаются в работу.

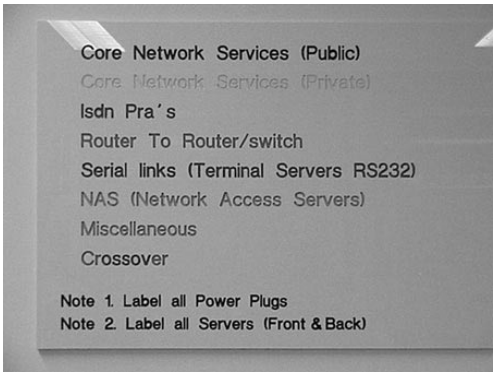

Рис. 6.13. *Памятка в вычислительном центре Eircom, в которой описана политика маркировки машин и кабелей*

6.1.9. Связь

Системным администраторам, работающим в вычислительном центре, часто приходится общаться с пользователями, другими системными администраторами (работающими за пределами центра) и поставщиками. Системным админис-

траторам может потребоваться кто-то, кто станет проверять, была ли решена проблема, кто будет следить за работоспособностью служб или заниматься поиском информации, оборудования и кадров. Иногда поставщики предпочитают поддерживать связь с сотрудником, проводящим процедуру диагностики.

Рекомендуем обеспечить какой-либо способ связи. Некоторые системные администраторы пользуются рациями или мобильными телефонами, так как многие из них редко находятся за своим рабочим столом. Все большую популярность приобретают мобильные телефоны с режимом нажми-и-говори (push-to-talk). Однако рации и мобильные телефоны могут плохо работать в вычислительных центрах из-за высокого уровня электромагнитных помех или (в некоторых компаниях) из-за экранирования от радиопомех. В некоторых случаях простые телефонные аппараты работают намного лучше. В таком случае рекомендуем установить телефон у края каждого ряда стоек. А шнур должен быть достаточно длинным, чтобы системный администратор мог в случае необходимости пройти весь ряд с трубкой в руке (рис. 6.14).

Рис. 6.14. *В Synopsys у всех системных администраторов есть рации, но в вычислительном центре стационарные телефонные аппараты работают лучше раций (обратите внимание на очень длинный шнур)*

Внимание! Мобильные телефоны с камерами

В колокейшн-центрах, как правило, запрещены фото- и видеосъемка, а следовательно, и использование мобильных телефонов с камерами.

6.1.10. Консольный доступ

Определенные задачи можно выполнить исключительно с консоли компьютера. Консольные серверы и переключатели KVM позволяют получить удаленный доступ к компьютерной консоли. Более подробно эта тема описана в разделе 4.1.8.

Консольные серверы позволяют получить консольный доступ ко всему оборудованию вычислительного центра без необходимости подключения клавиатуры, монитора и мыши к каждой системе. Наличие множества мониторов в вычислительном центре – неэффективный способ использования площади, электропитания, кондиционирования и противопожарной системы. Кроме того, клавиатуры и мониторы в вычислительном центре – это неэргономичное рабочее пространство, если вам приходится проводить много времени в консоли сервера, подключенного к монитору и клавиатуре.

Консольные серверы бывают двух основных видов. В одних есть переключатели, позволяющие подключить одну клавиатуру, видеомонитор и мышь (KVM) к портам клавиатуры, монитора и мыши нескольких машин. Старайтесь создавать подобных точек как можно меньше и располагать их в наиболее эргономичных местах вычислительного центра.

Другой тип – консольные серверы для машин, которые поддерживают последовательные консоли. К последовательному порту каждой такой машины подключается последовательное устройство, например терминальный сервер. Эти терминальные серверы подключены к сети. Как правило, определенная программа на центральном сервере все их контролирует (Fine and Romig 1990) и распределяет консоли машин по именам при аутентификации и определении уровня контроля доступа. Преимущество этой системы состоит в том, что системный администратор, пройдя аутентификацию, может получить доступ к консоли системы откуда угодно: с рабочего места, из дома или даже с дороги. Установка консольного сервера повышает производительность и удобство, а также освобождает пространство в вычислительном центре (Harris and Stansell 2000).

Также рекомендуется иметь под рукой несколько тележек с терминалами ввода-вывода или ноутбуками, которые можно использовать в качестве портативных последовательных консолей. Такие тележки можно подвезти к любой машине и использовать в качестве последовательной консоли при отказе основного консольного сервера или необходимости использовать дополнительные монитор и клавиатуру. Пример такой тележки показан на рис. 6.15.

6.1.11. Рабочее место

Еще один важный аспект любого вычислительного центра – легкий доступ к рабочему месту, оборудованному достаточным количеством розеток и антистатической поверхностью, где системный администратор может выполнять работу с машинами: устанавливать память, диски и процессоры на новое оборудование перед его установкой или решать ту или иную аппаратную проблему. В идеале рабочее место должно находиться рядом с вычислительным центром, но не внутри него. Таким образом, оно не будет использоваться в качестве временной стойки и не станет создавать беспорядок в вычислительном центре. В таких рабочих местах скапливается много пыли, особенно если там распаковывается новое оборудование. Очень важно не допускать появления пыли в вычислительном центре.

При отсутствии специального места для проведения подобных работ системным администраторам придется проводить ремонт на полу вычислительного центра,

Рис. 6.15. *В Synopsys предусмотрено несколько тележек с последовательными консолями, которые можно подвезти к машине при отказе основного консольного сервера или необходимости использовать дополнительные монитор и клавиатуру*

а новые машины собирать на своем рабочем столе, что приведет к непрофессиональному беспорядку на столе или к пирамидам из коробок и оборудования. Профессионально организованный отдел системного администрирования должен и выглядеть профессионально. А это означает, что должно быть организовано достаточно просторное и должным образом оборудованное рабочее пространство, специально выделенное для работы с аппаратурой.

Люди не должны проводить в вычислительном центре весь рабочий день

Время от времени мы сталкиваемся с ситуацией, в которой рабочие столы системных администраторов установлены непосредственно в вычислительном центре рядом со всеми машинами. Мы настоятельно рекомендуем не допускать этого.

Людям вредно проводить в вычислительном центре весь рабочий день. В таком центре поддерживается идеальная температура и влажность воздуха для компьютеров, но не для людей. В холодном помещении работать вредно для здоровья, а проводить много времени с источниками такого шума может быть даже опасно.

Кроме того, это вредно и для систем. Люди выделяют тепло. Каждому человеку, находящемуся в вычислительном центре, требуется дополнительно 600 БТЕ охлаждения. А это дополнительная нагрузка в 600 БТЕ на систему охлаждения и систему энергоснабжения.

Это невыгодно в экономическом плане. В вычислительном центре каждый квадратный метр площади значительно дороже, чем в других помещениях.

Системным администраторам необходим постоянный доступ к справочным материалам, эргономичным рабочим столам и т. д. Необходима среда, максимально повышающая производительность. Системы удаленного доступа некогда были достаточно редкими, но сейчас они стали недорогими и приобрести их очень просто.

Люди должны заходить в вычислительный центр исключительно для выполнения задач, которые невозможно осуществить каким-либо другим способом.

6.1.12. Инструменты и запасы

В вычислительном центре всегда должен иметься полный запас различных кабелей, инструментов и запасных деталей. Это проще сказать, чем сделать. В крупном отделе системного администрирования приходится постоянно отслеживать наличие запасных частей и материалов. Сами системные администраторы должны следить за тем, чтобы нужные запасы не заканчивались, а если заканчивались, то редко и ненадолго. Системный администратор, заметивший, что в вычислительном центре заканчиваются определенные запасы или предстоит использование большого количества тех или иных запасов, должен сообщить об этом сотруднику, который несет ответственность за отслеживание запасных деталей и материалов.

В идеале инструменты должны храниться в тележке с ящиками, которую в случае необходимости можно подвезти в нужное место. В крупном машинном зале потребуется несколько таких тележек. В тележке должны быть отвертки разных размеров, пара электрических шуруповертов, звездообразные отвертки, шестигранные ключи, приспособления для извлечения микросхем, игловидные кусачки, стандартные кусачки, ножи, антистатические браслеты, один-два маркировочных инструмента и все остальное, что может понадобиться (даже редко) для работы с оборудованием вычислительного центра.

Запасные детали и материалы должны быть грамотно организованы, чтобы в случае необходимости их можно было быстро найти, а также чтобы было проще проводить инвентаризацию. Некоторые вешают кабели на настенные крюки, приклеивая сверху соответствующие ярлыки. Другие используют маркированные контейнеры разных размеров, которые можно повесить на стену между рядами. Реализация подобных приемов отображена на рис. 6.16 и 6.17. Кон-

тейнеры позволяют более компактно разместить все материалы, но их местоположение необходимо распланировать еще до установки стоек в вычислительном центре. Дело в том, что такие контейнеры будут занимать значительное пространство в проходах. Небольшие предметы, такие как винты и терминаторы кабелей, необходимо хранить в контейнерах или небольших ящиках. Во многих компаниях предпочитают выделять отдельное помещение для хранения запасных частей, обеспечивая легкий доступ из этого помещения к информационному центру. Идеально для этих целей подходит рабочая комната рядом с информационным центром. Хранение запасных деталей в отдельной комнате может защитить их от события, из-за которого «погибают» используемые детали в вычислительном центре. Крупные предметы, такие как запасные машины, всегда должны храниться в отдельном помещении, чтобы не занимать ценное пространство в вычислительном центре. Ценные запасные части, такие как память и процессоры, как правило, хранятся в запирающемся шкафу.

Рис. 6.16. *В корпорации GNAC запасные материалы для вычислительного центра хранятся в маркированных синих контейнерах различных размеров*

Рис. 6.17. *В Eircom используют синие контейнеры и настенные крюки для кабелей*

Если это возможно, среди запасных частей должны быть компоненты, которые вы используете наиболее часто или которые чаще всего дают сбои. Кроме того, сюда могут входить стандартные дисковые накопители различной емкости, блоки питания, память, процессоры, кулеры или даже целые машины, если вы используете группы небольших выделенных машин для выполнения определенных функций.

Полезно иметь несколько видов тележек: двухколесные ручные тележки для перевозки ящиков, четырехколесные плоские тележки для различного оборудования, тележки с двумя и более полками для инструмента и т. д. Минипогрузчик отлично подойдет для установки тяжелого оборудования в стойки, позволяя поднять устройство на нужную высоту в стойке. После блокировки колес подъемник стабилен и оборудование устанавливается просто и без какого-либо риска.

6.1.13. Места для хранения

Простой, дешевый и эффективный способ упростить жизнь людям, работающим в вычислительном центре, – распределить место для хранения переносимых объектов. Для инструментов, хранящихся в тележке, должны быть точно распределенные и маркированные места. А для самих тележек должны быть маркированные парковочные места, где тележки будут стоять, когда ими никто не пользуется. Если кто-то пользовался приспособлением для демонтажа напольной плитки, он должен точно знать, куда этот инструмент потом положить. Зарядные устройства для инструментов, работающих на батарейках, должны храниться в строго отведенном месте. И в любом случае на мобильных объектах должны быть ярлыки с указанием места, в которое этот объект необходимо вернуть.

Пример: место для хранения инструмента

В первом вычислительном центре Synopsys, в котором был фальшпол, хранилось два приспособления для демонтажа напольной плитки. Однако определенного места для хранения этих инструментов не было и системные администраторы просто убирали их куда попало, чтобы о них никто не споткнулся. Каждый раз, когда системному администратору нужен был этот инструмент, ему приходилось искать его по всему центру. Однажды пара системных администраторов решили определить одно точное место для хранения этих инструментов. Они выбрали место на полу, где никто не ходит, и наклеили туда такой ярлык: «Здесь хранятся инструменты для плитки. Верните их сюда». На каждый инструмент приклеили ярлык «Вернуть на место в E5», воспользовавшись уже существующей маркировкой рядов в центре обработке данных. Об этом новшестве специально никому не сообщали, но когда сотрудники увидели ярлыки, они просто начали следовать указанным инструкциям: это было вполне разумно и больше не возникало необходимости обыскивать весь центр на предмет инструментов.

6.2. Тонкости

Помимо уже описанных приемов, вы можете дополнительно улучшить свой вычислительный центр. Оборудование такого центра требует больших затрат, и некоторые описанные нами улучшения могут еще больше повысить эти затраты. Но, если это возможно или если того требует коммерческая необходимость, вы можете улучшить свой вычислительный центр, сделав проходы шире и повысив избыточность систем энергоснабжения и отопления, вентиляции и кондиционирования воздуха.

6.2.1. Повышенная избыточность

Если от вас требуется особо высокая готовность, вам, среди прочего, необходимо распланировать избыточность систем электропитания и отопления, вентиляции и кондиционирования воздуха. Для этого вам необходимо разбираться в коммутационных схемах и строительных чертежах. Вы должны проконсультироваться с конструкторами системы, чтобы удостовериться, что вы усвоили малейшие детали, ведь именно малейшие детали могут все испортить, если их упустить.

Что касается систем отопления, вентиляции и кондиционирования воздуха, возможно, стоит предусмотреть наличие двух независимых систем, работающих параллельно. При отказе одной из них вторая тут же примет на себя всю нагрузку. Каждая из этих систем должна быть способна охладить все помещение в одиночку. Ваш местный техник по отоплению, вентиляции и кондиционированию сможет проконсультировать вас по поводу возможных альтернатив.

Что касается системы энергоснабжения, необходимо учитывать множество факторов. Просто продумайте, что произойдет при отказе ИБП, генератора или АВР. У вас должны быть дополнительные ИБП и генераторы, но что произойдет при отказе двух из них? Что если один из ИБП загорится? Если все ИБП находятся в одном помещении, придется отключить их все. Точно так же необходимо распределить генераторы. Подумайте над обходным выключателем, который позволит удалить из цепи вышедшие из строя устройства, вдобавок к обходному выключателю, который (в идеале) у вас уже есть для ИБП. Они не должны располагаться непосредственно рядом с оборудованием, которое вы хотите обойти. Таким образом, вы сможете получить доступ к выключателям, если устройства загорятся. Все ли электропровода проходят параллельно друг другу или в какой-то точке они пересекаются? Может ли это вызвать какие-либо проблемы?

В вычислительном центре, возможно, стоит предусмотреть несколько источников электропитания. Может быть, вам понадобится переменный и постоянный ток, но, возможно, вам также понадобится два разных источника переменного тока для оборудования, которое будет подключаться к двум источникам или для разделения питания пар избыточных машин. Если оборудование подключается к нескольким блокам питания, стоит использовать для них разные источники питания (рис. 6.18).

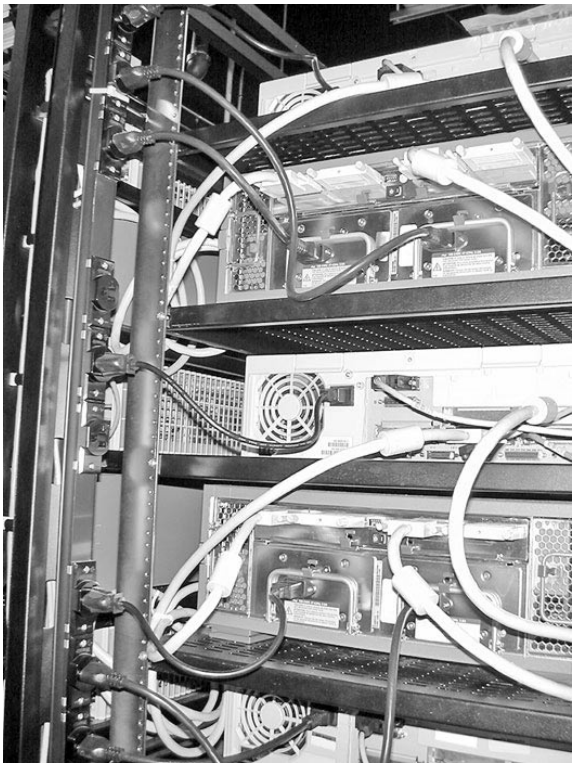

Рис. 6.18. *В корпорации GNAC три линии питания ИБП объединены в одном разветвителе. Резезвные блоки питания в одном устройстве подключены к разным линиям во избежание одновременного отключения обоих блоков питания при отказе одной из линий*

Высоконадежные вычислительные центры

В индустрии телекоммуникаций есть все необходимые концепции для создания надежного вычислительного центра, так как телефонная связь может потребоваться, например, для вызова скорой помощи и поэтому должна работать всегда. Стандарты были установлены, когда у телекоммуникационных монополистов было достаточно средств, чтобы не пожалеть усилий и сделать все как следует. NEBS (Network Equipment Building System) – американский стандарт для оборудования, которое может быть установлено в центральном офисе телефонной компании. В Европе оборудование должно соответствовать стандарту Европейского института телекоммуникационных стандартов (ETSI, European Telecommunication Standards Institute). NEBS и ETSI устанавливают физические требования и стандарты тестирования для оборудования, а также минимальные требования к самому помещению. Эти документы подробно освещают такие темы, как территориальное планирование, загрузка площадей, нагрузка на систему отопления, температура и влажность воздуха, зем-

летрясения и вибрации, пожарная безопасность, перевозки и установка, загрязнение воздуха, уровень шума, электробезопасность, электромагнитные помехи, иммунитет к электростатическим разрядам, грозовая защита, разность потенциалов постоянного тока, прочность конструкций и заземление. Все это мы перечисляем, чтобы продемонстрировать вам, насколько дотошной к мелочам является индустрия телекоммуникаций. С другой стороны, когда в последний раз было такое, что вы поднимали телефонную трубку и не слышали там длинного гудка? При создании собственных требований к высоконадежному информационному центру рекомендуем вам начать со стандартов NEBS и ETSI.

Надежный вычислительный центр также требует соответствия положениям регулирующих документов. Стандарт SAS-70 применим к обслуживающим организациям и особенно касается компаний, предоставляющих услуги через Интернет. SAS-70 расшифровывается как Statement of Auditing Standards № 70 (Положение о стандартах аудита № 70). Данное положение называется «Доклады по обработке протоколов обслуживающими организациями». Этот аудиторский стандарт был установлен Американским институтом дипломированных общественных бухгалтеров (AICPA, American Institute of Certified Public Accountants).

6.2.2. Больше пространства

Если площадь позволяет, проходы в компьютерном зале рекомендуется сделать шире, чем того требуют правила техники безопасности, чтобы можно было спокойно перемещать оборудование. В одном вычислительном центре, где побывала Кристина, проходы были достаточно широкими, чтобы положить на пол крупногабаритное устройство и провезти еще одно такое же рядом, ничего при этом не задев. В вычислительном центре Cray в городе Иган, штат Миннесота, США, проходы были в три раза шире длины самого крупного оборудования. Если вы можете выделить столько площади на проходы, учитывая долгосрочные планы (чтобы не пришлось впоследствии передвигать стойки), сделайте это. Это полезная роскошь, и благодаря ей в вычислительном центре создается более приятная атмосфера.

6.3. Идеальные вычислительные центры

Люди устраивают вычислительные центры по-разному, в соответствии со своими предпочтениями. Чтобы предоставить вам пищу для размышлений, Том и Кристина рассказали, каким они хотели бы видеть машинный зал.

6.3.1. Идеальный вычислительный центр Тома

При входе в идеальный, по моему мнению, вычислительный центр первое, что вы увидите, – это дверь с системой проверки по голосу. Чтобы устранить возможность записи и воспроизведения вашего голоса с целью открыть дверь, каждый раз вас просят повторить разные слова. И когда вы это сделаете, раздвижная дверь откроется. Дверной проем достаточно широкий, чтобы в него

мог пройти очень крупный сервер, такой как SGI Challenge XL, даже если такие серверы давно уже сняты с производства. В центре есть фальшпол, но находится он на том же уровне, что и пол коридора, поэтому никаких пандусов нет.

Центр расположен на четвертом этаже шестиэтажного здания. ИБП и системы отопления, вентиляции и кондиционирования находятся на чердаке шестого этажа, где достаточно свободного места и мощностей для подключения дополнительных систем электроснабжения и вентиляции, если в этом возникнет необходимость. Затопление такому помещению не грозит.

Все стойки одного цвета и от одного производителя, благодаря чему смотрятся очень красиво. Более того, все они были установлены одновременно, поэтому даже краска выцветает равномерно. В центре каждой третьей стойки расположен выдвижной ящик с блокнотом и парой ручек (слишком много ручек не бывает). Большинство серверов устанавливаются напрямую в стойку, но в некоторых стойках по пять полок: две под ящиком, одна над ящиком, и две на самом верху стойки. Все полки во всех стойках одной высоты, так что все выглядит достаточно опрятно. Полки достаточно прочные, чтобы выдержать установленное на них оборудование, и при этом могут выдвигаться вперед. Машины можно выдвинуть, чтобы провести с ними те или иные работы, а у кабелей достаточный допуск, чтобы позволить это сделать. Если оборудование крепится к стойке, полки убираются, или же установка производится в стойки без полок. Теперь вы замечаете, что некоторые стойки (те, что находятся в дальнем конце зала) стоят без полок и ждут, пока в них установят оборудование.

Все стойки – 19-дюймовые и двухрамные. В стойках для сетевых коммутационных панелей, которые не требуют охлаждения, предусмотрены дверцы вместо передней панели. Эти стойки полностью открыты сзади. Все стойки в каждом ряду скреплены друг с другом для повышения устойчивости.

Ширина каждой стойки должна равняться ширине напольной плитки: 2 фута (≈60 см), или по стойке на плитку. Глубина стойки составляет 3 фута (≈90 см), или 1,5 размера напольной плитки. Ряд стоек в ширину занимает 1,5 размера плитки, а проход – столько же. Таким образом, на каждые три плитки приходится стойка и проход, то есть одна плитка полностью свободна и может быть поднята, если в этом возникнет необходимость. Было бы прекрасно, если между некоторыми или всеми рядами имелась бы дополнительная плитка. При наличии дополнительного пространства в полметра громоздкое оборудование гораздо проще устанавливать в стойки (рис. 6.19).

В каждом ряду не более 12 стоек. Между рядами достаточно просторный проход, через который можно пронести самое крупное оборудование. Некоторые ряды пустые, или в них отсутствует одна-две стойки рядом с общим проходом. Это пространство зарезервировано для машин, которые поставляются с собственными стойками, или для напольных серверов.

Если помещение большое, в нем несколько общих проходов. Если помещение небольшое, один проход идет от входной двери через центр зала. В задней части помещения предусмотрена вторая дверь, которая используется реже (запасной выход на случай пожара). От главного входа отлично просматривается весь машинный зал, что полезно при служебных обходах. В центре есть большое окно с небьющимся пластмассовым стеклом. Рядом с окном стоит стол с тремя мониторами, на которых отображается состояние локальной сети, глобальной вычислительной сети и служб.

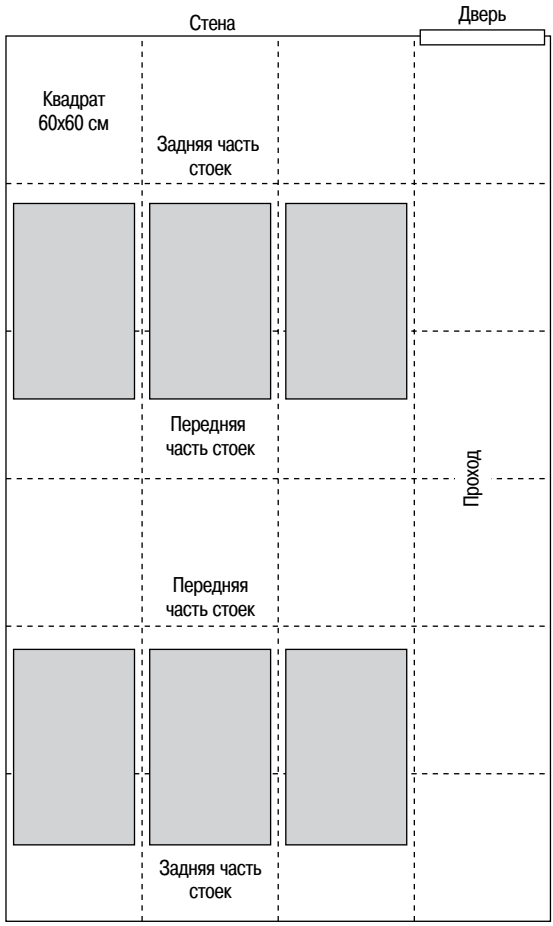

Рис. 6.19. *Простой план помещения, обеспечивающий открытое пространство*

Позади каждой стойки проходит сетевой кабель категории 6 с 24 штекерами. Первые 12 штекеров подключены к патч-панели рядом с сетевым оборудованием. Остальные 12 штекеров подключены к другой патч-панели рядом с консолидатором консолей. Хотя консолям не требуется кабель категории 6, однако постоянное использование одного типа кабеля означает, что сетевые подключения можно будет перенаправить в пространство консолей. Если есть вероятность, что рано или поздно потребуется оптоволокно, то в каждой стойке (или хотя бы через одну) будет по шесть пар оптоволокна, подключенных к оптоволоконной патч-панели. По мере роста популярности сетей хранения данных (Storage-Area Network, SAN) оптоволокно снова набирает популярность.

В последнем ряду стоек установлено исключительно сетевое оборудование. К патч-панелям подключено столько кабелей, что их нельзя перемещать, поэтому этот ряд находится в самом дальнем углу. Кроме того, в этой части помещения установлен стол с тремя мониторами и клавиатурами. Две пары из них

предназначены для переключателя KBM, а третий напрямую подключен к концентратору последовательной консоли. Одна стойка выделена для подключений, выходящих за пределы помещения. Рядом с ней находится ряд адаптеров волокно–кабели. Сегодня поставщики предоставляют единый блок, обеспечивающий питание нескольким таким адаптерам, которые в этот блок вставляются. Это позволяет избавиться от запутанных кабелей питания и пирамид из блоков питания.

У стойки с сетевым оборудованием установлена пара розеток в обход ИБП. От остальных розеток они отличаются цветом и соответствующей маркировкой. Бывают ситуации, когда ИБП не работает, а сеть должна функционировать. В таких случаях избыточные блоки питания подключаются к этим дополнительным розеткам.

Система кондиционирования проходит под полом. У каждой второй напольной плитки в проходах предусмотрена мелкая перфорация, чтобы пропускать воздух. В плитках под каждой стойкой сделаны более крупные отверстия, чтобы поток воздуха обдувал заднюю часть каждого устройства в стойке. Система подает воздух под достаточным давлением, чтобы должным образом охладить каждую стойку. Холодный воздух поднимается вдоль лицевой панели стойки, а кулеры каждой машины передают воздух к задней стороне стойки. Ориентация каждого ряда стоек попеременная, то есть, если вы идете по проходу между рядами, вы видите только лицевые панели стоек или только задние. Проход, к которому все стойки стоят лицевой стороной, называется «холодным рядом». Сюда поступает холодный воздух из напольных отверстий. Проход, к которому все стойки стоят задней стороной, называется «горячим рядом». Сюда поступает горячий воздух с задних панелей машин, который впоследствии выводится из помещения через вентиляционные отверстия на потолке.

По левую и правую сторону от каждой стойки с задней стороны установлен блок распределения питания, розетки на котором находятся на достаточном расстоянии друг от друга. Каждая пара стоек подключена к отдельной цепи из ИБП. Каждая цепь отмечена собственным номером, чтобы избыточные службы можно было поместить в другие цепи.

На каждом кабеле с обоих концов наклеены ярлыки с уникальным номером. На каждом узле сети есть ярлык с именем, IP- и MAC-адресом узла. В каждом зале находятся два принтера для ярлыков, и на каждом из них есть ярлык с номером зала и предупреждением, что кража данного устройства карается смертной казнью.

Под полом также проходят кабельные короба: отдельно для кабелей питания и для сетевых кабелей. Так как кабели питания и сетевые кабели уложены заранее, вряд ли когда-либо появится необходимость вскрывать пол.

Рядом с машинным залом (через второй выход) находится рабочая комната. Она отделена от основного зала, чтобы в нем не было лишней пыли. В этой комнате находятся широкие монтажные полки, на которых располагаются новые машины перед их установкой. Здесь же установлены рабочие столы с розетками и антистатическим покрытием, на которых производится ремонт оборудования, чтобы свести к минимуму возможное дальнейшее повреждение аппаратуры. В этой же комнате размещены ящики с инструментами и запасными частями, а также контейнеры с кабелями различных типов и длины. Запас инструмента включает 20 дополнительных пар кусачек, 40 дополнительных крестовых от-

верток и 30 дополнительных плоских отверток (учитывая скорость, с которой этот инструмент пропадает, такого запаса должно хватить на год).

На этом заканчивается экскурсия по идеальному информационному центру Тома. На выходе экскурсовод предложит вам в подарок коробочный дистрибутив Linux.

Игра с присосками

Мы расскажем вам об увлекательной игре, в которую вы сможете сыграть на открытом участке зала с фальшполом, например рядом со столом службы технической поддержки. Играть в эту игру рекомендуется в отсутствие начальства. Для игры нужны два участника и присоски для плитки.

Участники садятся или становятся в разных концах зала. Первый игрок бросает присоску на пол. Если она присасывается, игрок вытаскивает эту плитку и кладет ее в стопку в своей стороне зала. Участники делают ходы по очереди, пока на полу не останется ни одной плитки. Вы должны перемещаться по каркасу, не касаясь пола под фальшполом. Если вы дотронетесь до пола, то должны вернуть одну из плиток на место. Когда все плитки заканчиваются, выигрывает игрок, у которого собрано больше плиток.

Если играть в эту игру достаточно часто, через год края плиток будут сколоты и вам придется перестелить пол. Мы не советуем вам играть в эту игру, но если вы занимаетесь установкой и ремонтом напольных покрытий, то можете обучить этой игре своих клиентов, чтобы увеличить свой доход (мы вам этого не говорили!).

6.3.2. Идеальный вычислительный центр Кристины

В идеальном вычислительном центре Кристины установлены двойные двери, которые открываются с помощью автоматической системы безопасности, например бесконтактных пропусков или активации по голосу. Это облегчит доступ в центр людям, переносящим оборудование. Дверной проем достаточно широк, чтобы через него прошло даже самое крупное устройство. Двери находятся на том же уровне, что и разгрузочная площадка, и их разделяют широкие коридоры.

Вычислительный центр оснащен резервным генератором, мощность которого позволяет обеспечить питанием машины, освещение, системы отопления, вентиляции и кондиционирования, зарядку ИБП, АТС, рабочую область системных администраторов и центр технической поддержки. Система защиты доступа также подключена к защищенной системе энергоснабжения. Для генератора предусмотрены крупные баки, которые можно пополнять во время работы генератора. Проверка генератора осуществляется раз в неделю.

АВР можно настроить на приемлемое напряжение[1]. ИБП защищает вычислительный центр, и его мощности хватит на получасовую работу, чего должно

[1] Однажды Кристина видела АВР, который считал энергоснабжение приемлемым, в отличие от ИБП, поэтому, когда аккумуляторы ИБП сели, генератор не включился. Какой кошмар.

быть достаточно для ручного переключения на резервный генератор (при условии, что резервный генератор уже установлен).

В вычислительном центре нет фальшпола. Воздух подается сверху. В помещении высокие потолки без плиток. Стены выкрашены в матовой черный цвет на высоте примерно в полметра над стойками. Источники света направлены сверху вниз и установлены на уровне, на котором начинается черная краска. Благодаря этому потолочные системы отопления, вентиляции и кондиционирования менее заметны.

Подвесная шина питания поддерживает два источника питания. Отдельный ИБП, АВР, генератор, распределительные щиты и шина питания для каждого источника при разном физическом расположении каждого набора оборудования. Однако такой подход не был бы оправдан для вычислительного центра среднего уровня.

На верхней части каждой стойки предварительно установлена патч-панель на 36 портов, размером 2U, подключенная к стойкам в сетевом ряду. В сетевом ряду стойки с патч-панелями стоят между стойками с сетевым оборудованием. Все кабели аккуратно уложены.

В вычислительном центре установлены двухрамные (черные) стойки высотой 2 м, шириной 0,5 м и глубиной 1 м. На стойках нет ни задних, ни лицевых, ни боковых панелей. В стойках предусмотрены резьбовые отверстия, и полки закрепляются за боковины на вертикальные рельсы, которые могут свободно перемещаться. Глубина полок меньше глубины стоек и составляет всего 75 см, чтобы оставалось место для кабелей, подключаемых к машинам, а также блоков распределения питания и вертикальной укладки кабелей внутри стоек. Дополнительные вертикальные рельсы могут перемещаться для установки оборудования различной глубины. С одной стороны стоек установлены вертикальные блоки распределения питания с множеством розеток. Если в машинном зале используется несколько источников питания, к стойкам подведены все источники. В центре предусмотрен большой запас кабелей питания длиной 30 и 60 см, поэтому кабели питания не свисают со стоек. С другой стороны стоек проходит вертикальная укладка кабелей. Горизонтальная укладка используется по необходимости. В центре есть несколько небольших стремянок, которые позволяют даже не самым высоким системным администраторам достать до верхней части стоек.

В вычислительном центре есть запас сетевых соединительных кабелей длиной от 1 до 30 м с шагом 30 см, а также длиной 4,5; 6; 9; 10; 12; 13,5 и 15 м. На всех сетевых кабелях с обоих концов заранее наклеены ярлыки с уникальным серийным номером, в котором закодирована длина и тип кабеля. Везде, где это необходимо, установлены контейнеры со всеми видами кабелей и коннекторов.

На всех машинах с лицевой и задней стороны наклеены ярлыки с DNS-именем машины. На сетевых интерфейсах наклеены ярлыки с именем или номером сети.

В центре предусмотрена пара тележек с выдвижными ящиками для хранения самого разного инструмента. Здесь есть и простые отвертки, и аккумуляторные шуруповерты. В каждой тележке есть приспособление для создания ярлыков. Рядом с машинным залом расположена рабочая комната, в которой установлен прекрасный широкий стол с множеством розеток и антистатическим покрытием. Здесь также хранятся все необходимые инструменты.

6.4. Заключение

Чтобы вычислительный центр работал правильно, необходимо при его планировании учитывать множество факторов. Но, что бы вы ни планировали, будущий вычислительный центр будет работать долгое время, поэтому лучше с самого начала все сделать правильно. Вычислительный центр, который был плохо спроектирован, которому не хватает энергоснабжения или охлаждения, может стать источником множества проблем. Грамотно спроектированный вычислительный центр избавит вас от постоянной головной боли.

Системы энергоснабжения, кондиционирования и пожаротушения являются практически обязательными ключевыми компонентами вычислительного центра. Их отказ может значительно повлиять на его работу. С беспорядочными проводами и кабелями сталкивался каждый из нас, и никто не хочет повторения такого опыта. Если все грамотно распланировать заранее, вы можете избавить себя от кошмаров в этой области.

Еще один ключевой аспект, который необходимо продумать заранее, – доступ в центр для доставки и перемещения оборудования. А где доступ – там и система безопасности. Вычислительный центр – критически важное помещение, в котором находится множество ценного оборудования. Это должно быть отражено в политике получения доступа к центру, но при этом выбранная система должна быть удобной для людей, которым постоянно приходится работать с оборудованием.

Создание хорошего, надежного вычислительного центра требует немало вложений, но все они быстро окупаются. При этом можно внедрить простые, недорогие решения, которые позволят создать более приятную атмосферу в вычислительном центре, а также повысить эффективность его работы. Любой сотрудник оценит наличие удобного рабочего места, где можно производить ремонт оборудования и все необходимые инструменты, запасные части и материалы находятся под рукой. А ведь стоимость всего этого относительно мала. Ярлыки на всем оборудовании и строго отведенные места для передвижных устройств не требуют больших материальных затрат, но дают массу преимуществ, позволяя сэкономить время. Прислушайтесь к советам системных администраторов. У каждого из них есть свое мнение по поводу того или иного вопроса. Внедрите решения, которые они считают положительными, и усвойте уроки из их негативного опыта.

Если площадь позволяет, лучше сделать вычислительный центр просторнее, чем это необходимо. А если позволяют финансы и существуют очень жесткие требования к надежности, можно многого добиться с помощью избыточных систем энергоснабжения и кондиционирования, которые повысят надежность работы центра.

Чтобы использовать все возможности вычислительного центра, необходимо все правильно спроектировать с самого начала. Если вы знаете, что предстоит создание нового вычислительного центра, стоит все подготовить заранее и сделать грамотно.

Задания

1. Какие стихийные бедствия могут произойти в вашем регионе? Какие меры предосторожности вы приняли на случай стихийных бедствий и каким образом вы можете их улучшить?

2. С какими проблемами вы столкнулись при работе со своими стойками? Что бы вы хотели изменить?
3. Была бы для вас полезна предварительная укладка кабелей в вашем вычислительном центре? Если нет, что нужно было бы сделать, чтобы она была полезна? Как вы думаете, насколько предварительная укладка кабелей могла бы помочь устранить беспорядок с кабелями в вашем вычислительном центре?
4. Какова потребляемая мощность системы энергоснабжения в вашем вычислительном центре? Насколько вы близки к тому, чтобы уровень энергопотребления достиг максимального?
5. Если в вашем вычислительном центре используются отдельные цепи питания от разных ИБП, насколько хорошо они сбалансированы? Что можно сделать, чтобы улучшить этот баланс?
6. Какую площадь занимают мониторы в вашем вычислительном центре? От скольких из них можно избавиться, перейдя на последовательные консольные серверы? От скольких из них можно избавиться, внедрив переключатели KBM?
7. Где вы производите ремонт сломанного оборудования? Есть ли какой-нибудь участок, который можно переоборудовать в рабочую область?
8. Какие инструменты должны быть в тележке в вашем вычислительном центре?
9. Как вы думаете, какие материалы должны быть в вычислительном центре и сколько их должно быть по каждому наименованию? Какими должны быть высокий и низкий уровни запасов по каждому наименованию?
10. Какие запасные части вам нужны и сколько их должно быть по каждому наименованию?
11. Какое оборудование или инструменты постоянно «куда-то деваются»? Можно ли отвести подходящее место для их хранения?

Глава 7

Сети

Сеть компании – основа ее инфраструктуры. Плохо созданная сеть влияет на любое восприятие всех остальных компонентов системы. Сеть нельзя считать изолированным элементом. Решения, принимаемые при проектировании сети и в процессе ее внедрения, влияют на то, как инфраструктурные сервисы будут внедрены. Таким образом, с теми, кто несет ответственность за проектирование этих сервисов, обязательно стоит консультироваться в процессе проектирования сети.

В этой короткой главе мы не сможем подробно рассказать о проектировании сетей и их внедрении. Этой теме посвящено немало книг. Однако мы сможем выделить аспекты, которые нам кажутся наиболее важными. Начать изучение этой темы рекомендуем с книги Perlman 1999. По протоколу TCP/IP (Transmission Control Protocol/Internet Protocol) рекомендуем работы Stevens 1994[1] и Comer 2000[2]. Чтобы понять принцип работы маршрутизаторов и коммутаторов, прочтите книгу Berkowitz 1999. Этот автор также написал книгу по сетевым архитектурам (Berkowitz 1998). Более подробную информацию по конкретным технологиям вы найдете в книге Black 1999. По глобальным вычислительным сетям просмотрите книги Marcus 1999 и Feit 1999. По протоколам маршрутизации прочтите книгу Black 2000. Многие книги посвящены отдельным протоколам или технологиям: OSPF (Open Shortest Path First) – Moy 2000 и Thomas 1998[3]; EIGRP (Enhanced Interior Gateway Routing Protocol) – Pepelnjak 2000; BGP (Border Gateway Protocol) – Stewart 1999 и Halabi and McPherson 2000; MPLS (Mail Protocol Label Switching), VPN и QoS – Black 2001, Guichard and Pepelnjak 2000, Lee 1999, Vegesna 2001[4], Keagy 2000, Maggiora et al. 2000; групповая передача – Williamson 2000; ATM (Asynchronous Transfer Mode) – Pildush 2000[5]; Ethernet – Spurgeon 2000.

Организация сетей – область стремительного развития технологий, поэтому методы и возможности внедрения с годами серьезно меняются. В этой главе мы

---

[1] У. Ричард Стивенс «Протоколы TCP/IP. Практическое руководство». – Пер. с англ. – СПб.: BHV-Санкт-Петербург, 2003.

[2] Дуглас Э. Камер «Сети TCP/IP. Том 1. Принципы, протоколы и структура». – Пер. с англ. – Вильямс, 2003.

[3] Томас Т. М. II «Структура и реализация сетей на основе протокола OSPF». – Пер. с англ. – Вильямс, 2004.

[4] Шринивас Вегешна «Качество обслуживания в сетях IP». – Пер. с англ. – Вильямс, 2003.

[5] Галина Дикер Пилдуш «Сети ATM корпорации Cisco». – Пер. с англ. – Вильямс, 2004.

выделим области, которые со временем претерпевают изменения, а также некоторые константы в мире сетей.

Эта глава в основном посвящена внутренним локальными сетям и глобальным вычислительным сетям организации, занимающейся электронной коммерцией. Однако мы также рассмотрим вопросы, касающиеся помещения.

7.1. Основы

При создании сети ваша основная цель – предоставить надежную, хорошо документированную, простую в обслуживании сеть, которая отличается значительной пропускной способностью и потенциалом роста. На словах все просто, не правда ли?

От очень многих факторов зависит, достигнете ли вы этой цели. Данный раздел посвящен основам: вопросам физических сетей, топологии логических сетей, документированию, маршрутизации узлов сети, протоколам маршрутизации, мониторингу и управлению административными единицами. В этом разделе также описывается взаимодействие компонентов проектирования сети друг с другом и с проектированием сервисов для этой сети.

Подходы к проектированию глобальных вычислительных и локальных сетей значительно различаются. Со временем циклически меняющиеся тенденции делают их более похожими, затем менее похожими, затем вновь более сходными. К примеру, было время, когда популярной топологией локальных сетей было двойное кольцо подключений по стандарту FDDI (Fiber Distributed Data Interface – распределенный волоконный интерфейс данных), дававшее устойчивость к сбоям. Эта топология теряла популярность по мере распространения 100-мегабитного Fast Ethernet, построенного по топологии шинной архитектуры. Тем временем в глобальных вычислительных сетях стали применять кольцевые архитектуры, такие как SONET (Synchronous Optical Network – синхронная оптоволоконная сеть) и MONET (Multiwavelength Optical Network – оптоволоконная сеть с разделением по длине волны). В начале 2007 года черновой вариант 10-гигабитных локальных сетей вернулся к кольцевой архитектуре. Круг замкнулся.

7.1.1. Модель OSI

Модель OSI (Open Systems Interconnection – эталонная модель взаимодействия открытых систем) для сетей получила широкое распространение и будет неоднократно упоминаться в этой главе. В этой модели сеть рассматривается как логические уровни, кратко описанные в табл. 7.1.

Сетевые устройства определяют путь, который проходят данные по физической сети, состоящей из кабелей, беспроводных каналов и сетевых устройств (*уровень 1*). Сетевое устройство, принимающее решение, основываясь на аппаратном, или MAC-, адресе узла-отправителя либо получателя, относится к *устройствам уровня 2*. Устройство, принимающее решение, основываясь на IP-адресе (или AppleTalk, или DECnet) узла-отправителя либо получателя, известно как *устройство уровня 3*. Устройство, использующее транспортную информацию, такую как номера портов TCP, – это *устройство уровня 4*.

Техники, хорошо знакомые с сетями TCP/IP, часто упрощают эту схему следующим образом: физический кабель – уровень 1; устройства, работающие с от-

Таблица 7.1. Модель OSI

Уровень	Название	Описание
1	Физический уровень	Физическое подключение между устройствами: медные кабели, оптоволокно, радио-/лазерный канал
2	Канальный уровень	Интерфейсная или MAC-адресация, управление потоками данных, оповещения о низкоуровневых ошибках
3	Сетевой уровень	Логическая адресация (например, IP-адреса) и маршрутизация (например, RIP, OSPF, IGRP)
4	Транспортный уровень	Доставка данных, проверка на наличие ошибок и восстановление, виртуальные цепи (например, сеансы TCP)
5	Сеансовый уровень	Управление сеансами связи (например, привязка имен AppleTalk или PPTP)
6	Уровень представления	Форматы данных (например, ASCII, Unicode, HTML, MP3, MPEG), кодировка символов, сжатие, шифрование
7	Прикладной уровень	Протоколы приложений, например SMTP (электронная почта), HTTP (Веб) и FTP (передача файлов)

дельной локальной сетью, – уровень 2; маршрутизаторы и шлюзы, распределяющие пакеты между локальными сетями, – уровень 3; используемый протокол – уровень 4.

Уровень 5 плохо вписывается в мир TCP/IP. Уровень 6 – это формат данных: ASCII, HTML, MP3 или MPEG. Также обычно сюда относят шифрование и сжатие данных.

Уровень 7 – это, собственно, протокол приложения: HTTP (HyperText Transfer Protocol – протокол передачи гипертекста) для Веб; SMTP для отправки электронной почты; IMAP4 для доступа к почтовым ящикам, FTP (File Transfer Protocol – протокол передачи файлов) для передачи файлов и т. д.

Модель OSI – полезное руководство для понимания того, как должны работать сети, но в реальном мире границы уровней часто нарушаются. Например, VPN-подключение, осуществляемое через HTTP-прокси, посылает трафик уровней 3 и 4 по протоколу 7-го, прикладного уровня.

Уровни 8, 9 и 10

В шутку к модели OSI добавляют еще три уровня:

- Уровень 8 – пользовательский.
- Уровень 9 – финансовый.
- Уровень 10 – политический.

Многие архитектуры корпоративных сетей направлены на решение проблем уровня 10, но не могут добиться поставленной цели, так как ограничены уровнем 9.

7.1.2. Понятная архитектура

Сетевая архитектура должна быть максимально понятной и простой для восприятия. Должна существовать возможность кратко описать подход, применявшийся при проектировании сети, и проиллюстрировать проект несколькими простыми рисунками. Понятная архитектура значительно упрощает решение проблем с сетью. Вы можете сразу сказать, по какому пути идет трафик из точки А в точку Б. Вы можете сказать, какие каналы на какие сети влияют. Если у вас есть ясное представление о маршруте прохождения трафика в вашей сети, то вы можете ею управлять. Непонимание устройства сети оставляет вас на милость случайностей.

Понятная архитектура охватывает как физическую, так и логическую топологию сети, а также сетевые протоколы, используемые узлами и сетевым оборудованием. Понятная архитектура также просто определит стратегию роста в отношении как добавочных сегментов локальной сети, так и подключения новых удаленных офисов. Понятная сетевая архитектура – центральный компонент всего, что будет описано далее в этой главе.

Пример: сложность и поддержка поставщика

Сетевая архитектура, которую невозможно описать простыми словами, затрудняет получение поддержки от поставщика, когда у вас возникает проблема. Администратор одной сети испытал эти сложности на своем опыте. Когда случился отказ чрезмерно сложной сети, все, к кому он обращался как в своей организации, так и у поставщика, очень долго не могли разобраться в конфигурации, не говоря уже о том, чтобы что-то посоветовать для решения проблемы. Звонить в службу поддержки поставщика было бесполезно, потому что сотрудники, работающие с клиентами, не могли разобраться в сети, которую нужно было исправлять. Некоторые сотрудники поставщика даже не верили, что кто-то мог использовать настолько сложную схему! После того как администратор добрался до старших сотрудников службы поддержки, ему сказали, что в такой причудливой конфигурации невозможно поддерживать работу их продукции, и доказали, что нужно упростить систему, а не требовать невозможного от продукции поставщика.

Пример: сложность и поддержка администраторами сети

При поиске неисправностей в сложной сети сетевой администратор одной компании обнаружила, что у нее уходит больше времени на то, чтобы разобраться в существующих сетевых маршрутах, чем собственно на решение проблем. Как только архитектуру сети упростили, на устранение неисправностей стало требоваться меньше времени.

Мы советуем ограничивать количество сетевых протоколов в каждой отдельной глобальной вычислительной сети. Большинство компаний в последние годы так

и делают, переводя все сети передачи данных на TCP/IP, вместо того чтобы пытаться объединить этот протокол с Novell IPX, AppleTalk и другими протоколами. Если необходимо, для этих протоколов можно создать туннели поверх TCP/IP с помощью разных вложенных протоколов. К тому же такой подход обходится дешевле, чем организация отдельной глобальной вычислительной сети для каждого протокола.

7.1.3. Топологии сетей

Топологии сетей сменяют друг друга вместе с технологиями и структурой расходов по мере того, как компании развиваются, открывают крупные удаленные офисы или поглощают другие компании. Здесь мы расскажем о некоторых распространенных топологиях.

В глобальных, университетских и локальных сетях часто встречается топология «*звезда*», в которой одна компания, здание или часть сетевого оборудования находится в центре звезды, а остальные компании, здания или сети подключаются к центру. Например, в отдельном здании университета может находиться устройство уровня 2 или 3, к которому подключаются все узлы сети. Это устройство – центр звезды. Локальная сеть с топологией звезды изображена на рис. 7.1. Для глобальной вычислительной сети, в которой удаленные подключения сходятся к одному зданию, центром звезды будет это здание, как показано на рис. 7.2. Для топологии звезды свойственно одно уязвимое место: при отказе центра нарушается связь между лучами звезды. Иначе говоря, если все узлы в здании подключены к одному коммутатору, то при его отказе отключатся они все. Если все сети, входящие в глобальную сеть, подключены к одному зданию, в котором отключили электричество, они потеряют связь друг с другом, но внутри каждой удаленной сети связь будет работать. Однако топология звезды понятна, проста, а ее внедрение часто экономически эффективно. Эта архитектура может быть удобна в использовании, особенно для относительно малых организаций. Эту топологию можно легко улучшить, обеспечив избыточные подключения между конечными точками или продублировав центральный узел.

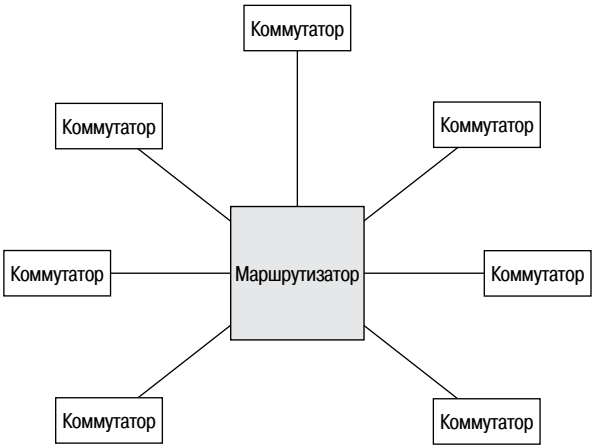

Рис. 7.1. *Локальная или университетская сеть с топологией звезды*

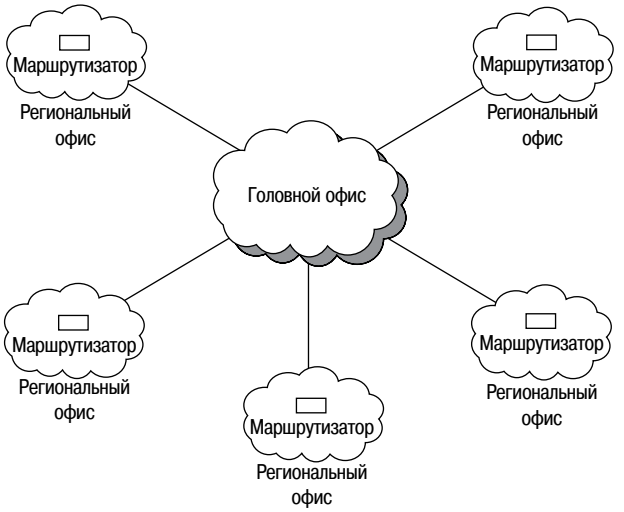

Рис. 7.2. *Глобальная вычислительная сеть с топологией звезды*

Распространен вариант топологии звезды, состоящий из нескольких звезд, центры которых связаны друг с другом избыточными высокоскоростными каналами (рис. 7.3). Такой подход ограничивает негативные последствия отказа центра одной из звезд. Компании с географически удаленными отделениями часто используют такой подход для сосредоточения всего удаленного трафика от одного географического региона в одном или двух дорогостоящих дистанционных каналах. Такие компании также обычно предоставляют большое количество сервисов прикладного уровня в центре каждой звезды, чтобы снизить трафик по дальней связи и зависимость от удаленных подключений.

Топология «*кольцо*» тоже широко распространена и чаще всего применяется для отдельных низкоуровневых топологий, таких как кольца SONET. Кольцевая топология также встречается в локальных и университетских сетях, а иногда бывает полезна и в глобальных вычислительных сетях. В кольцевой топологии каждый элемент сети – будь то сетевое оборудование, здание или корпоративная сеть – подключен к двум другим так, что схема подключений в сети образует кольцо, как показано на рис. 7.4. Выход из строя любого канала в сети не влияет на состояние связи между функционирующими составляющими кольца. Однако при увеличении числа элементов кольца, особенно в глобальных сетях, может потребоваться разделить конфигурацию подключений на несколько сетей.

Другая архитектура, используемая компаниями, которые заботятся об избыточности и надежности, выглядит как топология из нескольких звезд, но каждый краевой узел[1] связан резервным подключением с центром другой звезды,

[1] Краевой узел – это элемент сети, который работает только с трафиком, приходящим от локальных машин или предназначенным для них, и не используется для передачи другого трафика. В простой топологии звезды все узлы, кроме центрального, – краевые.

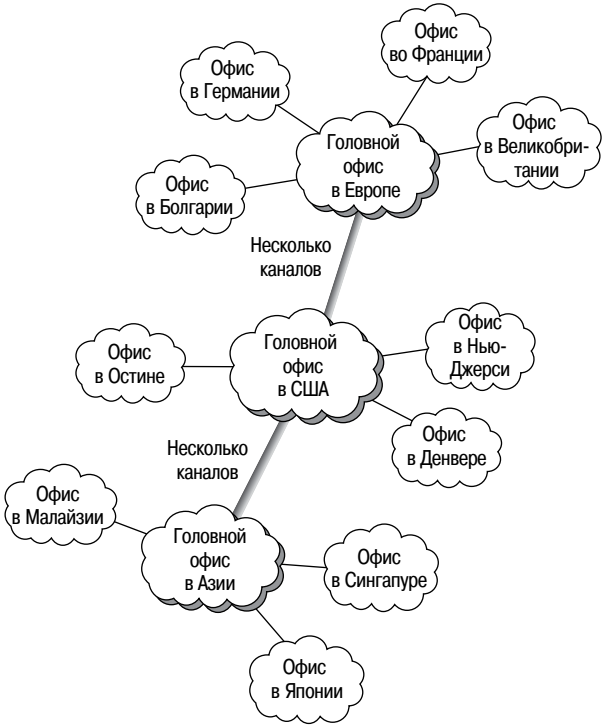

Рис. 7.3. *Топология глобальной вычислительной сети из нескольких звезд на основе географических узлов*

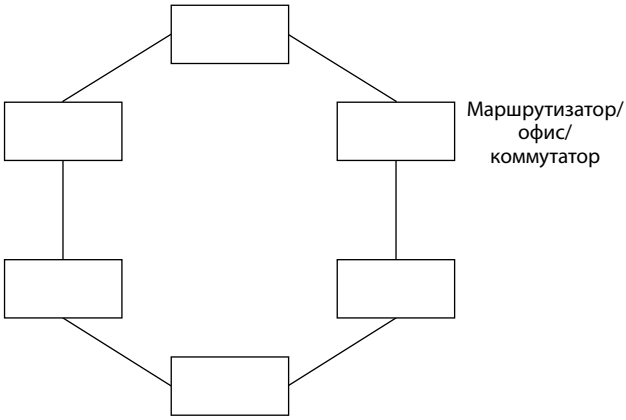

Рис. 7.4. *Кольцевая топология, в которой каждое сетевое устройство связано с двумя другими*

как показано на рис. 7.5. Если откажет центральный узел какой-либо звезды, ее краевые узлы переходят на резервное подключение, пока основное не будет восстановлено. Такая гибридная модель позволяет организации добиться компромисса между расходами и надежностью для каждой сети.

Существует множество вариантов сетевых топологий, в том числе топология хаоса, которой по большей части описывается топология Интернета. Топология хаоса возникает в случае, если каждый узел в качестве маршрута для доступа к остальной части сети может использовать один или несколько произвольных узлов. Но не стоит ожидать, что кто-то сможет точно описать или изобразить схему подключений хаотичной сети без помощи сложных специализированных программ. При попытке создания карты Интернета были сгенерированы интересные и полезные картины.

Архитектуру, которую невозможно изобразить или описать без дополнительной помощи, нельзя назвать понятной. Тем не менее Интернет продолжает существование, потому что он высокоадаптивен и отказоустойчив. При отказе одного из элементов все остальные продолжают работать. В действительности по всему Интернету постоянно возникают простои, но, так как они незначительны и затрагивают только отдельные участки сети (как правило, принимающие

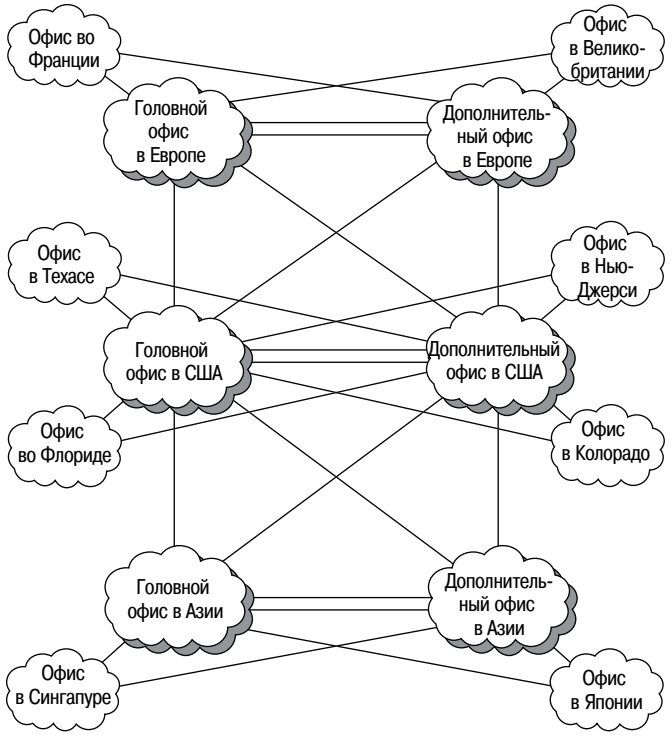

Рис. 7.5. *Избыточная топология глобальной вычислительной сети из нескольких звезд. Ядро сети для надежности образует кольцо. Меньшие сети подключены по топологии звезды для простоты и сокращения расходов*

данные), они проходят незамеченными для большой сети. Это не относится к корпоративным или университетским сетям, где каждая часть, как правило, сильно зависит от других частей. Хаотический подход – ненадежная модель для сетей, в которых имеет значение готовность каждого компонента.

То, что обычно изображается как схема сети, – это **логическая топология сети**. Она обычно показывает только сетевые устройства, такие как маршрутизаторы, работающие на уровне 3 и выше, и представляет как единый элемент каждую подсеть, работающую с одним и более устройствами уровня 2, такими как коммутаторы. Логические топологии сетей, наиболее соответствующие потребностям каждой конкретной сети, могут сильно различаться в зависимости от используемых технологий и структуры расходов. Для отдельной сети могут быть построены различные логические схемы в зависимости от того, на какие конкретно особенности нужно обратить внимание аудитории.

Простое практическое правило ограничения сложности сети заключается в том, что архитектор корпоративной сети и старшие сетевые администраторы должны быть способны без посторонней помощи схематично изобразить ключевые функции и основную структуру топологии сети. Если нужны дополнительные источники информации, то архитектуру нельзя назвать ясной и понятной.

Логическая топология сети не может разрабатываться изолированно. Она подвержена влиянию других аспектов вычислительной инфраструктуры и сама влияет на них. В частности, логический проект сети, его физическое воплощение и топология маршрутизации, которая будет задействована в сети, взаимозависимы. Помимо этого, архитектура сетевых сервисов, таких как электронная почта, доступ в Интернет, печать и сервисы каталогов, должна влиять на архитектуру сети и зависеть от нее.

Пример: несовместимая сетевая архитектура

Крупной международной компании-производителю компьютеров понадобилось перепроектировать свою глобальную вычислительную сеть, чтобы привести ее в соответствие современным технологиям. Были обновлены как физический уровень подключений между участками сети, так и архитектура маршрутизации сети. Новый протокол маршрутизации был довольно быстро выбран на основе оценки ограничений и требований. Физическая архитектура (в частности, широкополосное подключение между ключевыми сегментами сети) была выбрана позже независимо от выбора протокола маршрутизации. Показатели, используемые протоколом маршрутизации для определения пути, не принимались в расчет[1]. В результате некоторые высокоскоростные каналы использовались неэффективно, а часть медленных подключений была подвержена задержкам и потере пакетов из-за перегрузки. Неверный расчет пропускной способности подключений – слишком дорогая ошибка.

Сеть должна рассматриваться как единое целое. Изменения, сделанные в одной области, влияют на другие области.

[1] Выбранный протокол не учитывал пропускную способность сети, только число ее сегментов.

Пример: проектирование сетевых сервисов

В крупной международной компании, выпускающей программное обеспечение, в тесном сотрудничестве работали отделы базовых сервисов, региональных филиалов и сетевой. Сетевой отдел принял решение подключать региональные филиалы к корпоративной опорной сети по узким, недорогим глобальным каналам. Позже должны были появиться избыточные подключения по ISDN (Integrated Services Digital Network – цифровая сеть с интеграцией служб), поэтому изначально использовалось оборудование, поддерживающее резервные подключения по ISDN. Исходя из этого решения и обсуждения с сетевым отделом, отделы базовых сервисов и региональных филиалов решили сделать филиалы максимально независимыми, чтобы они могли вести большую часть своих дел при отсутствии подключения к корпоративной опорной сети.

В каждом филиале, независимо от его размера, устанавливался сервер, обеспечивающий работу локальной электронной почты, аутентификации, сервиса имен, файлового сервиса и печати, а также маршрутизатор удаленного доступа, настроенный на переключение на локальный сервер аутентификации, если невозможно подключение к центральному корпоративному серверу аутентификации. Эта архитектура работала хорошо, так как сети филиалов были практически полнофункциональными, даже если у них не было связи с остальной компанией. Для небольшого количества задач, требующих подключения к другим сетям, при необходимости предоставлялся обычный корпоративный удаленный доступ.

Если бы у всех филиалов были высокоскоростные избыточные подключения к корпоративной опорной сети, можно было бы выбрать альтернативную архитектуру сервисов, больше полагающуюся на эти сетевые подключения, хотя такой вариант был бы значительно дороже.

Топологии звезды, нескольких звезд или кольцевая, описанные выше, могут существовать на физическом уровне, на логическом уровне или на том и другом. Другие топологии распространены на логическом уровне сети, в том числе однородная сетевая топология, топология на основе функциональных групп и топология на основе локаций.

Плоская топология – единая большая сеть, состоящая только из устройств уровня 2. В терминах TCP/IP, это одна коммутируемая зона, один большой домен широковещательной рассылки. Без маршрутизаторов. Под *доменом широковещательной рассылки* подразумевается, что широковещательный запрос, отправляемый в эту сеть одной машиной, принимают все машины сети. В плоской топологии существует только один блок сетевых адресов, в который входят все машины. Все сервисы, такие как файловый сервис, печать, электронная почта, аутентификация и сервис имен, предоставляются серверами этой сети.

В топологии на основе местоположения сети уровня 2 назначаются исходя из их физического местоположения. Например, компания может создать сети уровня 2 на каждом этаже здания, а для связи между этажами использовать устройства уровня 3. На каждом этаже будет установлен коммутатор уровня 2 с высокоскоростным подключением к устройству уровня 3 (маршрутизатору).

Все машины одного этажа должны входить в один блок сетевых адресов. Машины с разных этажей должны входить в разные блоки сетевых адресов и подключаться друг к другу по крайней мере через одно устройство уровня 3.

В топологии на основе функциональных групп каждый член функциональной группы подключен к одной и той же (плоской) сети, независимо от размещения, наиболее разумным способом. Например, в здании может быть четыре локальных сети: отдела продаж, технического отела, руководства и отдела маркетинга. Сетевые порты каждой группы должны быть коммутированы между распределительными щитами, возможно, даже по каналам, связывающим разные здания, пока не дойдут до места назначения, где расположен коммутатор уровня 2 для этой сети. Также групповые сети, как правило, включают в себя файловый сервис, сервис имен и сервис аутентификации, что подразумевает распространение сети и на информационный центр. Одно (или больше) устройство уровня 3 соединяет групповую сеть с основной корпоративной сетью, в которой также предоставляются сервисы для групповой сети, такие как электронная почта, доступ к интрасети и к Интернету. Некоторые из сервисов, предоставляемых в групповой сети, такие как сервис аутентификации и сервис имен, обмениваются информацией с главными серверами основной корпоративной сети.

7.1.4. Промежуточный кабельный узел

Промежуточный кабельный узел (Intermediate Distribution Frame, IDF) – это «умное» название для коммутационного шкафа. Распределительная система состоит из нескольких сетевых шкафов и кабелей, которые подключают настольные компьютеры к сети. Потребность в IDF и способ их проектирования и размещения меняются не слишком быстро. Со временем меняются только технологии и особенности кабельных подключений.

Инновации в сетевом оборудовании требуют высококачественных медных или оптоволоконных подключений, способных справляться с возросшими скоростями. Если вы используете новейшие кабели с наилучшими характеристиками при создании кабельной системы, можно ожидать, что они проработают по крайней мере 5 лет, прежде чем устареют по сравнению с сетевыми технологиями. Но если вы пытаетесь сэкономить, используя старые, дешевые кабели с худшими характеристиками, то вам придется пережить связанные с модернизацией расходы и перерывы в работе раньше, чем если бы вы выбрали более качественные кабели. Компании, пытавшиеся сэкономить, используя медный кабель категории 3, хотя можно было уже приобрести кабель категории 5, в результате потратили больше на замену кабельной системы, когда распространился Fast Ethernet.

Категории кабелей

Кабели категории 3 рассчитаны на 10-мегабитные Ethernet-подключения дальностью до 100 м. Кабели категории 5 рассчитаны на 100-мегабитные Fast Ethernet-подключения дальностью до 100 м. Кабели категории 6 рассчитаны на 1000-мегабитные Gigabit Ethernet-подключения дальностью до 90 м. Кабели категории 7 требуются для нового стандарта 10-гигабитных Ethernet-подключений. Все они обратно совместимы. Обычно их наименования сокращаются до Cat3, Cat5 и т. д.

Более современные IDF упрощают подключение кабеля от сетевого разъема к нужной сети. Достаточно просто подключить короткий патч-корд от гнезда RJ-45, представляющего этот разъем, к гнезду RJ-45 Ethernet-коммутатора в нужной сети.

В более старых IDF подобные подключения осуществлялись с помощью **коммутационного блока**. В отличие от модульных разъемов RJ-45, здесь провода каждого кабеля смонтированы (подключены) к концевым кабельным муфтам. С другой стороны к муфтам подключены провода, ведущие к сети назначения. Для каждого сетевого разъема может потребоваться от четырех до восьми контактов. Мы рекомендуем использовать в сетях патч-панели, а не коммутационные блоки.

Подключение между IDF можно организовать двумя способами. Первый способ – проложить связки кабелей через все здание. Однако при большом количестве IDF такое количество каналов обойдется дорого и будет сложным в обслуживании. Другой способ – создать централизованное место для коммутации и проложить связки кабелей от IDF только до этого центра. В таком случае для соединения двух любых IDF будет достаточно только создать кросс-подключение в центре. Такой центр называется **центральным кабельным узлом** (Main Distribution Frame, MDF), подробнее о нем будет рассказано ниже.

Как правило, у вас есть возможность спланировать размещение ваших IDF только до переезда в здание. Если потом вы решите, что сделали что-то неверно, то вносить изменения будет трудно и дорого. Бегать с этажа на этаж, чтобы решить сетевую проблему с чьим-то компьютером, слишком долго и утомительно. У вас должен быть по меньшей мере один IDF на этаж или больше, если этажи широкие. Размещать IDF в здании следует строго по одной вертикали, на одном и том же месте каждого этажа. При вертикальном размещении прокладывать кабели между IDF и MDF будет проще и дешевле, а впоследствии при необходимости будет легче добавить дополнительные кабели между IDF. Также при таком размещении сотрудникам службы поддержки понадобится изучить только одну схему этажа, что снизит нагрузку на службу поддержки. Аналогично, в нескольких одинаковых зданиях следует размещать IDF в одних и тех же местах. На рис. 7.6 изображена схема подключений между IDF и MDF.

Нумерация IDF должна включать номер здания, этажа и шкафа. Нумерация шкафов должна быть единообразной для всех этажей всех зданий. Сетевые разъемы, обслуживаемые IDF, должны быть помечены ярлыком с номерами IDF и розетки[1]. Если в одной розетке расположено несколько сетевых разъемов, то обычно после номера розетки используются буквы. Номера и литеры розеток должны соответствовать номерам и литерам розеток на разъемах в IDF. При отсутствии нумерации или непоследовательной нумерации решение проблем в сети настольных компьютеров становится очень сложным. Цветовая кодировка разных разъемов в одной розетке хорошо подходит для людей, не страдающих цветовой слепотой, но создает проблемы для дальтоников. Если вы хотите использовать цветовую кодировку разъемов, применяйте параллельно и буквенные

[1] Розетка – это конечная точка сети, где заканчиваются один или несколько кабелей. Как правило, отдельный офис или секция будет иметь один номер розетки, соответствующий одной точке в помещении, в которой находится один или несколько сетевых разъемов. Но в более крупных помещениях, таких как конференц-залы, может быть несколько конечных точек сети и, соответственно, несколько номеров розеток.

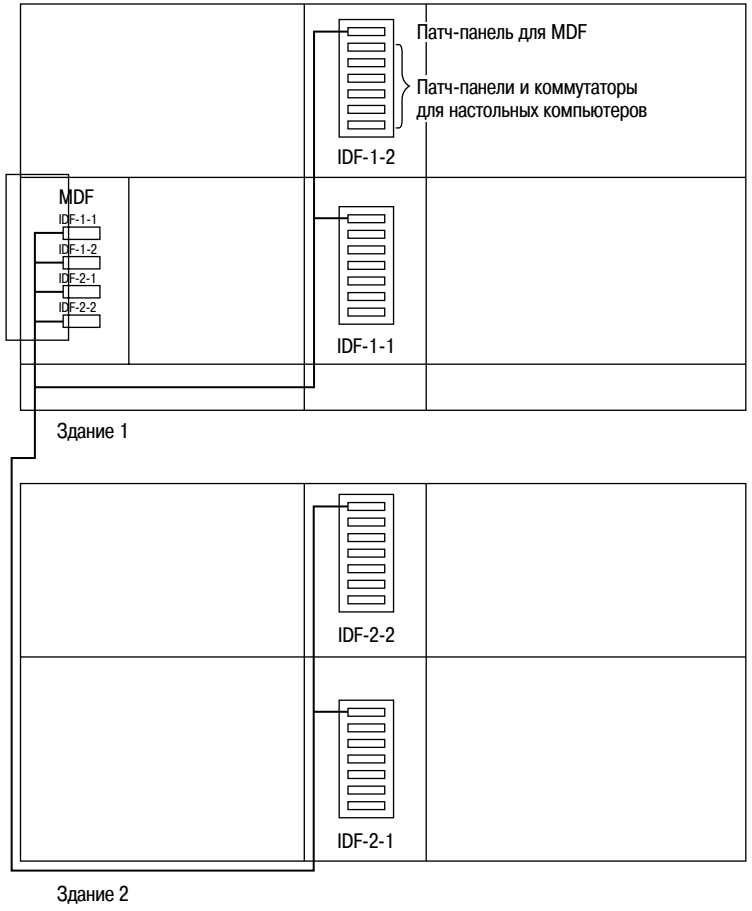

Рис. 7.6. *Патч-панели каждого IDF подключены к патч-панели MDF*

обозначения, чтобы избежать подобных проблем. В каждом шкафу должен быть надежно закреплен на стенке долговечный ламинированный план этажа для зоны обслуживания, на котором отображены номера розеток и сетевых разъемов. Вы удивитесь, насколько часто он будет нужен. Также хорошо будет повесить на видном месте доску для записей, чтобы записывать изменения. Например, в IDF, обслуживающем аудитории для подготовки корпоративных кадров и клиентов, доску для записей можно использовать для расписаний занятий, мероприятий, учета посещаемости и планов сетевых подключений.

На доске также должно быть выделено место для произвольного текста, чтобы вести записи о текущих проблемах.

IDF всегда должны быть закрыты, а доступ посторонних к ним – запрещен. Без должной подготовки и понимания того, что вы делаете, в коммутационном шкафу слишком легко все испортить. Если приходится вносить большое количество изменений, а штат сотрудников отличается высокой текучестью, рекомендуется проводить частые, но краткие инструктажи по работе с коммутаци-

онными шкафами. Если эти занятия проводятся в одно и то же время в одном и том же месте каждый месяц, то люди, имеющие доступ к коммутационным шкафам, но редко с ними работающие, смогут по необходимости посещать занятия, чтобы быть в курсе происходящего[1].

Еще одна причина закрывать IDF на замок – безопасность. IDF – слишком удобное место для размещения устройств слежения за сетью, так как туда редко заглядывают люди и там можно легко спрятать «жучок» среди другого оборудования. Кроме того, IDF – слишком легкая добыча для желающих нарушить работу сети.

Размер шкафов IDF должен быть больше, чем это необходимо для размещения вашего сетевого оборудования, но не настолько большим, чтобы в них устанавливали серверы и оборудование, не имеющее отношения к компьютерам. В шкафу для IDF должно размещаться только сетевое оборудование для его зоны обслуживания. Серверы, размещенные в не предназначенных для этого местах (коммутационных шкафах и т. д.), сильнее подвержены сбоям, вызванным случайными толчками или отключениями кабелей, а при возникновении проблем их сложнее найти.

Иногда к коммутационным шкафам имеют доступ больше людей, чем к серверной. Возможно, некоторые доверенные, подготовленные сотрудники из числа пользователей могут иметь доступ к шкафу, например, чтобы подключать порты в лаборатории, в которой часто сменяется оборудование. Особо крупные лаборатории могут конфигурироваться так же, как IDF, и даже отмечаться в сетевых диаграммах как единое целое. Это должно обеспечить достаточное количество сетевых подключений в лаборатории. В некоторых ситуациях менее крупные лаборатории могут конфигурироваться как подстанция IDF путем подключения IDF к сетевому коммутатору в лаборатории через высокоскоростной канал.

Коммутационные шкафы должны быть обеспечены защитой электропитания. Сетевое оборудование, так же как и компьютерное, должно быть защищено от всплесков напряжения и перебоев в электроснабжении. Если ваш информационный центр питается через ИБП, то также надо защитить и сетевое оборудование в коммутационных шкафах, которое является продолжением вычислительного центра. Вряд ли кому то понравится, если информационный центр и персональные компьютеры будут работать во время перебоев с энергоснабжением, а промежуточные сетевые устройства отключатся. Учитывая то, что ноутбуки оснащены батареями, а настольные компьютеры часто подключаются через небольшие персональные ИБП, сохранение работоспособности сети во время отключений электроэнергии становится все более важным (подробнее источники бесперебойного питания и вопросы электроснабжения рассматриваются в разделе 6.1.4).

Шкафы IDF должны иметь дополнительное охлаждение помимо того, что обеспечивает система кондиционирования здания. Сетевое оборудование компактно, поэтому на ограниченном пространстве плотно размещается большое количество нагревающихся устройств. Сетевые устройства обычно неприхотливы и надежны, но и для них существуют ограничения. В небольшом шкафу IDF будет слишком жарко без дополнительного охлаждения.

---

[1] В быстрорастущих компаниях мы рекомендуем проводить подобные встречи ежемесячно, чтобы новые сотрудники могли пройти обучение как можно скорее. В более стабильных компаниях можно проводить инструктаж не так часто.

Также вы должны обеспечить удаленный консольный доступ ко всем устройствам в IDF, которые поддерживают такую функциональность. Консольные порты всех устройств должны быть должным образом защищены. По возможности стоит использовать строгую аутентификацию или хотя бы пароли.

Более экономично устанавливать сетевые разъемы на этапе строительных работ, а не добавлять их потом по одному по мере надобности. Следовательно, имеет смысл установить на каждом столе на один или два разъема больше, чем, по вашему мнению, может когда-либо понадобиться вашим пользователям. При проводке кабелей в офисе не так дороги сами кабели, как высоки строительные расходы на прокладку их в стенах. Если разъемы можно установить на этапе строительства, это принесет заметную экономию.

Мертвые президенты

При смене проводки в здании строительные расходы обычно превосходят любые другие. Производственники говорят, что расходы на монтаж самые высокие, что бы вы ни «замуровывали в стены – медный кабель категории 5 или мертвых президентов» (жаргонное название долларов).

Вместо того чтобы пытаться учитывать, например, что в офисах инженеров должно быть больше сетевых разъемов, чем в офисах отдела маркетинга, лучше устанавливайте одно и то же количество разъемов на каждом столе и столько же на потолке. Распределение мест никогда не бывает постоянным. Со временем инженеры будут работать там, где предполагалось разместить отдел маркетинга, и вам понадобится приводить кабели в этих помещениях в соответствие стандартам остальных инженерных помещений.

Те же экономические соображения действительны и при прокладке оптоволокна к настольным компьютерам. Оптоволокно редко используется для персональных компьютеров, в основном только в исследовательских подразделениях. Как и с медными кабелями, основная часть расходов – строительные работы, необходимые для прокладки кабеля в стенах. Однако есть и еще одна существенная статья расходов – **оконцовка оптоволокна**, включающая в себя полировку концов волокна и обжимку разъемов, – это трудная и дорогостоящая работа. Если нужно проложить оптоволокно, то это следует сделать до возведения перегородок или одновременно с прокладкой в стенах других коммуникаций. Проложите оптоволокно к каждому настольному компьютеру, но разъемы ставьте только там, где они нужны незамедлительно. Позже, если другим компьютерам потребуется оптоволоконное подключение, можно будет сделать разъемы для них. Расходы на оконцовку меньше, чем затраты и перерывы в работе, связанные с прокладкой нового оптоволокна к IDF.

После прокладки кабелей надо их протестировать. У поставщиков есть специальное оборудование для тестирования, они могут предоставить журнал тестовых распечаток, по странице на каждый сетевой разъем. На графике будет линия или отметка, означающая спад; точка выше такой отметки означает, что разъем не сертифицирован. Мы советуем включить в контракт на монтажные работы условие предоставления такого журнала. Это единственный способ удостовериться, что такое тестирование было проведено. Мы сталкивались с компаниями, которые прокладывают кабель без всякого тестирования.

Чтобы оценить поставщика, осведомитесь об отзывах клиентов и предыдущих заказчиках, к которым можно было бы сходить, чтобы расспросить их и посмотреть на качество работы. Посмотрите на произведенные работы, оцените аккуратность монтажа в IDF. Попросите посмотреть журнал тестовых распечаток поставщика. Прокладка кабелей – дорогостоящая операция, в ней ни на чем нельзя экономить. Устранение проблем позже обойдется гораздо дороже, чем в то время, пока монтажники проводят работы в вашей компании. Экономия в несколько долларов на этапе монтажа не стоит головной боли с постоянным исправлением разнообразных проблем сети. Нередки случаи, когда спустя годы после того, как подрядчик закончил работу, обнаруживаются неисправности, особенно со вторым или третьим разъемом на столе, и выясняется, что разъем никогда и не был работоспособен и не проходил никакого тестирования.

Пример: значение распечаток тестов кабелей

В одной компании из штата Орегон поддерживали каталог кабельных тестов, выполненных на всех разъемах в их зданиях. Когда поступали сообщения об уникальных или трудно воспроизводимых проблемах с отдельными разъемами, в компании выясняли, что быстрый обзор результатов теста разъема, как правило, показывал, что данный разъем проходил тест при минимально допустимых показателях. Процесс исправления неполадок сводился к поиску работоспособного разъема и пометке старого разъема ярлыком «не использовать». Подключения неисправных разъемов ставились в очередь на переобжимку. Дополнительные расходы на покупку полного журнала результатов тестирования окупаются в короткий период.

Короткий кабель от разъема до устройства называется **патч-кабелем**. Как уже говорилось в разделе 6.1.7, мы рекомендуем приобретать готовые патч-кабели, а не делать их самостоятельно. Некачественный кабель может создавать проблемы с надежностью, которые возникают случайным образом и трудно отслеживаются. Замена самодельного патч-кабеля на сделанный профессионально и протестированный может волшебным образом повысить надежность, когда другие методы не помогают.

Еще один момент, который необходимо учитывать при монтаже сетевых разъемов, – это их ориентация. Разъемы устанавливаются в так называемых распределительных коробках или розетках, что и определяет, как будет расположен разъем. В потайных розетках подключенный кабель будет торчать из стены, и потребуется место, чтобы кабель не изгибался на излом. Удостоверьтесь, что места достаточно. Распределительные коробки обычно накладные и, соответственно, выступают из стены. Если разъемы находятся на боковой грани коробки, то они могут быть направлены вверх, вниз, влево или вправо. Разъемы, направленные вверх, будут собирать пыль и строительный мусор. Это плохо. Если они направлены вниз, то трудно будет увидеть, как подключать в них кабель, а при слабом креплении кабельные разъемы будут выпадать. Это тоже нехорошо. Поэтому мы рекомендуем направлять разъемы распределительных коробок влево или вправо.

7.1.5. Центральный кабельный узел

Центральный кабельный узел (Main Distribution Frame, MDF) соединяет все IDF. Между MDF и IDF всегда должно быть достаточно запасных кабелей, так как довольно часто требуются новые подключения, а прокладка дополнительного оптоволокна или кабеля между этажами стоит дорого, и лучше сделать все за один раз. MDF, как и IDF, – продолжение вашего вычислительного центра. Ему необходим тот же уровень физической безопасности, защиты электропитания и охлаждения.

Очень часто MDF является частью вычислительного центра. В таких случаях MDF часто называют **сетевым рядом** или **сетевыми стойками**. Патч-панели в этих стойках подключены к патч-панели на верхней части каждой стойки в информационном центре (рис. 7.7). Более подробно план вычислительного

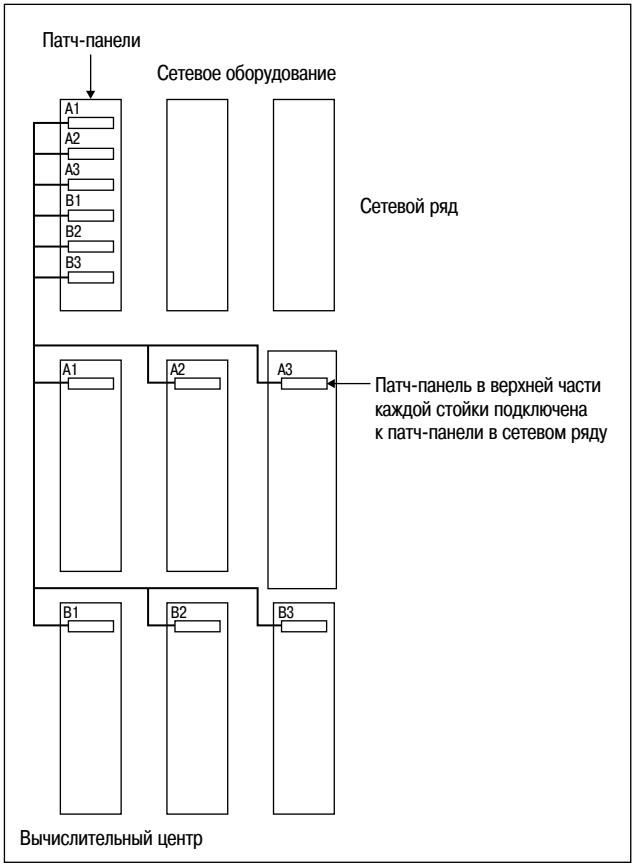

Рис. 7.7. *Патч-панель в каждой стойке вычислительного центра подключена к патч-панели MDF или сетевого ряда*

центра описан в главе 6. В компаниях с большим количеством небольших компьютерных залов каждый из них, как правило, имеет встроенный IDF.

Если вычислительный центр занимает несколько зданий, IDF и MDF, как правило, располагают одним из двух способов. В небольших комплексах каждый IDF подключен к одному MDF в центральном здании. Либо во всех зданиях устанавливаются MDF, каждый из которых затем подключается к центральному MDF. Иногда используются комбинации этих двух способов. Например, каждое малое здание считается крылом ближайшего более крупного здания и все IDF малого здания подключаются к MDF крупного здания.

7.1.6. Точки разграничения

Точка разграничения – это граница между вашей организацией и поставщиком услуг, например телефонной компанией или интернет-провайдером. Точка разграничения может представлять собой распределительный шкаф оптоволоконной линии, коммутационные блоки, щит в стойке, сетевое устройство или даже небольшую пластиковую коробку на стене с разъемом для кабеля. Телефонная компания отвечает лишь за проводку кабеля до своей точки разграничения. Если у вас проблемы с линией, вы должны узнать, где находится соответствующая точка разграничения, и сказать об этом технику, чтобы он не пытался проверить и починить другую эксплуатируемую линию. Кроме того, у вас должна быть возможность тестировать проводку от точки разграничения до сетевого оборудования. Главное, что вам следует знать о точках разграничения, – так это то, где они находятся. Не забудьте об их маркировке.

7.1.7. Документирование

Сетевая документация бывает нескольких видов, и самое основное – маркировка. Необходимость в документировании и его основные виды вряд ли изменятся со временем.

Частью сетевой документации должны быть карты как физической, так и логической сети. Карта физической сети должна отображать, где проходит проводка, местоположение конечных точек и радиус действия беспроводных точек. Если в схеме физической сети предусмотрена избыточность, необходимо четко обозначить и задокументировать физически разные пути. Необходимо обозначить объем и тип подключения для каждого канала. Например, если 200 витых пар и 20 оптоволоконных кабелей соединяют между собой два здания, необходимо четко задокументировать класс обоих типов кабелей, местоположение точек их подключения и расстояние между ними.

Карта логической сети должна отображать топологию логической сети, сетевые номера, имена и скорость. Эта карта также должна показывать все протоколы маршрутизации и административные домены, существующие в сети. Карты физической и логической сетей должны создаваться в масштабе сети организации и определять ее внешние границы.

Маркировка – основная и самая главная составляющая сетевого документирования. Особенно важное значение имеют понятные и последовательные ярлыки на патч-панелях и междугородных каналах. Для патч-панелей должно быть четко обозначено физическое местоположение соответствующей патч-панели или разъемов. Все подключения к патч-панели должны быть четко и последовательно промаркированы с обоих концов. Для междугородных линий на яр-

лыках должно быть четко указано, куда ведет линия, к кому обращаться в случае проблем, какую информацию необходимо приложить к заявке о проблеме (например, идентификатор цепи и ее точку подключения). Такой ярлык, наклеенный непосредственно рядом с индикатором сбоя устройства, может значительно облегчить жизнь. Подобные ярлыки устраняют необходимость отслеживания кабелей с целью поиска необходимой информации при сбое. Например, в некоторых случаях приходится отслеживать кабели от CSU/DSU (Channel Service Unit/Data Service Unit – модуль обслуживания канала и данных) до монтажного блока в точке разграничения телекоммуникационной компании или до разъема на стене.

Временная проводка, такая как сетевые кабели ко всем узлам сети, также должна быть маркирована. Маркировку всех проводов проще поддерживать в относительно спокойном окружении и гораздо сложнее – в динамичном. Не стоит тратить время на маркировку такого уровня, если вы не сможете его поддерживать. Неверные ярлыки хуже, чем их отсутствие.

Компромисс между отсутствием ярлыков и полноценной маркировкой всех кабелей заключается в приобретении кабелей с уникальным серийным номером, указанным на обоих концах кабеля. С помощью этих серийных номеров вы сможете быстро отследить любой кабель, если хотя бы примерно представляете, где находится второй его конец. На ярлыке с серийным номером также может указываться длина и тип кабеля. Например, первые две цифры могут означать прямой кабель, перекрестный кабель, витую пару, FDDI или другой тип кабеля, после чего идет косая черта, а далее три цифры, означающие длину кабеля, затем еще одна косая черта и серийный номер. Для обозначения типа кабеля также могут использоваться разноцветные ярлыки на коннекторах.

Маркировка сетевых кабелей – дело сложное. Один из самых эффективных способов маркировки – использование связки для кабелей с плоским ушком, на которое наклеиваются стандартные самоклеющиеся ярлыки. Ярлыки крепятся легко, и их достаточно просто изменить.

Еще один ключевой аспект документирования – онлайн-документирование, являющееся частью конфигурации самих сетевых устройств. При каждом возможном случае стоит использовать поля комментариев и имен устройств, обеспечивая таким образом документирование для администраторов сети. Стандарты имен устройств могут значительно упростить администрирование сети, сделав его более интуитивно понятным.

Пример: соглашения об именах

В одной транснациональной компании, занимающейся программным обеспечением, для подключения к глобальной сети использовалась топология нескольких звезд. Центр одной из звезд находился в городе Маунтин-Вью, штат Калифорния, США. Маршрутизатор каждой удаленной площадки, подключенный к Маунтин-Вью, носил имя `mesto2mtview` (например, `denver2mtview` или `atlanta2mtview`). Соответствующий маршрутизатор в Маунтин-Вью помимо остальных возможных имен носил имя `mesto-router` (например, `denver-router` или `atlanta-router`).

Если на удаленной площадке возникали проблемы с подключением, можно было мгновенно определить, какие маршрутизаторы обслужива-

ют эту площадку, не прибегая при этом к сетевым картам или к отслеживанию кабелей. Такая стандартизация значительно повысила уровень поддержки по сравнению с тем, на который удаленные площадки могли рассчитывать от обычного системного администратора. Всем, кто был способен устранить обычные ошибки в сети, был дан доступ к сетевому оборудованию с защитой от записи. Эти сотрудники проводили базовую диагностику, прежде чем сообщить о проблеме администраторам сети.

Как правило, маршрутизаторы позволяют для каждого интерфейса записывать текстовый комментарий. Для ГВС-соединений такие комментарии могут включать в себя любую информацию, которая может понадобиться технику в аварийной ситуации при сбое канала (например, название поставщика канала, телефон поставщика, идентификатор цепи, номер договора с поставщиком). Для ЛВС-соединений такие комментарии могут включать в себя имя подсети и контактную информацию владельца подсети (если это не основной отдел системных администраторов). Если ваше оборудование для локальной сети подразумевает наличие поля комментария для каждого порта, в этих полях укажите номера комнаты и разъема на другом конце кабеля.

7.1.8. Простая маршрутизация

Маршрутизацией пусть занимаются маршрутизаторы. Не стоит возлагать обязанность по маршрутизации на узлы сети. Конфигурация узлов должна включать в себя стандартный шлюз (маршрут). Не стоит все усложнять. Маршрутизация в пределах одной площадки должна быть простой, детерминированной, предсказуемой, доступной для понимания и диагностики.

UNIX-системы позволяют использовать многие из тех же протоколов маршрутизации, что и маршрутизаторы, например RIP (Routing Information Protocol), RIPv2. В прошлом, когда на всех узлах сети TCP/IP использовались те или иные UNIX-системы, очень часто все узлы применяли протокол RIP, чтобы определить, куда отправлять пакет. Для 99% узлов, в которых была установлена только одна плата сетевого интерфейса, такое решение было неподходящим, так как большая часть ресурсов процессора и пропускная способность сети использовались для генерации огромной таблицы маршрутизации, которая просто сообщала о том, что необходимо применять только эту единственную плату для всех исходящих пакетов. Такой подход, кроме всего прочего, был небезопасным. Многие сбои в работе локальной сети были вызваны неверными пользовательскими настройками узла, из-за чего последний передавал неверную маршрутную информацию. Все остальные узлы принимали эту информацию, но, ориентируясь на нее, теряли способность соединиться с остальной сетью.

Если ваш маршрутизатор поддерживает такую возможность, запретите отправку протоколов маршрутизации в локальные сети, которым они не нужны. Таким образом вы предотвратите случаи, в которых случайные ошибки в конфигурации приводят к отправке протоколов маршрутизации, а также предотвратите намеренное включение ложной или неверной маршрутной информации.

У узла с одним сетевым интерфейсом должен быть один стандартный маршрут. Он не должен принимать никакую динамическую маршрутную информацию. Узел с несколькими сетевыми интерфейсами не должен отправлять пакеты от

других узлов, но при этом обязан принимать только трафик, адресованный ему. Для такого узла необходима статичная таблица маршрутизации, он не должен принимать динамическую маршрутную информацию, а его конфигурация должна быть максимально простой. Если узел с несколькими сетевыми интерфейсами подключен к сетям A, B и C и ему необходимо связаться с другим узлом в сети B, необходимо использовать сетевой интерфейс, подключенный к сети B. Это самый простой, самый очевидный и самый прямой способ. При отсутствии причин поступить иначе весь трафик для сетей, которые не подключены напрямую к узлу с несколькими сетевыми интерфейсами (то есть к узлам, которые не находятся в сети A, B или C), должен направляться к статичному стандартному маршрутизатору. Это и есть простейшая конфигурация маршрутизации для узла с несколькими сетевыми интерфейсами. В некоторых случаях может понадобиться добавление дополнительных статичных маршрутов в узел с несколькими сетевыми интерфейсами для направления трафика по рекомендуемым путям. Например, узел с несколькими сетевыми интерфейсами можно сконфигурировать для отправления трафика для сети D через маршрутизатор в сети C и для отправления трафика для сетей, отличных от A, B, C или D, через маршрутизатор в сети A. Однако по возможности лучше избегать сложности даже такого уровня.

Простая маршрутизация является более детерминированной, благодаря чему упрощает и делает более предсказуемым решение сетевых проблем. Если все узлы сети сконфигурированы одинаково, они должны и вести себя одинаково. Если узлы получают динамическую маршрутную информацию, может произойти непредвиденное. Что еще хуже, если узлы активно участвуют в динамической маршрутизации, поведение всей среды может стать абсолютно непредсказуемым. Если это возможно, внедрите инструкцию, в соответствии с которой узлы не смогут участвовать в вашей инфраструктуре динамической маршрутизации с использованием всех механизмов безопасности и аутентификации, предусмотренных протоколом.

Пример: проблемы из-за сложной маршрутизации

В одной крупной транснациональной компании, занимающейся производством компьютеров, в период, пока основные протоколы маршрутизации все еще были в разработке, на всех настольных компьютерах и серверах для маршрутизации использовалось программное обеспечение. Каждый раз, когда какое-либо из устройств в сети отправляло неверную или ошибочную информацию, это отражалось на всех машинах. Кроме того, в компании постоянно возникали проблемы с несовместимостью между ее разработками некоторых протоколов и разработками поставщика сетевых устройств. Если бы узлы сети использовали простую статичную маршрутизацию, этих проблем можно было бы избежать.

Если узлы занимаются маршрутизацией, это может привести к снижению быстродействия. По мере роста количества маршрутов в сети проводить обновление протоколов маршрутизации становится все сложнее. Нам доводилось встречаться с крупными сетями, в которых работа каждого узла приостанавливалась каждые 300 с при отправке протокола RIP и одновременной его обработке всеми узлами локальной сети. Если подсеть содержит ровно один маршрутизатор, нет

необходимости трансляции протокола маршрутизации в эту подсеть. Это означает, что можно использовать **пассивный режим**. Более того, если протокол маршрутизации использует широковещательные трансляции (другими словами, **оповещения**), может возникнуть серьезная проблема с быстродействием, даже если конфигурация узлов сети не предусматривает связь с протоколами маршрутизации. Трансляции не только занимают полосу пропускания сети. Кроме того, все узлы подсети прекращают обработку трансляции, даже если обработка заключается в простом отказе от пакета.

7.1.9. Сетевые устройства

«Строительным материалом» для любой современной сети должны быть выделенные сетевые устройства, такие как маршрутизаторы и коммутаторы, а не универсальные узлы сети, сконфигурированные для маршрутизации. Эти сетевые устройства должны быть созданы специально для выполнения одной задачи, связанной с передачей пакетов или управлением трафиком, а также с самим устройством. Не следует использовать универсальные устройства, сконфигурированные только для управления сетевым трафиком. И разумеется, это не должны быть устройства, которые параллельно пытаются выполнять другие задачи и предоставлять дополнительные услуги.

До того как появились сетевые маршрутизаторы, для маршрутизации использовали сконфигурированные UNIX-системы с несколькими Ethernet-картами. Позднее Cisco и другие компании выпустили в продажу маршрутизаторы и другие сетевые устройства, основанные на собственных конфигурациях оборудования и прошивки. Сетевые устройства оптимизированы для максимально быстрой передачи пакетов. Они снижают задержки при передаче пакетов (или время ожидания), лучше подходят для интеграции со средствами управления сетью, предоставляют хорошие средства мониторинга и являются более простыми устройствами, что означает пониженную склонность к поломкам, так как в них меньше подвижных деталей.

Маршрутизация пакетов производится в ядре – это означает, что ей отводится наивысший приоритет по сравнению со всеми другими функциями. Если роль маршрутизатора у вас выполняет файловый сервер, вы заметите, что чем больше сетевого трафика обрабатывается, тем медленнее работает файловый сервис. Время работы ядра часто не учитывается системными средствами. Мы встречались с проблемами быстродействия, которые невозможно было определить обычными средствами диагностики, так как ядро незаметно передавало циклы процессора на маршрутизацию трафика.

Пример: центральный узел сети

У одного производителя компьютерного оборудования[1] была сеть, построенная вокруг одного узла сети с несколькими сетевыми адаптерами, который в основном занимался маршрутизацией трафика. Однако, из-за того что это была универсальная машина, удобно подключенная ко всем ключевым сетям, со временем в узел добавлялись другие сервисы. Иногда в работе этих других сервисов возникали проблемы или перегрузки, что

[1] Парадоксально, но сама эта компания занималась разработкой и производством выделенных устройств, выполняющих одну конкретную операцию в сети.

приводило к разрыву соединения с сетью или к серьезным проблемам быстродействия сети.

Когда пришло время заменить эту машину другой выделенной машиной, сделать это оказалось намного сложнее, чем могло бы быть. Новое оборудование было предназначено исключительно для маршрутизации пакетов. Это не была универсальная машина. Все остальные сервисы, выполняемые на старой машине, пришлось отследить и соответственно изменить архитектуру сети, в которой они более не должны были запускаться на одной машине, подключенной ко всем сетям.

Через подобную схему эволюции прошли брандмауэры. Изначально брандмауэры представляли собой серверы или рабочие станции со специальным программным обеспечением, которое добавляло в операционную систему функциональность фильтрования. Но потом на рынке появились готовые отдельные аппаратные брандмауэры. Преимуществом этих устройств была возможность обрабатывать больший объем трафика без снижения скорости работы. При этом в такие брандмауэры добавлялось множество новых возможностей. Позднее их догнали по функциональности программные брандмауэры, и с тех пор оба эти вида находятся в постоянном соперничестве друг с другом. Недостатком программного подхода является соблазн добавить на ту же машину дополнительные сервисы, что повышает риск возникновения бреши в безопасности. Мы предпочитаем, чтобы брандмауэр занимался исключительно фильтрацией и не выполнял бы роль файлового сервера, почтового сервера и вдобавок открывалки и штопора. Программные системы зачастую являются заказными или импровизированными решениями, которые абсолютно не поддаются обслуживанию после того, как человек, внедривший их, покидает компанию. С другой стороны, программные решения, как правило, являются более гибкими и характеризуются лучшим расширением возможностей, чем у аппаратных решений. Но в целом мы предпочитаем использовать выделенные аппаратные брандмауэры.

У компьютерного и сетевого оборудования разные графики обновления. После установки сетевого устройства обновлений программного обеспечения и изменений в конфигурации начинают избегать и откладывать их до самых крайних случаев. Серверы приложений обновляются, переконфигурируются и перезагружаются чаще. Несоответствие этих графиков на одной машине становится причиной неудобств для каждого сотрудника, имеющего дело с данной машиной.

Хотя в сообществах с системами UNIX уже не используют рабочие станции и серверы в качестве маршрутизаторов, наблюдается тревожная тенденция, в соответствии с которой такие поставщики, как Майкрософт, Novell и Apple, поощряют использование универсальных машин в качестве маршрутизаторов, брандмауэров или сервисов удаленного доступа. Мы же считаем, что это те самые грабли, на которые не стоит заново наступать.

Слишком много яиц в одной корзине

В 2004 году одна небольшая компания, представительства которой располагались по всему миру, решила внедрить новую компьютерную и сетевую архитектуру. В соответствии с этим в каждом офисе был уста-

новлен сервер Apple OS X, который играл роль интернет-маршрутизатора, брандмауэра, а также почтового, файлового и веб-сервера в подразделении компании. Любая проблема с любым приложением на сервере превращалась в проблему для всех приложений на сервере. Ошибку в файловом сервере можно было устранить только путем перезапуска всей системы. При отказе жесткого диска все подразделение компании лишалось доступа к Интернету и сотрудники не могли даже сделать заявку на замену диска. Установка срочных патчей и обновлений программного обеспечения откладывалась из опасения, что она может нарушить работу какого-нибудь сервиса. Если в Интернет выходило слишком большое количество пользователей, работа файлового сервиса замедлялась, что приводило к эффекту домино, отследить который было практически невозможно.

Тома пригласили для повышения стабильности работы сети. Ушло несколько месяцев на то, чтобы перевести все подразделения компании на выделенные аппаратные брандмауэры, но вскоре приложения были отделены от маршрутизации и фильтрации брандмауэра. И хотя это было основное изменение, внедренное Томом, повышение стабильности не заставило себя ждать.

Домашние маршрутизаторы

Конфигурация системы Linux или FreeBSD в качестве маршрутизатора для домашней сети – отличный способ узнать много нового о сетях и брандмауэрах. И тем не менее для дома мы рекомендуем использовать аппаратные маршрутизаторы пользовательского класса. Приобрести такое устройство вы сможете за 50–100 долларов. Его функциональности вам хватит за глаза, а стоимость окупится на экономии электроэнергии. Кроме того, у таких устройств нет кулера, поэтому работают они бесшумно, что тоже является плюсом.

7.1.10. Оверлейные сети

Оверлейная сеть – логическая топология, наложенная на физическую топологию. Примерами таких сетей являются VLAN, Frame Relay и ATM. Этот принцип позволяет создавать простые физические архитектуры, которые могут поддерживать любую необходимую сложность логического наложения и при этом сохранять простоту на физическом слое.

Можно создать очень простую (а значит, стабильную) однородную физическую сеть, а затем построить оверлейные сети на этой прочной основе, чтобы получить возможность для более сложных подключений. На уровне глобальной вычислительной сети это может означать, что у всех площадок установлено единое подключение к ATM или распределенная сеть Frame Relay. Затем коммутаторы ATM или Frame Relay конфигурируются таким образом, чтобы между площадками был создан виртуальный канал. Например, от каждого удаленного офиса может идти виртуальный канал к главному офису. Если какая-либо пара удаленных площадок обменивается трафиком большого объема, достаточно просто

изменить конфигурацию коммутатора, добавив виртуальный канал между этими площадками. Одной из распространенных конфигураций является полная **ячеистая топология**, в которой каждая площадка с помощью виртуального канала подключена ко всем остальным площадкам. Преимуществом такой сети является тот факт, что основная площадка не перегружена проходящим через нее трафиком, а компании не приходится нести дополнительные затраты и проходить через процедуру установки нового физического канала. Еще одним примером для ГВС является использование туннелей с шифрованием (виртуальных частных сетей) при передаче данных через Интернет. Компании достаточно обеспечить каждую площадку брандмауэром, VPN-устройством и подключением к Интернету и создать ГВС через Интернет. Кроме того, интернет-провайдеры могут использовать этот подход для создания и обслуживания одной стабильной инфраструктуры, которая буквально снова и снова продается разным клиентам.

На уровне локальной сети оверлейная сеть, как правило, означает создание простой однородной физической топологии и использование VLAN-протоколов IEEE 802.1q для наложения подсетей, необходимых пользователям. Например, каждый IDF можно подключить к MDF с помощью высокоскоростных избыточных каналов, которые служат связующим звеном на уровне 2 (уровень канала Ethernet) при использовании протокола STP (Spanning Tree Protocol).

Пример: крупные локальные сети, использующие VLAN

Самая крупная локальная сеть, проведенная в одном здании, с которой когда-либо приходилось сталкиваться Тому, включала в себя почти 100 IDF и поддерживала 4000 пользователей по всему зданию. Каждый IDF был подключен исключительно к одному MDF. Даже если на одном и том же этаже было установлено два IDF, подключение шло от одного IDF к MDF, а уже затем ко второму IDF. Такая простая схема означала, что подключение двух IDF проходило через MDF. Хотя это может показаться излишним, ведь в некоторых случаях IDF устанавливались всего на расстоянии одного этажа друг от друга, такая схема намного лучше, чем тот кошмар, через который пришлось бы проходить при прямом подключении всех IDF друг к другу.

Но один аспект с трудом поддавался обслуживанию и поддержке. Некоторым пользователям требовалось наличие их подсетей в одном IDF или в паре IDF, а другим – наличие их подсетей практически во всех IDF. Каждая подсеть была индивидуально привязана к MDF с соответствии с необходимостью. Например, если нужен был разъем, находящийся в крыле, обслуживаемом IDF, который не включал в себя необходимую подсеть, между данным IDF и MDF протягивалось оптоволокно. Затем в этом IDF устанавливался хаб, который подключался к хабу нужной подсети в MDF. Все это означало, что при первом запросе к подсети в любой части здания на подключение уходило немало времени. По мере роста сети и включения сотен подсетей обслуживание сети превратилось в настоящий кошмар. Сложно было даже отследить, какие подсети в каких IDF присутствовали. При активации практически каждого нового разъема требовались огромные усилия и ручной труд.

После проведения модернизации эта сеть обслуживала то же физическое оборудование, но отдельные оптоволоконные каналы были заменены в ней на крупную плоскую сеть с оверлеями. В каждом IDF был установлен большой коммутатор Fast Ethernet. Каждый коммутатор был подключен еще к более крупным коммутаторам в MDF. Эти подключения были избыточными подключениями Gigabit Ethernet. Несмотря на то что это была огромная однородная сеть с точки зрения уровня 1, на уровне 2 на нее были наложены VLAN. Таким образом, запросы на изменение сети подразумевали изменение в коммутаторах, которые происходили без непосредственного вмешательства системных администраторов. Чтобы доставить определенную подсеть к IDF, системному администратору больше не приходилось протягивать и подключать оптоволокно. Вместо этого достаточно было сконфигурировать соответствующий VLAN, чтобы расширить его до нужного IDF, и сконфигурировать коммутатор в IDF, чтобы предоставить этому VLAN соответствующий порт. В результате значительно снизились издержки на обслуживание и ускорился отклик на запросы изменения.

Эта схема будет надежна и в будущем. Каналы до MDF можно заменить на более быстрые технологии (если, конечно, будущие технологии будут совместимы с типом оптоволокна, которое уже установлено, а также смогут поддерживать VLAN). Если новые технологии будут основаны на кольцевых топологиях, эти топологии можно создать по схеме топологии звезды IDF и коммутаторы станут узлами кольца.

При использовании VLAN и наложенных сетей очень сложно создать точные диаграммы сетевых топологий. Рекомендуем создать две диаграммы: одну, изображающую физическую топологию, и вторую, представляющую логические сети.

7.1.11. Количество поставщиков

Использование оборудования от большого количества разных поставщиков может излишне усложнить управление сетью. Чем больше поставщиков предоставляют вам сетевое оборудование, тем больше проблем с взаимодействием у вас, скорее всего, появится. Кроме того, увеличивается нагрузка на администраторов сети, которым придется изучить конфигурации и особенности разного оборудования, а также следить за обновлением программного обеспечения и отслеживать ошибки. Если свести количество поставщиков к минимуму, можно повысить надежность и упростить обслуживание сети. Кроме того, это поможет компании получить дополнительные скидки на оборудование благодаря увеличению объема поставок.

Однако сотрудничество с одним эксклюзивным поставщиком тоже имеет свои недостатки. Не может быть такого, чтобы один поставщик производил лучшую продукцию во всех областях. При сотрудничестве исключительно с одним поставщиком ваш протокол остается непроверенным на взаимодействие, что может привести к неприятным сюрпризам при первом же контракте с новым поставщиком.

Необходимо найти золотую середину. В некоторых компаниях предпочитают сотрудничать с одним поставщиком на каждом уровне протоколов или сети.

Например, можно использовать ГВС-маршрутизаторы от одного поставщика, центральные коммутаторы локальной сети – от другого, а хабы и коммутаторы в офисах – от третьего.

7.1.12. Стандартные протоколы

Сеть организации должна быть создана с использованием стандартных протоколов. Это правило со временем не меняется. Проприетарные протоколы поставщиков привязывают вас к одному конкретному поставщику, осложняя при этом интеграцию оборудования от других производителей. Привязка к одному поставщику усложняет получение скидок и мешает внедрить продукцию других компаний, лишая вас возможности использовать ее преимущества. Кроме того, на вас сказываются деловые проблемы вашего поставщика.

Если вам нужны возможности, предоставляемые исключительно проприетарными протоколами поставщика, старайтесь убедить поставщика открыть стандарт. В идеале стандарты должны быть проверенными, а не новыми, чтобы обеспечить совместимость со всем оборудованием. Использование проверенных временем стандартов IETF означает, что любое выбранное вами оборудование или программное обеспечение будет совместимо с этими стандартами. Проверенные временем стандарты IETF отличаются стабильностью и не вызывают проблем совместимости версий. Если поставщик хвалится новыми исключительными возможностями, узнайте у него номер IETF RFC или название документа IEEE, описывающего данный стандарт. Если новые возможности не стандартизированы, спросите у поставщика, каким образом данное оборудование будет взаимодействовать с устройствами других поставщиков, имеющимися у вас. По данной теме также смотрите разделы 5.1.3 и 23.1.6.

7.1.13. Мониторинг

Мониторинг сети необходим для построения быстрой и надежной сети, для масштабирования сети в соответствии с растущими потребностями, для поддержания безотказности сети. Только мониторинг позволит вам узнать, насколько хорошо работает ваша сеть и насколько она надежна. Сетевой мониторинг представлен двумя основными типами. Первый – мониторинг и оповещение о работоспособности в реальном времени. Второй тип – сбор данных для анализа тенденций изменения, который проводится с целью предсказания будущего спроса и составления счетов за пользование. Для компаний, предоставляющих услуги через Интернет (будь то интернет-провайдер, провайдер услуг доступа к приложениям или электронная коммерция), оба типа мониторинга являются неотъемлемой частью работающего бизнеса. В корпоративных сетях оба вида рекомендуются к использованию, но, как правило, они не имеют критичного значения для самого бизнеса.

Мониторинг сети в реальном времени должен быть внедрен во все используемые у вас системы уведомления о неисправностях. Как минимум, такой мониторинг должен оповещать вас об изменениях состояния сетевого интерфейса. Другими словами, система мониторинга должна сообщать об отказах сетевого интерфейса и, предпочтительно, о восстановлении его работоспособности. В идеале система мониторинга также должна оповещать о проблемах с маршрутизацией, хотя конкретный вид мониторинга при этом обуславливается протоколом маршрутизации. Также необходимо учитывать оповещения на основе необычных

явлений. Например, неожиданные всплески или падения трафика могут означать наличие той или иной проблемы. Всплески могут означать сбои в конфигурации компьютера, наличие нового проблемного приложения, вируса или червя. Падение трафика может свидетельствовать о проблемах с проводкой или об обеденном перерыве.

Сетевой трафик и обеденные перерывы

Однажды Тому пришлось иметь дело с демонстрацией работы системы мониторинга сети. Представитель поставщика подключил систему и увидел, как огромный объем трафика практически перегружает все порты. Так продолжалось в течение нескольких минут, после чего наступило почти полное затишье.

Представитель поставщика сначала решил, что он имеет дело с самой перегруженной сетью в мире, а потом начал сомневаться, подключены ли вообще к сети какие-либо устройства. В результате выяснилось, что в этой компании, занимающейся автоматизированным проектированием, практически все сотрудники уходили на обед ровно в полдень. Каждый день в 11:59 все сохраняли свои тяжеловесные проекты и уходили в столовую. Одновременная запись такого огромного объема данных перегружала сеть и файловые серверы, но пользователей на месте не было, так что этого никто даже не замечал. После завершения сохранения данных в сети было тихо до того момента, как пользователи возвращались на свои рабочие места.

Так случилось, что систему мониторинга включили почти ровно в полдень. В остальное время объем трафика был в норме.

Самая распространенная и самая важная цель сбора статистических данных – прогнозирование будущих потребностей. В большинстве сетей достаточно просто вести мониторинг всех нужных сетевых интерфейсов, отслеживая проходящий через них объем трафика и проводя анализ тенденций изменения. Это позволит определить момент, в который понадобится увеличение пропускной способности. В других сетях (особенно в компаниях, связанных с интернет-услугами) предпочитают собирать данные о трафике в сети, определяя, с кем необходимо осуществить прямое подключение, какой должна быть пропускная способность таких подключений и где должны находиться такие пункты географически, чтобы можно было оптимизировать трафик в сети.

Сбор статистических данных по сбоям, ошибкам и отказам также может оказаться полезным и информативным, отображая моменты появления проблем и их исчезновения. С помощью анализа статистических данных можно выделять аномалии в поведении систем, которые могут свидетельствовать о наличии проблем (Brutlag 2000), или создавать статистику работоспособности для руководства или пользователей. Вы поймете, насколько полезен статистический мониторинг, когда посмотрите на график использования сети, проследите за траекторией роста и определите момент перегрузки данной линии и необходимость увеличения ее пропускной способности.

Более подробно мониторинг описан в главе 22.

7.1.14. Одна административная единица

Грамотное создание сетей, их обслуживание и решение связанных с ними проблем одновременно в нескольких организациях – задача сложная. Сеть должна быть единым организмом, передающим трафик последовательно и координированно. Сеть должна регулироваться единым набором правил и инструкций, которые единообразно используются по всей сети. Чем больше независимых групп управляют движением трафика, тем выше риск, что работа сети станет несогласованной и нескоординированной. Использование одной административной единицы означает наличие одной организованной административной группы с единой структурой управления. Если разные отделы группы администраторов подчиняются структурам управления, которые пересекаются лишь на уровне генерального директора, различные подразделения компании неизбежно начнут двигаться в разных направлениях, следуя своим собственным инструкциям и правилам.

Пример: проблемы из-за отсутствия единой административной группы

В одной крупной транснациональной компании, занимающейся производством компьютерного оборудования, за разные части сети отвечали различные группы сотрудников. Эти группы подчинялись разным структурам управления. В каждом подразделении одна узкоспециализированная группа отвечала за глобальные вычислительные сети, а другая более или менее свободная группа – за локальные сети. Разные группы не смогли прийти к единому мнению, какой протокол маршрутизации следует использовать в компании. Отчасти эти разногласия были связаны с наличием разных органов управления. Некоторые сетевые группы, работающие в том или ином подразделении, подчинялись технической группе, которая считала, что все настольные компьютеры (для них использовалось исключительно то программное обеспечение и оборудование, которое производила сама компания) должны участвовать в маршрутизации. Это условие жестко ограничило набор возможных сетевых протоколов, ни один из которых не отвечал другим требованиям, выдвинутым группой ГВС. В результате эти две группы использовали разные протоколы маршрутизации, выделив несколько избыточных точек для обмена маршрутной информацией. Однако из-за несогласованности работы этим двум группам так и не удалось вывести правильную конфигурацию, что приводило к маршрутным петлям при каждом одновременном подключении обеих избыточных точек передачи управления. Если бы в компании существовала единая административная группа, всех этих проблем можно было бы избежать.

С отсутствием одной административной единицы связаны и проблемы безопасности. Если разные части сети контролируют различные группы, у каждой такой группы будут свои правила относительно подключения других сетей к их участку сети и обеспечения безопасности таких подключений. Это приводит к невозможности контролировать уровень безопасности сети, так как сеть – единое целое и ее безопасность определяется ее слабейшим звеном.

Наличие единой административной единицы не исключает возможность привлечения групп администраторов из других подразделений или регионов, которые должны подчиняться одной и той же структуре управления и одному и тому же своду правил и инструкций. Сеть останется единым организмом, если несколько групп администраторов будут работать согласованно друг с другом (раздел 7.2.2).

7.2. Тонкости

Помимо базовых задач существует несколько дополнительных аспектов, которые помогут вам улучшить свою сеть. Вы должны добиться баланса между рискованным внедрением новых передовых технологий и использованием более старых, но и более надежных технологий и оборудования. И наконец, если вы окажетесь в ситуации, которая потребует от вас создания нескольких административных единиц, вы можете последовать нашим советам, чтобы снизить опасность возникающих проблем.

7.2.1. Передовые технологии или надежность

Как правило, самое важное качество сети, которого все добиваются, – это надежность. Более старые решения, которые прошли множество проверок как в аппаратном аспекте, так и в отношении прошивки, обычно отличаются повышенной надежностью. Все ошибки в них уже исправлены. С другой стороны, новые возможности и увеличенная скорость подключения, как правило, доступны только в новых продуктах, которые, возможно, еще не прошли полевые испытания. И именно вы должны добиться нужного баланса.

Существует множество способов для управления этим риском. Вы можете проводить в лаборатории собственную сертификацию новых решений до их внедрения, а затем приступить к их постепенному развертыванию. Это позволит повысить уверенность в успехе до того, как вы приступите к массовой установке новых решений. Сертификация должна включать в себя документирование процесса установки и стандартов конфигурации.

Вы можете создать отдельные клиентские группы, различающиеся между собой степенью риска, на который они готовы пойти. Кто-то, возможно, согласится несколько снизить надежность в обмен на доступ к новым возможностям. Но даже в этом случае такое оборудование необходимо сначала протестировать в лаборатории. Даже тем, кто предпочитает передовые технологии, все же нужна надежность.

В некоторых случаях клиентские группы, которые согласны пойти на риск, находятся в ведении другого отдела системного администрирования. А у этого отдела могут быть клиентские группы с бизнес-требованиями, такими как необходимость использовать некоторые новые технологии, как только они становятся доступными. Если это возможно, предоставьте *им* разбираться с проблемами и используйте свой шанс позволить другим вместо вас исправлять ошибки. Учитесь на их опыте.

Если вы используете новейшие технологии, удостоверьтесь, что каждый сотрудник, который может столкнуться с проблемами на первых этапах внедрения этих технологий, знает, что из-за их новизны возможны сбои и простои в работе. Если не сделать этого заранее, ваши пользователи расстроятся, а репутация

вашей сети в целом серьезно пострадает. Если кто-либо из руководства одобряет подобный риск, обязательно сообщите об этом конечным пользователями и их непосредственным руководителям, чтобы в возможных простоях не обвиняли лично вас. И даже в этом случае оборудование необходимо сначала настроить и протестировать в лаборатории.

Технологии

- *Ведущие технологии*. Самые современные технологии. Вы возглавляете движение в эру новых технологий.
- *Передовые технологии*. Это означает, что вы внедряете инновации раньше, чем они становятся ведущими технологиями. Слово «передовой» также означает «ближайший к неприятельскому фронту».
- *Ударные технологии*. Удар – именно то, что получают юзеры, если они постоянно находятся на передовой.

7.2.2. Несколько административных единиц

По различным политическим, практическим или связанным с безопасностью причинам создать одну административную единицу может быть невозможно. Если разные организации управляют различными частями сети и не подчиняются единому уставу или единому органу управления, сети необходима другая модель. Между различными частями сети должны быть явные границы, созданные с использованием пограничных протоколов маршрутизации, таких как BGP, и систем безопасности, в число которых входят брандмауэры. Это позволит обеспечить стабильность маршрутизации и создать известные уровни безопасности в каждой административной единице независимо от других.

Достаточно часто используется следующее разделение: одна группа – для возможности подключения к глобальной вычислительной сети, а другая – для обеспечения подключения к локальной сети. Такой подход разумен, так как для поддержки этих сетей требуется разная квалификация. То же самое касается создания отдельной группы для управления подключением к Интернету или для сетевой безопасности.

Если вам требуется создать несколько административных единиц, сделать это необходимо должным образом. Действия и решения одной группы администраторов должны быть полностью независимыми от действий других групп и при этом не должны влиять на работу или надежность других сетей. Проведите совещание с целью выработки общепринятых стандартов и утвердите комиссию из представителей каждой группы, которая будет отвечать за внедрение главных стандартов.

7.3. Заключение

В этой главе мы рассмотрели различные аспекты разработки и создания сети. Так как сетевые технологии стремительно меняются, некоторые из этих аспектов со временем также претерпят значительные изменения. Но остальные аспекты создания сети являются неизменными (константами). В этой главе мы

описали, каким образом технологии повлияли на сети, а также рассказали о факторах, которые всегда необходимо учитывать.

Итак, хотя многие ключевые факторы, определяющие способ создания сети, постоянно меняются, у вас есть возможность в качестве основы для своей сети использовать некий фундамент, который упростит создание надежной сети и позволит вам двигаться в ногу со временем.

7.3.1. Константы создания сети

- Необходимость четкой архитектуры.
- Надежность.
- Грамотное документирование и ярлыки.
- Соответствие IDF и MDF высочайшим стандартам проводки.
- Надежные системы энергопитания и охлаждения для IDF и MDF.
- Последовательное размещение IDF на всех этажах и во всех зданиях.
- Точки разграничения.
- Если возможно, создание одной административной единицы. В противном случае четкое разграничение обязанностей.
- Стандартные открытые протоколы (IETF и IEEE).
- Простая маршрутизация узлов.
- Выделенное сетевое оборудование для передачи пакетов.
- Минимальное количество поставщиков.
- По возможности отказ от использования ударных технологий.

7.3.2. Изменчивые аспекты создания сети

- Необходимый тип проводки в помещении и между помещениями.
- Топологии физических и логических сетей.
- Сетевые устройства и протоколы.
- Возможности подключения к глобальной вычислительной сети.
- Структура подключения к Интернету.
- Методы избыточности.
- Технологии мониторинга.

Задания

1. Нарисуйте карту физической сети вашей организации.
2. Нарисуйте карту логической сети вашей организации.
3. Каким образом осуществляется маршрутизация пакетов между узлами сети? Где в сети существует избыточность? Если избыточности нет, каким образом ее можно внедрить?
4. Представьте, что ваша компания только собирается переезжать в помещение, которое вы сейчас занимаете. У вас есть возможность изменить размещение IDF и MDF. Что бы вы сделали? Насколько такое размещение отличалось бы от существующего в настоящий момент?

5. Где располагаются ваши точки разграничения? Каким образом они документированы и маркированы?
6. Какие протоколы используются в вашей сети и какие соответствующие RFC-номера они имеют? Есть ли среди них проприетарные протоколы? Если да, каким образом можно избежать использования этих протоколов?
7. Оборудование каких поставщиков вы используете в сети? Каким образом можно снизить количество этих поставщиков? Каковы преимущества и недостатки такого шага?
8. Какова политика (неофициальная или какая-либо другая) вашей организации относительно использования оборудования ведущих технологий? Каким образом вы ограничиваете отрицательное влияние этого оборудования на надежность?
9. Если в вашей организации существует несколько административных единиц, каким образом можно применить подход, описанный в разделе 7.2.2?
10. Мониторинг чего ведется в вашей сети? Мониторинг чего вы хотели бы проводить и что нужно для этого сделать?

Глава 8

Пространства имен

В этой главе мы опишем принципы организации и управления пространствами имен. Пространство имен – это набор уникальных ключей и связанных с ними атрибутов. Примерами пространства имен могут служить используемые регистрационные записи, доступные принтеры, имена хостов, Ethernet-адреса, списки названий сервисов/номеров портов и карты расположения домашнего каталога. В пространстве имен для каждого элемента предусмотрены атрибуты. Для регистрационных записей существуют идентификаторы UID (UNIX) или SID (Windows), домашние каталоги, владельцы и т. д. Атрибуты имени хоста, как правило, включают в себя IP-адреса, серийные номера оборудования, информацию о пользователе (владельце), MAC-адрес Ethernet и т. д.

Термин *пространство имен* может сбить с толку, поскольку относиться он может как к абстрактному понятию, так и конкретному явлению. Например, имена пользователей – это пространство имен. В каждой многопользовательской операционной системе есть пространство имен, которое представляет собой список идентификаторов пользователей. То есть в любой среднестатистической компании есть абстрактное понятие пространства имен для имен пользователей. Однако пространство имен одной компании будет отличаться от пространства имен любой другой компании (если, конечно, вы не переманили у меня всех сотрудников!). В этом смысле компании обладают разными пространствами имен для имен пользователей (ваш набор пользователей и мой набор пользователей). По большей части в данной главе термин «пространство имен» относится к определенной (конкретной) базе данных пространства имен. В случаях, когда требуется уточнение смысла, мы это указываем.

Пространства имен бывают самых разных видов. Некоторые из них являются плоскими, то есть не имеют копий. Например, в Windows каталог **WINS** является плоским пространством имен. В UNIX набор идентификаторов UID – плоское пространство имен. Другие пространства имен являются иерархическими, например дерево каталогов. В каждом отдельном каталоге не могут существовать два файла с одинаковым именем. Но два файла с одним и тем же именем example.txt могут находиться в разных подкаталогах.

Чем крупнее и сложнее система, тем важнее формализовать управление пространством имен. Небольшие системы требуют значительно меньшей формализации своих пространств имен. Один человек в состоянии управлять ими и держать необходимую информацию в памяти. Но мегакорпорации должны разделять и делегировать ответственность между несколькими подразделениями и сотрудниками.

В первую очередь важно осознать, какую роль играют пространства имен в вашей системе. Без них у вас была бы просто беспорядочная куча данных. Рассматривая каждое пространство имен независимо от других, мы упускаем преимущества от их взаимосвязи. Начинающие системные администраторы зачастую воспринимают каждое пространство имен как отдельный элемент, но со временем приобретают навык видеть более общую картину. Они учатся видеть весь лес целиком, а не каждое дерево в отдельности. Рассмотрение отдельного пространства имен в контексте общего плана дает новые возможности.

В этой главе мы рассмотрим основы управления пространствами имен, а затем исследуем более сложные темы управления и использования пространств имен. Эта глава должна помочь вам увидеть лес за деревьями.

8.1. Основы

Основы пространств имен очень просты:

- Пространствам имен необходимы политики по именам, долговечности, локальности и защищенности.
- Пространствам имен необходимы процедуры: добавление, изменение и удаление.
- Пространствам имен необходимо централизованное управление.

8.1.1. Политики для пространств имен

Пространства имен должны подчиняться общим политикам, а не отдельным технологическим системам. Чем крупнее ваш отдел системных администраторов, тем важнее оформить политики в письменном виде, а не просто полагаться на устные традиции. По мере роста отдела такие письменные политики становятся средством взаимодействия с системными администраторами и обучения новых системных администраторов. Нельзя сделать выговор системному администратору за то, что он разрешил дать имя новому компьютеру вразрез с правилами, если эти правила не оформлены в письменном виде. Письменные политики должны быть основой требований, составляемых при создании автоматизированного обслуживания пространств имен. Кроме того, письменные политики регулируют отношения с клиентами.

8.1.1.1. Назначение имен

Политика по назначению имен для пространств имен должна отвечать на следующие вопросы. Какие имена разрешены в пространстве имен? Какие имена запрещены в пространстве имен? Каким образом выбираются имена? Каким образом решается проблема перекрытия имен? В каких случаях допускается переименование?

Необходимы правила, какие имена могут стать частью пространства имен. Некоторые правила диктуются технологией. Например, в UNIX-системах логины могут включать в себя только алфавитно-цифровые символы при ограниченном их количестве. Кроме того, правила могут диктоваться корпоративным стилем, например ограничениями на «оскорбительные» логины. Внешние стандарты также влияют на правила. До RFC 1123 (Braden 1989, Section 2.1)

имена DNS не могли начинаться с цифры, из-за чего компании 3Com было сложно зарегистрировать свой домен.

При выборе имен можно использовать несколько методов:

1. *Шаблонный*. Все имена составляются по строгому шаблону. Например, все настольные рабочие станции получают имена `pc-` и четырехзначное число. Логины могут составляться по следующей формуле: инициалы плюс шесть первых букв фамилии плюс случайный набор цифр, чтобы сделать имя уникальным.
2. *Тематический*. Все имена соответствуют определенной теме. Например, все серверы можно назвать в честь планет (если названий настоящих планет слишком мало, можно использовать планеты из научной фантастики).
3. *Функциональный*. Имена соответствуют функциям. Учетные записи могут соответствовать должностям и ролям (`admin`, `secretary`, `guest`); имена узлов могут отражать обязанности машины (`dns1`, `cpuserver22`, `web01`) или группы доступа (`webmaster`, `marketing`).
4. *Описательный*. Описательные имена обычно отражают фактическую информацию, а не правила. Подходящими примерами здесь являются метки разделов диска, описывающие пользователей или данные, для которых предназначен данный раздел диска (`S:\Otdel\Finance`, `test data`). Имена принтеров могут сообщать, какой используется принтер с драйвером (`laserjet`, `photo`, `11Ч14`) или где этот принтер установлен (`testlab`, `inkjet`, `CEO-desktop`). Крупные организации часто используют географические названия (названия городов или коды аэропортов) для групп доступа и почтовых списков (`sjc-all`, `chicago-execs`, `reston-eng`).
5. *Нет метода*. Иногда шаблоном является отсутствие шаблона. Каждый выбирает что-нибудь свое. Конфликты и перекрытия имен решаются по принципу обслуживания в порядке поступления.

Эти четыре метода малосовместимы. После того как вы выберете одну определенную схему, изменить ее будет достаточно сложно. Многие организации избегают использования только одного метода, объединяя несколько методик. Но, как правило, один метод берется за основу, а другой является вторичным. Наиболее распространено использование функционального метода в сочетании с описательным, если офисы компании находятся в разных географических регионах (например, `nyc-marketing` или `sjc-web-03`). Особенно это касается сетевого оборудования, имена которого, как правило, делаются максимально информативными для решения проблем. В таких именах используются аббревиатуры провайдера сети, колокейшн-центра или даже координаты стойки.

Слияние существующих пространств имен

При слиянии организаций решение конфликтов пространств имен может стать не только технической, но и политической проблемой. Многие слияния на самом деле являются поглощениями и слияниями называются лишь затем, чтобы поглощаемую группу не так пугали грядущие изменения. Взаимное одобрение политики разрешения конфликтов пространств имен еще до того, как эти проблемы появятся, поможет предотвра-

тить обиды, особенно если такая политика признана честной обеими сторонами.

Шансы перекрытия имен повышаются, если обе организации используют один и тот же метод назначения имен. Чей сервер с именем `gandalf` придется переименовать? Какой из Сьюзен придется изменить свой логин на `sue` или что-то другое? Куда будут доставляться письма, если отделы продаж обеих компаний используют один псевдоним? По нашему опыту, решением могут стать следующие варианты.

- *Серверы*. Все серверы с одинаковыми именами переименовываются с добавлением псевдонима компании в директории или DNS. Например, если существуют два сервера с именем `gandalf`, их можно переименовать в `gandalf-CompanyaA` и `gandalf-CompanyaB` до тех пор, пока один из этих серверов нельзя будет списать или переименовать другим образом.
- *Логины*. Свой логин сохраняет тот сотрудник, который дольше работал в своей организации. При одном слиянии, в котором помогала Страта, некий менеджер высшего звена уступил свой логин сотруднику из поглощаемой фирмы, хотя менеджер мог воспользоваться своим положением в компании и сделать для себя исключение. Слухи об этом быстро распространились и оказали положительное влияние на всеобщее настроение.
- *Электронная почта*. Проблемы с перекрытием почтовых адресов, созданных по системе «имя.фамилия», могут доставить массу неприятностей. Метод, который кажется нам наиболее подходящим для их решения, заключается в смене адресов обоих сотрудников. Затем почтовые шлюзы настраиваются таким образом, чтобы почта переадресовывалась пользователям на основе домена, которому она была адресована. Письма для susan.jones@companyaA будут переадресованы на адрес susan.a.jones@novaya.companya. А письма для susan.jones@companyaB будут переадресованы на адрес susan.b.jones@novaya.companya. Большинство компаний предпочитают переадресацию почты ее возврату, но ту же стратегию можно использовать для возврата почты с определенным сообщением, например «Адрес Susan.Jones@companyaA сменился на адрес Susan.A.Jones@companyaA. Пожалуйста, обновите эту информацию в своей адресной книге». При внедрении политики маршрутизации почты, например, описанной выше, важно определить временной период (если он будет), по истечении которого особая маршрутизация будет отключена.

Функциональные имена могут упростить конфигурацию программного обеспечения. Службе поддержки будет проще обслуживать программное обеспечение, если почтовый сервер носит имя `pochta`, а календарный сервер – `calendar`. Однако, если такие серверы придется переносить на другие узлы, могут возникнуть сложности. Лучше всего ввести функциональные псевдонимы, указывающие на такие узлы. Такие псевдонимы, как `DNS CNAME`, отлично подходят для неинтерактивных служебных машин, таких как почтовый сервер, веб-сервер, DNS

и т. д. Псевдонимы не так эффективны для интерактивных вычислительных серверов, поскольку пользователи заметят имя узла и начнут его использовать. Может возникнуть путаница, если файлы регистрации генерируются с реальным именем узла, а не с функциональным псевдонимом. Но еще большая путаница может возникнуть при ссылке на псевдоним без возможности определить, какая именно машина подразумевается.

Последовательные имена

Шаблонные имена создают ложное впечатление завершенности. Одна сотрудница в панике подала заявку о неисправности, когда заметила, что узлы `software-build-1`, `-4`, `-5` и `-7` не пингуются. Естественно, дело было в том, что существовали только узлы `-2`, `-3`, `-6` и `-8`. Остальные были убраны и переведены в другие отделы. Такая ситуация может представлять проблему только в том случае, если используется четкая последовательность.

Тематические имена могут быть очень милыми. Иногда даже слишком милыми. В одном подразделении Bell Labs, где работал Том, для принтеров использовали имена, связанные с видами кофе: `latte`, `decaf`, `grande`, `froth`. И хотя этот подход был очень мил, намного меньше нервов уходило на поиск нужного принтера в тех подразделениях, в которых принтерам давали имена по номеру кабинетов, в которых эти принтеры установлены, плюс добавляли букву `c` (сокращение от англ. color – цветной), если принтер был цветным. Некоторые подходы к назначению имен намного логичнее других. Имена в честь кофе раздражали новых сотрудников, а шаблонные имена устраняли необходимость в дополнительных списках, указывающих, где можно найти тот или иной принтер.

Метод, используемый для назначения имен, отражает корпоративную культуру. Если вы хотите установить свободную и непринужденную рабочую атмосферу, `latte` – отличное имя для принтера. Если вы сторонник культуры, в которой работа скучна, неинтересна и ужасно занудна, пусть именем узлов станет `pc` и четырехзначный номер. Разумеется, в этом случае стоит начинать нумерацию с `pc0011`, чтобы пользователи не завидовали везунчикам, которым достались однозначные номера. Кроме того, не забудьте пропустить числа, заканчивающиеся на 00, простые числа, числа с непристойным значением и любые другие «интересные» числа, открытые математиком Рамануджаном.

Имена обладают и аспектом безопасности. Внимание мошенников скорее привлечет имя `sourcecodedb`, чем имя `server05`. Кроме того, мошенники давно уже поняли, что системные администраторы, как правило, нарушают правила назначения имен в своих собственных системах. Цель мошенников – как можно дольше оставаться незамеченными. Поэтому они избегают узлов, за которыми может быть установлено пристальное наблюдение, например настольных машин системных администраторов. Если они обнаружат сеть, в которой все имена узлов составлены по четкому шаблону, за исключением нескольких машин, названных в честь персонажей «Звездного пути», мошенники решат, что последние и есть машины системных администраторов. Мошенники будут стараться избегать этих узлов, чтобы снизить свои шансы быть обнаруженными. В таком случае вполне логично предположить, что узел с именем `picard` принад-

лежит старшему системному администратору, а за машиной `worf` работает сотрудник, отвечающий за безопасность. И хотя мы не рекомендуем никому «усиливать» безопасность, намеренно запутывая имена, лучше всего замаскировать машины с помощью ничем не выделяющихся имен.

RFC 1178 (Libes 1990) содержит отличный совет по поводу выбора имен для узлов сети. Однако нам хотелось бы отметить, что в случае настольных рабочих станций жизнь системного администратора будет намного проще, если имя узлов будет отражать имя пользователя. Если вы получаете письмо от `ajay` с текстом «У меня проблемы с машиной», будет намного удобнее, если вы знаете, что имя этой машины – тоже `ajay`. Разумеется, некоторые сервисы каталогов не позволяют устанавливать имена узлов, аналогичные именам в каталоге пользователя. В таком случае достаточно назначить узлам такие имена, как `ajaypc`.

Сложные для ввода имена

Архитектура одной площадки была построена таким способом, что каждый кластер включал в себя файловый сервер и несколько вычислительных серверов. Пользователи должны были работать на вычислительных серверах и не использовать протокол telnet для обращения к файловому серверу. Чтобы отучить пользователей заходить на файловые серверы, таким серверам были присвоены длинные, сложные имена, а вычислительным серверам – простые. В одном таком кластере машины были названы в честь известных математиков. Файловый сервер получил имя `ramanujan`, а вычислительный сервер – `boole`. Ведь гораздо проще ввести `boole`!

8.1.1.2. Контроль доступа

Политика по контролю доступа к пространству имен должна отвечать на следующие вопросы.

- Какие защита и уровень безопасности требуются данному пространству имен?
- От чего мы пытаемся защитить имена и зачем?
- Нужно ли защищать имена в пространстве или только их атрибуты?
- Кто имеет право добавлять, изменять или удалять целые записи?
- Может ли владелец записи изменять определенные поля своей записи?

От кого необходимо защитить содержимое пространства имен? Это зависит от пространства имен. Доступ к просмотру пространства имен стоит запретить всем, если речь идет о списке паролей. Доступ к некоторым пространствам имен ограничивается узким кругом лиц. Это могут быть пользователи в кластере, все сотрудники, все, за исключением конкурентов, или вообще кто угодно. Кому какая разница, что у Тома идентификатор пользователя 27830?

Ответ зависит от каждого конкретного пространства имен, а также может зависеть от контекста. Например, отдельные логины в UNIX-системе можно спокойно указывать в исходящих письмах, на визитных карточках, в рекламе и т. д. Однако полный список таких идентификаторов не стоит нигде публиковать, так как его могут использовать спамеры для рассылки нежелательных

писем. Разумеется, нельзя раскрывать и пароли, связанные с логинами. Таким образом, в UNIX-системах файл /etc/shadow, в котором хранится пароль, должен быть лучше защищен, чем файл /etc/passwd, где хранятся UID (идентификатор пользователя), полное имя пользователя, домашняя директория и предпочитаемая командная оболочка. С другой стороны, хотя мы и не возражаем против внутренней публикации UID, но не советуем раскрывать их всему свету.

Печать файла /etc/passwd

Один системный администратор настраивал принтер и в качестве тестовых страниц распечатывал файл /etc/passwd. В той компании не существовало инструкций по контролю доступа к пространствам имен, поэтому системный администратор не понимал, что раскрытие содержимого файла /etc/passwd – не самая удачная мысль (он не знал, что мошенники иногда просматривают корпоративный мусор как раз на предмет подобных документов[1]). Ему порекомендовали распечатывать файл /etc/motd или создать собственный файл с тестовой страницей. Более опытный системный администратор имел бы лучшее представление о защите пространств имен и не стал бы делать ничего подобного.

Изменения – совсем другое дело. Пользователи должны иметь возможность менять только определенные параметры, и лишь отдельные сотрудники могут иметь право создавать или удалять учетные записи. С другой стороны, интернет-провайдеры часто позволяют пользователю создать учетную запись при условии, что он предоставит номер своей кредитной карты, и удаление учетной записи также производится пользователем. В университетах часто используется система, по которой профессора могут создавать десятки учетных записей для студентов определенного потока, которым потребуется доступ к тем или иным машинам. Однако никто, кроме системных администраторов, не может создать привилегированную учетную запись или удалить учетную запись другого пользователя. У одного крупного провайдера электронной почты, использующей веб-интерфейс, не предусмотрена процедура удаления учетных записей по запросу. Если учетная запись не используется определенное время, она автоматически удаляется.

Еще один аспект защиты включает в себя политики по контролю изменений и резервному копированию. Контроль изменений описан в главе 17. Здесь же достаточно упомянуть, что важно иметь возможность отменить изменения. Пространства имен, которые хранятся в формате нешифрованного текста, можно включить в систему контроля изменений, например в SubVersion (UNIX) или SourceSafe (Windows) для сетевого управления. Политики по резервному копированию должны особое внимание уделять пространствам имен. Резервное копирование – главный страховой полис.

Каким образом пространство имен защищено от изменений – это другой вопрос. В некоторых случаях пространство имен хранится в текстовом файле и изменения можно предотвратить с помощью соответствующего контроля доступа к файлам. В других случаях изменения вносятся через базу данных, которая

[1] Такая практика получила название «разгребание мусора».

включает собственную систему контроля доступа. Важно помнить, что степень защищенности пространства имен определяется методами, используемыми для его изменения. Метод, используемый для обновления пространства имен, должен быть более защищенным, чем системы, чья безопасность зависит от данного пространства имен. Например, используется ли шифрование для доступа и обновления пространства имен? Проводится ли аутентификация через защищенный механизм? Если для этого требуется только пароль, значит, существует серьезный риск, что кто-то может внести несанкционированные изменения.

8.1.1.3. Долговечность пространства имен

Политика по долговечности пространства имен должна отвечать на следующий вопрос: когда необходимо удалять записи в данном пространстве имен? Срок действия некоторых записей в пространстве имен должен заканчиваться в установленный день или через определенный период бездействия. Можно указать, что учетные записи должны обслуживаться одним из сотрудников, который будет обновлять запрос раз в год. При отсутствии обновления учетные записи должны удаляться. IP-адресов может быть недостаточно, и в слабо контролируемой среде можно завершить срок действия IP-адреса, который был передан пользователю, если система сетевого мониторинга показывает, что этот IP-адрес не использовался в течение определенного количества месяцев.

Долговечность имен, которые были когда-либо присвоены пользователям, дольше, чем вы можете себе представить. Как только имя закрепилось в памяти пользователей, изменить его очень сложно. Вы должны быть к этому готовы. Если адрес электронной почты печатается на визитках, очень сложно будет отозвать все карточки в случае необходимости смены этого адреса. Как только репозиторий документов выложен на файловый сервер `fred`, даже не думайте о том, чтобы переместить его на `barney`.

Грамотные технологии позволяют вам маскировать имена, которые не должны быть взаимосвязаны. Средство автоматического монтирования UNIX можно использовать для того, чтобы пользователи обращались к репозиторию как к `/home/docs` при скрытом имени файлового сервера. Расположение документов не должно быть привязано к имени сервера. Тот факт, что они взаимосвязаны, не должен касаться ваших пользователей. Отличным решением здесь являются псевдонимы, хотя некоторые технологии, такие как NFS, требуют перезагрузки клиентов, чтобы изменения вступили в силу. Никогда не называйте веб-сервер `www`. Дайте ему общее имя, а `www` сделайте псевдонимом. Пользователям сообщите только псевдоним `www`, и тогда вы сможете спокойно переносить функциональность сервера на другой узел. Если вы постоянно используете псевдонимы и другие технологии, должным образом скрывающие имена, вы сможете без проблем переносить функциональность с одного узла на другой.

Машина с именем calendar

В течение многих лет календарный сервер, который использовал Том, находился на узле с именем `calendar`. В момент назначения такое имя казалось очень удачным, так как этот узел был приобретен специально для того, чтобы использоваться в качестве календарного сервера. Но впоследствии он также стал выполнять роль главного сервера печати,

и пользователи приходили в замешательство каждый раз, когда задания печати передавались на узел с именем `calendar`. Имя узла нельзя было изменить, так как к нему была привязана лицензия программного обеспечения. Этой проблемы можно было избежать, если бы узлу изначально присвоили любое другое имя, а `calendar` использовалось бы в качестве псевдонима машины. В идеальном мире Том мог бы присвоить узлу псевдоним `printer`, чтобы клиенты были довольны или хотя бы не приходили каждый раз в замешательство.

8.1.1.4. Вопросы сферы действия

Политика по сфере действия пространства имен должна отвечать на следующий вопрос: где будет применяться данное пространство имен? Степень глобальности или локальности того или иного пространства имен определяется двумя факторами: диаметром (географически, то есть насколько широко оно используется) и плотностью (сколько сервисов его используют).

Диаметр – это число систем, использующих конкретную базу данных пространства имен: один узел, кластер, отдел, вся организация и т. д. И хотя вся ваша организация может пользоваться Microsoft ActiveDirectory, конкретная база данных пространства имен – например, имена пользователей и пароли, – может использоваться только машинами вашего подразделения. У иных подразделений есть другие списки пользователей и паролей для своих машин.

RADIUS (Rigney et al. 1997), протокол аутентификации для модемных пулов, VPN-серверов и других сетевых устройств, можно применять таким образом, чтобы устройства всей глобальной системы имели доступ к одной базе данных имен пользователей и паролей. Люди могут входить в систему под одним и тем же именем пользователя и паролем вне зависимости от того, каким модемным пулом они пользуются, путешествуя по всему миру.

Для сайтов, использующих сетевую информационную службу NIS, которые часто являются UNIX-системами, характерно применение пространства имен диаметром в один кластер UNIX-узлов. Каждый кластер имеет свои базы данных пространства имен.

Плотность пространства имен определяется количеством служб, которые его используют. Например, компания может создать уникальный идентификатор для каждого сотрудника, такой как `tal` или `chogan`, и использовать его для адреса электронной почты человека, логина, идентификатора входа во внутрисетевые службы, имени в модемных пулах, службах VPN и т. д. Даже несмотря на то что эти системы используют различные базы данных и протоколы – ActiveDirectory, NIS, RADIUS и т. д., – идентификатор применяется везде. Фактически, даже несмотря на то что идентификатор в каждой из этих систем может использоваться с разными паролями, они будут определять плотность.

Диаметр пространства имен – очень важный фактор во многих случаях. Если каждый отдел имеет свое пространство имен логинов, какими должны быть учетные записи одного человека в базах данных двух пространств имен? Например, что если в одном отделе `tal` – это Том Лимончелли (Tom Limoncelli), а в другом – Терри Левайн (Terry Levine)? Все может быть хорошо, пока Тому не понадобится войти в систему в отделе Терри. Должен ли Том быть `tal2` толь-

ко в отделе Терри или нужно потребовать, чтобы он изменил имя своей учетной записи везде? Это может создать очень много проблем, особенно если учетная запись в сети Терри нужна Тому лишь на небольшой срок.

Пример: «метки» в Lucent

Может быть полезно иметь единое, глобальное пространство имен и обеспечивать согласование с ним других пространств имен. Компания Lucent дает каждому сотруднику «метку», которая является уникальным идентификатором. Сотрудники могут выбирать метки сами, но по умолчанию метка состоит из первых букв имени и фамилии человека. Данное пространство является глобальным пространством уникальных имен, хотя их уникальность довольно сложно обеспечить, учитывая, что в 2000 году в Lucent было более 160 тыс. сотрудников. Доступ к базе данных меток можно получить как к полю корпоративного онлайн-каталога. Каждый отдел должен создавать имена учетных записей, совпадающие с метками сотрудников. Все службы, поддерживаемые группой руководителя информационного подразделения, – электронная почта, кадры, удаленный доступ и т. д. – используют метки только для моделирования правильного поведения. В результате выигрывают обе стороны. Локальные службы могут применять идентификаторы, соответствующие метке сотрудника, но при желании могут и отказаться от них, но тогда им приходится идти на риск, что нынешние и будущие коллизии могут вызвать дезорганизацию. Преимущества применения меток Lucent над предоставлением пользователям возможности выбирать уникальные идентификаторы очевидны, и поэтому принуждения практически не требуется. При поглощении компаний присоединяемая компания должна разобраться с возможными коллизиями в пространстве имен.

Иногда глобальное плоское пространство имен нежелательно. В некоторых случаях используемая технология обеспечивает иерархическое пространство имен. Например, именам узлов необязательно быть уникальными в масштабе всей корпорации, потому что DNS обеспечивает зоны и подзоны. При наличии зон DNS в подразделениях каждое подразделение может иметь машину `www.` – в идеале псевдоним реального сервера с более уникальным именем. Подразделение может даже называть свои настольные ПК как `pc` и номер, и сайтам не придется координироваться друг с другом, чтобы обеспечить использование непересекающихся номеров.

Пример: широкие и плотные пространства имен в электронной коммерции

Сайты электронной коммерции могут иметь очень широкое и плотное пространство имен пользователя. Пользователь создает и применяет одно имя и пароль для всех служб на сайте, вне зависимости от того, располагаются ли они на одной машине или на сотнях. Подобное характерно для Yahoo. Когда пользователь создает профиль, он применяется

во всех предоставляемых службах. Пользователю может понадобиться активировать дополнительные службы, но они все привязаны к одному имени и паролю, которые человеку нужно помнить.

8.1.1.5. Целостность

Политика целостности пространства имен должна отвечать на следующий вопрос: целостность каких атрибутов должна сохраняться при использовании одного имени в нескольких пространствах имен?

Высокая целостность означает, что имя, применяемое в одном месте, будет иметь те же самые атрибуты во всех других местах, где оно существует. Например, вы можете создать такую политику: если у кого-то есть учетная запись UNIX, цифровой идентификатор пользователя UID должен быть одним и тем же везде, где у человека есть учетные записи.

Пример: простой способ установки стандартов назначения имен

В компании Bell Labs Research много UNIX-систем, или кластеров, но удивительно мало конфликтующих UID. Этот факт был обнаружен, к нашему глубокому удивлению, при слиянии некоторых из этих систем. Как же это случилось?

Много лет назад кто-то пригласил всех системных администраторов из всех вычислительных центров на бизнес-ланч. На этом бизнес-ланче системные администраторы разделили пространство UID, отдав большие диапазоны каждому исследовательскому центру. Все согласились придерживаться рамок выделенных пространств, за исключением создания учетных записей для людей из других вычислительных центров – в этом случае переносились UID из их центра. Не было создано политики, не был назначен ответственный руководитель по распределению, а также не была реализована система санкций. Все согласились соблюдать решения, поскольку знали, что это разумно. Через некоторое время после встречи кто-то отправил электронное письмо с описанием диапазонов.

Спустя годы эти диапазоны UID все еще соблюдаются. При найме новых системных администраторов кто-нибудь дает им копию того электронного письма, объясняя, о чем договорились много лет назад. В каждом центре есть свой скрипт «создания учетной записи» в соответствии с правилами, определенными в том письме. Упомянутое соглашение эффективно работало все эти годы, потому что оно действительно было простейшим решением проблемы.

Единый UID для учетной записи во всех системах

В Bell Labs большинство людей могут входить в систему на всех машинах общего назначения с одним и тем же именем и паролем, используя один

UID. Однако не все могут иметь доступ к машинам особого назначения. Том обнаружил, что одной из таких машин был DNS-сервер. Учетные записи были только у тех, кому нужно было вносить обновления в DNS, и их UID размещались в диапазоне от 1000 и далее. Предыдущий системный администратор оправдывал это решение тем, что для DNS-сервера было необходимо обеспечить такую безопасность, что об NFS даже не приходилось говорить. Поэтому UID не должны быть такими же, как во всех остальных системах, иначе определение обычного UID одной учетной записи занимало бы целых 10 с. За три года эксплуатации машины такое решение позволило сэкономить, пожалуй, одну-две минуты в год. Но в итоге, когда резервные копии данных с этой машины восстанавливались на других узлах, UID оказывались другими. Для предотвращения будущих проблем Том установил такую политику, что все новые учетные записи должны создаваться с использованием UID их домашних систем, а старые UID переназначались во время модернизации, когда разрешался простой.

8.1.1.6. Повторное использование

Политика повторного использования пространства имен должна отвечать на следующий вопрос: через какое время после удаления или прекращения срока действия имя может использоваться повторно? Обычно можно немедленно повторно использовать имя. Например, вы можете сразу повторно использовать имя принтера без необходимости перенастройки компьютера.

Однако с адресом электронной почты следует быть более осторожным. Возможно, ваша политика предполагает, что после удаления адреса электронной почты никто не может пользоваться им в течение 6 месяцев, чтобы снизить вероятность получения новым владельцем электронной почты, адресованной другому лицу. Эта политика предотвращает следующий злонамеренный прием: в некоторых компаниях есть автоматизированная процедура перенаправления почты с именных адресов. Например, вы можете задать перенаправление почты с foosupport@companyname.com вам – человеку, который поддерживает продукт foo. Если ваши служебные обязанности изменятся, почта с этого адреса может быть перенаправлена тому, кто вас сменит. Однако, если Джон До (John Doe) (jdoe@companyname.com) уволится из компании, вы можете воспользоваться этим, чтобы перенаправить себе почту jdoe и получать его письма, пока все его корреспонденты не узнают новый адрес. Будет особенно плохо, если компанию покинет генеральный директор. Устанавливая требование недействительности удаленных адресов электронной почты в течение 6 месяцев, вы будете иметь бóльшую уверенность в том, что повторное применение этого адреса безопасно.

Политика повторного использования может быть реализована программно. Однако в небольших и редко изменяющихся пространствах имен системному администратору просто следует учитывать последствия повторного использования. Например, если вас просят дать компьютеру пользователя имя, которое недавно использовалось для популярного сервера, вы можете предложить другое имя, чтобы предотвратить путаницу. Путаница будет особенно серьезной, если все еще используется большое количество бумажной документации, содержащей имя сервера.

8.1.1.7. Выводы

Политики назначения имен, контроля доступа, долговечности, охвата, целостности и повторного использования должны быть записаны, одобрены управляющим и техническим персоналом и доступны для ознакомления пользователям и системным администраторам, четко устанавливая таким образом правила ваших пространств имен. Так можно избежать многих проблем. Небольшие сайты могут себе позволить работать без такой документации потому, что в данном случае требуется совсем немного системных администраторов, которые работают вместе, и такая политика является частью их культуры. Однако такой неформальный подход становится препятствием расширяемости. Сайты со временем становятся крупнее и вдруг оказываются под управлением большего количества системных администраторов, не посвященных в «стандартные» методы работы. Документирование упомянутых политик может предотвратить многие разногласия. Таким образом, новый системный администратор, несогласный с ними, может обсудить любые предлагаемые изменения. Без документации каждый системный администратор волен полагать, что его способ – правильный (более подробно процедуры документирования рассмотрены в главе 9).

8.1.2. Процедуры изменения пространства имен

Всем пространствам имен требуются процедуры добавления, изменения и удаления их элементов. Эти процедуры должны документироваться так же, как и политики, но документация может быть недоступной пользователям. Опять же, малая группа сможет работать без явного письменного указания этих процедур. Эти действия осуществляются только людьми, создавшими систему, и поэтому не требуют документации. Однако с ростом системы и привлечением новых системных администраторов появляется беспорядок. Документация может выполнять двойную функцию, предоставляя как основу для обучения, так и пошаговую инструкцию при выполнении задачи.

Если что-то можно кратко и понятно задокументировать, то это можно автоматизировать. Как вы увидите в следующем разделе, автоматизация необязательно должна быть сложной.

8.1.3. Централизация управления пространством имен

Управление пространством имен должно быть максимально централизованным, насколько это возможно для любой конкретной среды. С централизацией приходит целостность. Иначе пространства имен становятся разрозненными на различных серверах или даже в различных директориях на одном сервере. Лучше иметь один узел, поддерживающий ваши пространства имен, и распространять их по другим узлам.

> **Пример: очистка пространства имен**
>
> На одном сайте Том обнаружил, что некоторые пространства имен имели контрольные копии на конкретном узле и распространялись по всем узлам UNIX-командой `make`. На паре других узлов хранились контрольные копии других пространств имен. Для этих пространств нужно было

отредактировать файл и затем запустить скрипт, чтобы распространить данные по другим узлам. Фактически это был не один скрипт, а набор скриптов с именами типа `update_printcap`, `aliases_push` и `push_stuff`. Имена этих скриптов были неупорядоченными, потому что система представляла собой совокупность нескольких более мелких систем. Директории, в которых хранились файлы и скрипты, часто были различными для разных узлов.

Свою работу на этом сайте Том начал с изучения того, в какой директории хранилось каждое пространство имен, на какой машине и какой скрипт нужно было запустить для распространения изменений на другие машины. Всю эту информацию Том получил от старшего системного администратора, потому что она не была задокументирована. Профессионализм системного администратора оценивался не по тому, насколько хорошо он знает UNIX, а по тому, как легко он может запомнить список скриптов с неинформативными названиями. К концу недели Том собрал всю эту информацию в большую схему. У Тома была не очень хорошая память, и эта сложная система сильно обеспокоила его.

Ни один из файлов не был записан в системе управления редакциями (RCS – Revision Control System) или системе контроля исходного кода (SCCS – Source Code Control System), поэтому для любого управления изменениями системные администраторы были вынуждены полагаться на резервные копии на магнитных лентах. Системные администраторы не могли отменить какое-либо изменение без значительных усилий. Том тоже мог ошибиться, поэтому его и беспокоило такое положение вещей.

После месяца работы контрольные файлы всех пространств имен были перемещены в единую директорию на одном узле. Эти файлы поддерживались системой управления редакциями (RCS), чтобы изменения можно было отменить. Новая команда `Makefile` в той директории заменила соответствующий старый скрипт, зависимый от того, какой файл изменялся. После этого перехода система стала не только проще в администрировании, но и более целостной. Стало легче обучать новых системных администраторов, которые теперь могли сосредоточиться на более важных технических задачах.

Со стабилизацией новой системы ее стало возможно оптимизировать. Некоторые старые скрипты были неустойчивыми или медленными. С объединением системы основное внимание было уделено замене отдельных скриптов на более эффективные.

Также это объединение упростило введение новых автоматизированных процессов, например для создания новых учетных записей. Вместо того чтобы требовать от системных администраторов запоминать имена скриптов для создания учетной записи, например `make newuser`, стали создавать памятки. Сами скрипты были интегрированы в `Makefile`. Поэтому, вместо того чтобы запоминать, какой скрипт создавал учетную запись, человек просто вводил команду `make account` – и скрипт задавал соответствующие вопросы и завершал задачу.

GNU-приложение cfengine Марка Барждеса (Burgess 1995) – отличное средство под UNIX для поддержки контрольных копий пространств имен и файлов и распространения их по узлам. Преимуществами этого средства являются автоматическое поддержание любой конфигурации узла UNIX и возможность программирования других конфигураций для определенных узлов. Microsoft ActiveDirectory и OpenDirectory в Mac OS X были созданы по другому принципу – клиенты должны отправлять запросы на LDAP-серверы, которые централизованно хранят информацию о пространствах имен.

8.2. Тонкости

Теперь мы можем выйти на новый уровень за счет дальнейшей централизации и автоматизации. Применение пространств имен может стать общим методом ведения дел.

8.2.1. Одна большая база данных

Централизация – хорошая практика, а централизация всех пространств имен в базе данных SQL даже лучше. Вы можете разработать клиент (веб-приложение или приложение с оконным интерфейсом), который позволит операторам вносить большинство изменений. Затем программы могут передавать данные другим системам, например ActiveDirectory, LDAP, NIS, конфигурациям принтера и т. д. Джон Финке (John Finke) из политехнического института Ренсселера написал по этой теме ряд статей (Finke 1994a, 1994b, 1995, 1996, 1997). До недавнего времени многие организации не могли воспользоваться этим решением. Но реализации баз данных SQL с открытым исходным кодом, такие как Postgres и My SQL, существенно снизили финансовые затраты на централизацию баз данных.

8.2.2. Дальнейшая автоматизация

После завершения основ дальнейшая автоматизация упрощается. Если первичная автоматизация была сделана правильно, более высокие ее уровни могут быть интерфейсами первичной автоматизации и обеспечивать, например, дополнительную проверку данных или возможность повторять процесс многократно.

Если вы способны повторно проводить процесс по элементам пространств имен, автоматизация может управляться последними. Например, простая итерация по пространству имен `passwd` может быть основой системы, которая проверяет различные параметры безопасности, например содержимое файла .rhosts. Многие сайты имеют один список рассылки на подразделение, и эти списки рассылок могут автоматически генерироваться из корпоративной директории.

Учетная база данных всех систем может быть одним из ваших наиболее мощных пространств имен, если поддерживается его актуальность, а этот процесс можно частично автоматизировать.

Автоматизированная учетная база данных

Однажды Том работал над сайтом с учетной базой данных, к которой можно было легко отправить запрос из командных скриптов. Также на этом

сайте была программа, которая могла выполнять одну и ту же команду на списке узлов. Их объединение упростило написание программы, которая могла вносить изменения глобально или на узлах с указанными характеристиками, например с определенной операционной системой, версией операционной системы, количеством памяти и т. д. С развертыванием нового приложения запрос мог быстро определить, каким узлам потребуется дополнительная память, чтобы это приложение поддерживать. Отделение процессов поддержки от базы данных узлов было очень эффективным.

8.2.3. Обновление, управляемое пользователем

Автоматизация также может пойти в другом направлении: к большей самостоятельности пользователей. В каждой среде есть много возможностей для автоматизации служб. Периодически просматривайте свои журналы запросов и проведенных работ, обсудите с пользователями, что бы они хотели автоматизировать. В разделе 3.1.3.3 описана система DHCP, которая автоматизирует выдачу IP-адресов.

Пример: создание учетных записей в университете Ратджерса

Во многих компьютерных аудиториях университета Ратджерса требовалось, чтобы для каждого студента создавались учетные записи на машинах кластера информатики и вычислительной техники. Массовое создание учетных записей обеспечивалось за счет автоматизации. Лаборанты имели доступ к команде, которая создавала большое количество учетных записей для группы, запрашивая базу данных по зачислению. Похожая команда удаляла все учетные записи конкретного класса, когда курс завершался. В результате такой автоматизации больше не нужно было привлекать системных администраторов для поддержки этого аспекта пространства имен, что было довольно существенным преимуществом для образовательного учреждения.

8.2.4. Эффективное использование пространств имен

Всеобъемлющие пространства имен могут быть полезны не только в вашей компьютерной инфраструктуре, но и в других инфраструктурах. Существует тенденция по снижению нагрузки по администрированию некомпьютерной инфраструктуры за счет ее привязки к пространствам имен компьютерной инфраструктуры. Например, офисные АТС, а также системы голосовой почты, доступа по смарт-картам и обслуживания кредитных карт в кафе все чаще обращаются к LDAP. Представьте дополнение вашей корпоративной базы данных LDAP, когда при найме новых сотрудников создаются их учетные записи электронной почты, копируются шаблоны внешних домашних страниц, настраиваются телефон, голосовой почтовый ящик и доступ по смарт-карте для обеспечения прохода в нужные части здания.

8.3. Заключение

В этой главе мы установили ряд правил для пространств имен. Во-первых, мы должны осознать, какую роль выполняют пространства имен в системе. Далее, очевидно, что всем пространствам имен присущи определенные качества. Пространствам имен требуются правила для присвоения имен, контроля доступа, долговечности, сферы действия, целостности и повторного использования. После определения правил можно установить процедуры. Правила необходимо сформулировать до установки процедур, потому что первые должны определять последние.

Установление записанных правил и процедур для пространств имен улучшает согласованность в работе команды системных администраторов и дает пользователям представление о том, на что они вправе рассчитывать. Пространства имен могут значительно выиграть от централизованного управления и автоматизации.

Пространства имен являются частью базовой инфраструктуры компьютерной среды. Эффективно управляемые пространства имен являются одной из ключевых систем, которые обеспечивают стабильную работу других систем. Например, вы можете поддерживать систему электронной почты без эффективно управляемого пространства имен, но это будет сложно, утомительно и непонятно пользователям системы.

Для эффективной работы по поддержке пространств имен требуется автоматизация, а хорошие пространства имен могут помочь в дальнейшей автоматизации, если они обеспечивают стандартизированные методы, или API. Перенос всех пространств имен в единую крупную систему баз данных позволяет нам получить максимальное преимущество.

После создания основы появляются новые возможности. Создание всех пространств имен из единой системы баз данных может быть выгодным. Можно обеспечить лучшую автоматизацию, в том числе такую, которая позволит пользователям удовлетворять свои потребности без вмешательства системного администратора. Наконец, мы позитивно отметили тенденцию привязки некомпьютерной инфраструктуры, такой как кадры, офисная АТС и системы доступа по смарт-картам, к централизованным базам данных.

Задания

1. Какие пространства имен есть в вашей системе? Как они поддерживаются?
2. Одним из признаков хорошо развитой системы является наличие базовых признаков в пространствах имен системы, которые были рассмотрены в разделе 8.1. Оцените свою систему.
3. Какая автоматизация применяется для поддержки пространств имен? Какую автоматизацию нужно обеспечить?
4. Какие задачи по поддержке системы можно переложить на пользователей благодаря автоматизации?
5. Предположим, вы перешли в новую организацию и ваш логин уже используется. Что вы будете делать?
6. Кем был Рамануджан и какие числа он посчитал интересными?

Глава 9

Документация

В терминах системного администрирования, документирование означает ведение записей о том, где что находится, объяснение того, что и как выполняется, и обеспечение доступности полезной информации для пользователей. Обычно системные администраторы не любят писать документацию: времени едва хватает на текущие задачи, зачем еще писать документацию? Причина в том, что документация во многом помогает и ее недостаток снижает возможности системных администраторов эффективно работать.

Бывает трудно решить, что нужно документировать. Мы рекомендуем исходить из собственных потребностей: применяйте документацию как средство для облегчения вашей работы. Служба поддержки постоянно завалена одними и теми же вопросами? Создайте документацию, чтобы пользователи могли сами себе помочь. Есть задачи, которые вы не любите? Внесите их в документацию, чтобы было проще передать их решение кому-нибудь, например менее опытному системному администратору. Вам трудно забыть о работе, находясь в отпуске? Вы вообще не можете позволить себе уйти в отпуск? Задокументируйте процессы, которые можете выполнять только вы. Вы целыми днями исправляете ошибки, появление которых можно было бы предотвратить? Создайте инструкции и памятки, чтобы улучшить воспроизводимость.

Документация – это способ создания «памяти» организации, которая позволяет команде системных администраторов повышать свой уровень знаний и навыков. Считайте документацию RAID-массивом для системных администраторов: она обеспечивает избыточность группы. Некоторые системные администраторы боятся, что документация сделает их менее незаменимыми, и поэтому отказываются документировать то, что делают. В результате они обычно оказываются в собственной ловушке, загнанные в угол и неспособные покинуть свое рабочее место. Истина заключается в том, что за счет одновременного хранения и распространения знаний документация позволяет организации развивать своих людей.

В данной главе представлены советы о том, как создавать документацию, как хранить ее и обеспечивать к ней доступ и как управлять все бóльшими и бóльшими хранилищами. Мы обсудим методы упрощения создания документации за счет устранения препятствий, реальных и воображаемых, не позволяющих людям поддерживать документирование.

9.1. Основы

Основы включают некоторые простые способы создания документации, ее хранения, позволяющего легко ее применять, и обеспечения доступа к ней всех, кому она может понадобиться.

9.1.1. Что документировать

Наиболее важные для документирования процессы чаще всего являются либо (1) сложными и неприятными, либо (2) теми, которые вы постоянно объясняете кому-то. Иногда предмет документирования принадлежит обеим категориям, например доступ к корпоративной сети в поездках. Мы используем характеристику «*сложный и неприятный*» по отношению как к самому процессу, так и к последствиям в случае ошибки. Хорошим примером является процесс подготовки рабочего места для нового сотрудника: настройка компьютера, создание нужных учетных записей, в том числе необходимых в конкретном подразделении, уведомление нужных людей и т. д.

Таким образом, если процесс имеет множество этапов, требующих точного порядка выполнения, – особенно если в случае ошибки вам приходится звать на помощь своего руководителя, – имеет смысл задокументировать его как можно скорее. Вы избавите кого-нибудь от множества трудностей, и этим «кем-нибудь» можете быть вы сами.

Документация неприятных процессов

Том считает, что он плохо выполняет работу, которая ему не нравится. Он отвлекается, забывает о некоторых этапах и т. д. Благодаря документации в виде инструкции он с меньшей вероятностью может пропустить этап и сделать ошибку. Также проще поручить кому-то другому завершение процесса после того, как выполнена самая сложная его часть.

Документирование нелюбимых вами задач упрощает поиск других людей для их выполнения. Часто самым сложным элементом является собственно разработка процесса, а затем его выполнение становится проще. При получении разрешения включить еще одного системного администратора в нашу группу нам часто хочется нанять кого-нибудь с такими же навыками, как у нас, чтобы поровну разделить работу. Но может быть трудно найти кого-то, настолько же опытного. Однако, если мы задокументировали задачи, выполнять которые не любим, мы можем нанять для их выполнения менее опытного человека, со временем обучая и продвигая его. Менее опытный сотрудник обходится дешевле и в конце концов становится человеком, знающим, как работает компания и ваше IT-подразделение, и владеющим переданными вами навыками.

Должностные инструкции обычно состоят из двух частей – списков обязанностей и требуемых навыков. Создайте список обязанностей, перечислив процессы, которые вы не любите выполнять и которые были задокументированы. Создайте список требуемых навыков, рассмотрев каждый документ и определив навыки и технологии, с которыми системный администратор должен быть знаком, чтобы понимать документацию. В принципе, все должностные инструкции пишутся сами собой.

9.1.2. Простой шаблон для начала

Самый сложный этап создания документа – это начало. Вот простой принцип: определите четыре основных элемента документа – *название*, *метаданные*, *что*

и *как*. Создайте шаблон или план документа и заполните его разделы с начала до конца.

1. *Название*: простое название, понятное другим.
2. *Метаданные*: контактная информация автора документа – обычно ваша, дата последней редакции или история изменений. Люди, читающие документ, смогут обратиться к автору с вопросами, а когда вы получите повышение, ваши преемники будут помнить вас как человека, давшего им этот документ. Дата последней редакции и история изменений помогут людям понять, является ли документ все еще актуальным.
3. *Что*: предложение, описывающее содержание документа или цель, которой человек должен достичь, следуя указаниям. Достаточно одного-двух предложений.
4. *Как*: шаги, предпринимаемые для выполнения задачи. Для каждого шага, который может быть непонятным или запутанным, вы можете добавить *почему*, например «Перемотать ленту (*Почему?* Потому что мы выявили, что в этом случае при полном резервном копировании ошибки записи случаются реже, даже с новыми лентами»).

Затем тщательно проверьте уровень качества документа. Точность имеет очень важное значение. Опечатка или пропущенный шаг может привести к тому, что человек создаст больше проблем, чем предполагалось решить с помощью документа.

Выполните шаги, указанные в документе, самостоятельно вводя каждую команду. Затем попросите кого-нибудь другого выполнить задачу, используя документ, и предоставить вам отчет, где он встретил какие-то затруднения. Дайте человеку бумажный экземпляр, чтобы он сделал пометки, которые вы потом сможете посмотреть.

Хотя можно сделать это интерактивно, наблюдая и записывая за человеком его замечания, очень легко превратить сеанс в беседу, помогая человеку в процессе и запоминая то, что нужно будет записать потом, когда вы вернетесь за свой стол. Будьте сдержанным: если вы не позволяете человеку сделать работу самому, он не тестирует ваши инструкции. Если ваше присутствие не вызывает у человека недовольства, сядьте вне его поля зрения и наблюдайте, записывая вопросы, вызывающие затруднение.

После успешного использования этой документации несколькими сотрудниками создайте на ее основе более емкое «краткое руководство», обобщающее шаги. Это руководство просто поможет опытным системным администраторам ничего не забыть. У системных администраторов должна быть возможность вырезать и вставлять командные строки из этого документа в консоль, чтобы ускорить процесс.

Пример: два набора документации

Клифф Миллер (Cliff Miller) в компании Bell Labs создал систему поддержки базы программного обеспечения для однородных UNIX-систем. Важным элементом структуры базы было пространство имен, применяемое для различных дистрибутивов, часть которых должна быть видима только на определенных платформах или конкретных узлах. Процесс добав-

ления дистрибутивов в пространство имен был немного сложным. Несмотря на то что он был подробно документирован, инструкция содержала много пояснительных данных. Это было замечательно при первом добавлении дистрибутива, но потом начинало раздражать. Решением стало создание «краткого руководства», содержавшего только необходимые для ввода команды с лаконичными пояснениями о том, что выполняется, и гипертекстовыми ссылками на соответствующий раздел полной документации. Теперь как новые, так и опытные системные администраторы могли легко выполнять процесс, пользуясь документацией в необходимом объеме.

9.1.3. Простые источники для документации

Один из способов упрощения ваших задач по документированию – сделать пометки при следующем выполнении задачи. Даже если это замедлит процесс, это будет проще, чем написание документа по памяти.

9.1.3.1. Сохранение скриншотов

Научитесь пользоваться средством для снятия скриншотов. Когда вы в следующий раз будете делать что-то, что хотите описать в документации, снимайте скриншоты при выполнении каждого шага. Если вы создадите документ из скриншотов, все, что вам останется, – это добавить одну-две строки текста к каждому изображению, описывающие, что выполняется на данном этапе. Таким образом вы получите детализированный и наглядный мультимедийный документ. Такое наглядное пособие великолепно для дополнительной проверки правильности, так как любой, кто воспользуется документом, может на каждом этапе сравнивать скриншот с изображением на мониторе с целью убедиться, что все выглядит так, как предполагалось, прежде чем идти дальше.

9.1.3.2. Сохранение содержимого командной строки

Если вы чаще работаете с командной строкой, чем с графическим интерфейсом, копируйте и вставляйте в документ содержимое окна терминала или консоли. Некоторые программы терминалов или консолей содержат функцию сохранения в файл, UNIX-команда `script` сохраняет в файл весь сеанс.

UNIX-команда `history` возвращает список последних выполненных команд. Эти сохраненные команды при преобразовании в автоматизированный скрипт могут быть начальной точкой документации процесса. Документация является первым шагом к автоматизации: если вы не знаете точно, как вы что-то делаете, вы не сможете это автоматизировать.

Комбинация команд `script` и `history` является мощным средством. Команда `script` сохраняет то, что вводите вы, и то, что выводит компьютер, однако может запутать непонятными символами, если вы пользуетесь различными средствами редактирования командной строки. Команда `history` точно показывает использованные команды и может применяться для проверки того, что они были записаны.

Вне зависимости от того, используете ли вы буфер обмена или автоматически сохраняете результаты, это лучше, чем заново набирать текст, потому что такие способы требуют меньше усилий и отличаются большей точностью.

9.1.3.3. Применение электронной почты

Как часто вы переписываетесь с коллегами по электронной почте относительно той или иной задачи? Это готовый источник подходящей документации, которая может быть собрана при приложении незначительных усилий.

Две основные проблемы в непосредственном применении электронной почты для документации заключаются в том, что электронную почту трудно использовать совместно и что она, скорее всего, окажется плохо организованной. Другие люди не могут получить доступ к вашей электронной почте, а вы, скорее всего, не всегда сможете найти то, что вам нужно. Вряд ли у вас есть хотя бы одно электронное письмо, содержащее все, что вы хотите иметь в документе. Обычно имеется большое сообщение и несколько входящих и исходящих сообщений меньшего размера, в которых что-то решается или обсуждается. Объедините эти отдельные сообщения в один файл и поместите его там, где ваши коллеги смогут его найти.

Если вы уже сохраняете копии всех отправляемых сообщений электронной почты, то вам повезло. У вас есть материал для ряда простых и полезных документов, который ждет, когда вы вырежете и вставите его в шаблон, рассмотренный в разделе 9.1.2.

В своей папке отправленной почты вы можете поискать сообщения, которыми можно воспользоваться, чтобы собрать документ на определенную тему. Пользуйтесь возможностью своего клиента электронной почты сортировать сообщения по сеансам или темам, чтобы найти сообщения, подходящие для преобразования в документацию. Если по какой-то теме было более одного или двух обменов сообщениями, переписка, скорее всего, содержит достаточно информации для преобразования в документ. Даже если ваш клиент электронной почты не поддерживает сеансы, сортируйте сообщения по темам.

9.1.3.4. Изучение системы заявок

Другим хорошим источником потенциальной документации является система заявок на устранение неисправностей или обработки запросов в вашей организации. В некоторых таких системах есть средства создания *базы решений* или *документов решений*, которые могут отправляться при поступлении новых запросов, похожих на уже решенные.

На многих сайтах используются программы с поддержкой *базы решений*, но эта возможность никогда не применяется и даже не включается. После первых нескольких применений пользоваться ею становится проще, поэтому включите ее и начните пользоваться ею прямо сейчас.

Если вы знаете, что при написании документации будете пользоваться своей системой заявок, то можно упростить процесс и сделать информацию в запросах более полезной. Если ваши системные администраторы отмечают, как они решают проблему, в том числе сохраняют команды и результаты и включают их в журнал обработки заявки, это быстро повышает ценность таких журналов для совместно используемой документации.

Вы можете дополнить свою систему заявок пометкой «база знаний» и полем для комментария, где будете отмечать процессы, которые нужно описать в документации. Вам также понадобится метод обобщения таких отмеченных заявок – например, еженедельный отчет по электронной почте. Если вашу систему заявок нельзя легко дополнить таким образом, вы можете создать отдельную очередь запросов для внесения элементов в базу заданий и просто копировать заявки в эту очередь. Первоначальный запрос пользователя может быть закрыт, а копия останется в отдельной очереди, пока у кого-нибудь не появится возможность преобразовать ее в документ. Данные о заявках позволяют системным администраторам быстро создавать формальную документацию. Применение этих методов обычно приводит к написанию большего количества документации и, как результат, меньшему количеству жалоб о ее отсутствии – ситуация беспроигрышная во всех отношениях.

9.1.4. Преимущества контрольных листов

Хорошим способом начать создание документации и вообще более эффективно работать является использование **контрольных листов**, или списков действий, организованных таким образом, что каждая строка или абзац содержит только один шаг. Каждый завершенный этап можно будет отметить значком.

Контрольные листы позволяют вам выполнять сложные задания с уверенностью в том, что вы завершили все этапы. Пропуск шага будет очевиден, если вы отмечаете их по мере завершения. Контрольный лист может применять кто-то менее опытный, чтобы убедиться в том, что каждый элемент процесса был завершен. Хорошим способом создания отчетности является требование к младшему персоналу подшивать контрольные листы или просто передавать их своему руководителю. Для действительно важных процессов, особенно для тех, которые для выполнения могут требовать сотрудничества нескольких человек или подразделений, подписанный контрольный лист может быть хорошим способом документации выполнения всех шагов соответствующими сторонами. Многие системные администраторы пользуются контрольными листами в своей повседневной работе, чтобы отслеживать все шаги в сложных задачах и всех процессах, которые нужно выполнить.

Типичные контрольные листы включают:

- Задачи, которые необходимо выполнить при каждом найме на работу нового сотрудника.
- Задачи, которые необходимо выполнить при каждом увольнении сотрудника.
- Задачи по установке каждой операционной системы, которая используется в организации.
- Процессы по архивации и внешнему хранению данных в соответствии с требованиями юридического отдела.
- Процессы по обеспечению безопасности ОС перед вводом машины в эксплуатацию.

Добавьте контрольные листы к обычной документации, особенно для часто выполняемых задач. После нескольких применений полного документа человеку понадобится только контрольный список.

Автоматизация целых процессов может быть трудной, но автоматизация наиболее подверженных ошибкам шагов из контрольного листа может быть более простой. Если процесс достаточно часто повторяется, в конце концов будет автоматизирована вся последовательность.

9.1.5. Хранение документации

Создание места для хранения документов, или **хранилища документов**, является важным шагом в процессе документирования. Централизованное размещение обеспечивает начальную точку для организации и обновления документов. Обычно у каждого системного администратора есть свои копии документов и личные записи, наличие центрального хранилища облегчает людям поиск последней версии документа.

Создание хранилища документов также является прекрасным способом обнаружения документации, о существовании которой вы не знали. Если существует центральное хранилище, люди будут приносить различные документы, написанные ими. У большинства системных администраторов есть одна или больше директорий со справочными документами, и они с радостью поделятся ими, если появится место, где их можно разместить.

Самым простым методом создания хранилища документов является создание директории с документацией на диске с общим доступом. Начните ее заполнение с файла README, описывающего все правила и политики, которым необходимо следовать при создании документации для включения в данное хранилище. Вам может потребоваться добавить шаблон из раздела 9.1.2. Создайте несколько начальных поддиректорий с названиями нужных тем, например рабочие станции, принтеры или Linux.

По мере создания системными администраторами документов вносите их в соответствующую поддиректорию, создавая ее по необходимости, и используйте информативные имена для файлов с документацией. Человек, который ищет что-то конкретное, может просто вывести список содержимого поддиректории и найти интересующие его объекты. Например, человек, ищущий документ о добавлении принтеров, может вывести список содержимого поддиректории printers или провести во всех поддиректориях поиск с фильтром по имени файла, включающему слово print.

В хранилище документов полезно ввести контроль исходного кода, помогающий при поиске более ранних версий документов, если кто-нибудь внесет изменения, которые окажутся неверными, или файл будет случайно удален. Обычно гораздо проще проверить наличие дубликата в хранилище исходного кода, чем восстанавливать копию с резервного носителя. Продукты с открытым исходным кодом, например SubVersion, обеспечивают легкую организацию простого хранилища.

Веб-сайт может быть отличным хранилищем документов, но поддержка таблицы содержания вручную и другие задачи могут потребовать больше работы, чем вы сэкономите за счет наличия документов. Одно из решений – настроить веб-сервер, чтобы он выводил содержимое директорий. Стандартные программы вывода содержимого директорий многих веб-серверов поддерживают имена файлов только определенной длины, поэтому длинные описательные имена могут быть обрезаны. На других веб-серверах легко управлять длиной имени файла, отображаемой в содержании.

Создание общей директории

Когда Том работал в Mentor Graphics, его группа имела директорию /home/adm/docs на центральном сервере, которая содержала неформальные инструкции по различным темам. Имена файлов были длинными и описательными: how-to-create-accounts.txt или reasons-why-printer-p32-fails.txt. Поиск осуществлялся при помощи средств командной строки UNIX, таких как `ls` и `grep`. Возможности для поддержания порядка были очень примитивными: всем приходилось проверять дату последнего изменения файла с целью убедиться, что информация не устарела. Сейчас вместо этого использовалась бы система контроля версии.

Несмотря на простоту, эта система хорошо выполняла свою задачу. Было легко создавать новые документы, редактировать старые и искать нужную информацию.

9.1.6. Системы wiki

Wiki – веб-средство для публикации и совместной работы, которое произвело революцию в хранилищах документов. Название произошло от *Wikiwiki*, разговорной формы слова «быстрый» (quick) по-гавайски. Первая программа для wiki называлась WikiWikiWeb, она и дала начало общему термину *wiki*.

Wiki – это веб-хранилище документов, которое обеспечивает простое добавление и редактирование документов любому, кто имеет соответствующий доступ. Документы могут содержать обычный текст, текст на языке разметки гипертекста (HTML) или текст с особыми тегами или командами wiki. Часто в wiki имеется встроенная система контроля исходного кода для проверки создаваемых и удаляемых файлов документации и хранения истории изменений. Более продвинутые системы wiki поддерживают аутентификацию пользователя, автоматизированное добавление тегов или обновление (дата, время, пользователь), блокировку файлов для отдельных пользователей, контроль доступа по имени пользователя или группе и различные степени детализации чтения/изменения/публикации директорий или поддиректорий отдельных документов.

Наиболее сильная сторона wiki заключается в том, что кто угодно может редактировать любую страницу. Если что-то неправильно или устарело, то человек, заметивший ошибку, может исправить ее либо оставить замечание, чтобы кто-нибудь проверил и поправил информацию. Документы магическим образом обновляются, тем самым сохраняя свою актуальность. Вы можете спросить, а что мешает кому-то просто удалить произвольный текст и ввести неверные данные. Все изменения отслеживаются по пользователю, поэтому любой нарушитель будет определен. В корпоративной среде такие происшествия будут редкими за счет общественного давления. Если они случаются, страницы могут быть возвращены к предыдущему состоянию при помощи полных историй изменения. Можно защитить страницы, чтобы редактировать их могли только определенные люди, это хорошая мера предосторожности для важных документов.

Команды форматирования wiki очень легко запомнить и гораздо проще применять далеким от техники людям, чем HTML. Поддерживаются многие условные обозначения электронной почты, которыми они уже пользуются, например `*этот текст будет полужирным*` и `_этот текст подчеркнут_`. URL автоматически преобразуют-

ся в гиперссылки. Имена других страниц wiki распознаются и преобразуются в ссылки. Страницы wiki обычно именуются на языке CamelCaps, известном также как WikiWords или StudlyCaps, поэтому программы легко могут их выявить. При применении слова WikiWord, не связанного ни с какой существующей страницей wiki, будет сформирована ссылка с предложением пользователю создать страницу.

Возможность создавать заранее подготовленные страницы для объектов, которые, по вашему мнению, вам скоро понадобятся, очень полезна. Она чрезвычайно полезна, но, пока вы с ней не столкнетесь, вы можете и не подозревать о ее важности. Можно создать таблицу содержания хранилища документов и вносить в нее документы по мере их создания.

Вместе эти функции создают идеальное средство для совместной работы. Оно может быть очень удобным для того, чтобы посмотреть, как быстро документы обретают форму и хранилище начинает выглядеть реальным и полезным. Это побуждает других людей вносить свой вклад и поддерживает динамику.

Использование wiki

Простота, с которой при помощи wiki можно создавать различные формы документации, стала особенно очевидной для Страты во время работы в небольшой начинающей компании в старом заводском здании в Сиэтле. Ряд сотрудников, в том числе Страта, жили за городом, много ездили, обедали в офисе и имели нерегулярный график. Частицы полезной информации начали появляться на внутреннем wiki-сайте без каких-либо требований или указаний, как на досках для презентаций в общем офисе. Различие было в том, что удаленные сотрудники могли участвовать в работе так же легко, как и те, что находились в офисе. При этом круг затронутых тем был широчайшим, начиная от контактных данных небольшой компании, которая использовала то же самое сетевое подключение, до графиков поездок сотрудников и советов, как самостоятельно выбраться из старого, дребезжащего служебного лифта, который иногда застревает между этажами. Там была даже страница с рецептами для рисоварки в офисе. Сайт wiki был элегантной демонстрацией того, как можно использовать преимущества технологии для беспрепятственного развития самоорганизующихся систем.

Помощь в выборе wiki

WikiMatrix (*www.wikimatrix.org*) предоставляет средства для помощи в сравнении и выборе правильного пакета для конкретной ситуации.

9.1.7. Средство поиска

Функционирующей системе документации необходимо средство поиска. Люди часто помещают данные туда, где другим трудно их найти. К счастью, для вебхранилищ существует много встраиваемых поисковых систем. Эти средства варьируются от пакетов с открытым исходным кодом до аппаратных средств, созданных для индексирования данных всей организации. При выборе поиско-

вой системы учитывайте уровень детализации поиска и наличие нужных вам опций поиска, а также то, какие типы документов доступны для полнотекстового индексирования.

Предпочтительно иметь возможность ограничения поиска по определенным областям или объектам. Можно задать поиск только по названиям документов или тексту на страницах, с которыми они связаны ссылками. Другие виды поиска могут работать с содержимым самих документов или ключевыми словами либо тегами, связанными со страницами.

Не все системы поиска поддерживают сложные запросы, например требование присутствия или отсутствия определенных слов, или позволяют запрашивать метаданные о документах. В качестве примера последнего можно привести задание поиска документов, содержащих фразу «лицензия на ПО», созданных до 1 января.

9.1.8. Проблемы внедрения

Важнейшим аспектом при создании нового хранилища документов является обеспечение заинтересованности и участия сообщества, которое будет им пользоваться. Пользователи хранилища являются также и авторами, и если большинство людей не захотят проявлять инициативу, эффективность всего проекта будет сомнительной. Как ни странно, среди противников этого проекта бывает много специалистов «старой закалки». Они привыкли к миру общения по электронной почте и считают, что не стоит тратить свое время на создание общего веб-ресурса. Естественно, в данном случае стоит привести аргументы в пользу создания единой папки входящих сообщений для обзора новых материалов. Одним из способов решения данной проблемы является обеспечение автоматической генерации раздела «Последние изменения» как элемента wiki. Некоторые системы позволяют периодически рассылать эту страницу по списку заинтересованных людей либо настроить ее для предоставления информации в виде RSS-трансляции[1], чтобы ее можно было читать, как блог. Предоставление различных способов доступа к информации упрощает принятие людьми новшества.

Внедрение лучших методов документирования

Сила wiki в ее комфортности: для создания документации требуется так мало усилий, что люди невольно втягиваются в этот процесс. На одном сайте Том, не получив официального одобрения создания wiki-системы, тем не менее установил ее на сервере и стал хранить в ней свою собственную документацию. Когда его спрашивали, где найти ту или иную информацию, он просто давал ссылку на подходящую страницу wiki.

По мере того как люди все лучше и лучше знакомились с wiki, они стали просить научить их работать с ней. Том немного сопротивлялся, а затем «сдался». Чем больше он сопротивлялся, тем сильнее сотрудники хотели научиться работать с этой системой. Вскоре ею стало пользоваться столько человек, что все новые сотрудники воспринимали ее как официально установленное хранилище документации. А затем она стала таковым.

[1] RSS – это семейство форматов веб-трансляций; аббревиатура расшифровывается как Really Simple Syndication, Rich Site Summary или RDF (Resource Description Framework) Site Summary.

9.1.9. Самоуправление или прямое управление

Лучше заранее решить, должен ли менеджер либо администратор библиотеки сайта обеспечивать всю необходимую поддержку хранилища документов или сайт должен быть самоуправляемым. Большинство групп занимают позицию где-то посередине, когда руководитель отдела или менеджер периодически направляет деятельность в нужное русло, изменяя формат разделов или оставляя на страницах комментарии о том, какой он хотел бы видеть работу.

Если можно включить управление сайтом в чьи-нибудь служебные обязанности, то при помощи последовательных улучшений можно будет создать гораздо более полезный сайт. В качестве примера можно привести обзор журналов поиска и журналов ссылок, по которым обращаются пользователи, чтобы определить информацию, которую людям трудно найти, а затем более явно выделить ее на сайте. Другой пример – работа с системой заявок для создания документа, где представлены результаты рассмотрения заявок или журналы решений, которые в дальнейшем могут быть доработаны и внесены в FAQ.

Если учреждена должность менеджера сайта, он должен способствовать самостоятельному развитию системы, а не быть цензором. Менеджер сайта не должен контролировать каждое добавление в хранилище или отменять правки других участников, за исключением случаев явных ошибок или злого умысла. Менеджер сайта нужен для поддержки и развития инфраструктуры сайта, перемещения документов в нужные места и повышения удобства пользования.

9.2. Тонкости

Теперь, рассмотрев основы создания простых документов и хранилищ документов, мы обратимся к созданию хранилищ большего объема, более формальному подходу и управлению содержимым.

9.2.1. Динамическое хранилище документов

Идея сайта «живой документации», или динамического хранилища документов, заключается всего лишь в том, что предполагается периодическое обновление сайта или хранилища для удовлетворения потребностей среды. Интернет-феномен Википедии (*www.Wikipedia.org*) является прекрасным примером такой системы. После появления первой энциклопедии Wiki Encyclopedia десятки групп создали хранилища материалов специализированной тематики по данной модели. В отличие от стандартного хранилища документов, «живое» хранилище документации смещает акцент на взаимодействие пользователя с документами. Пользователь может комментировать, редактировать, собирать документы в обзоры, отправлять ссылки на документы коллегам и т. д., а не просто найти и прочитать документ.

Важно отметить следующее: несмотря на то что мы используем wiki в качестве основного примера сайта «живой документации», это не означает, что в wiki необходимо интегрировать все. Достаточно создать центральную точку организации информации, содержащую ссылки на другие информационные системы.

> **Применение различных wiki для разных ситуаций**
>
> Различные программные пакеты имеют разные преимущества. На одном сайте посчитали, что лучше использовать DocuWiki для пользовательской

справочной документации, Trac – для документов и обработки заявок, связанных с исходным кодом собственной разработки, и RT – для обработки запросов пользователей. На сайте обнаружили, что эти документы довольно редко пересекаются в каких-то аспектах и в этих редких случаях легко скопировать и вставить данные или дать гиперссылку, чтобы их связать.

9.2.2 Система управления содержимым

Система управления содержимым CMS (Content-Management System) – это система публикации для веб-сайтов. Например, система CMS в газете может помогать репортерам в написании статей, которые затем направляются редакторам, корректируются и одобряются на публикацию. Система CMS выпускает статью в определенное время, размещая ее на веб-сайте, обновляя таблицы содержания и разбираясь с другими деталями. На IT-сайте CMS может предоставлять дополнения, расширяющие функции портала, например возможность отображать обзор недавних сбоев.

Для реализации функционирующей CMS требуется ряд элементов. Система управления содержимым состоит из трех уровней: хранилище, история и представление. Уровень хранилища обычно представляет собой базу данных, но также может быть структурированной файловой системой с метаданными. На этом уровне хранится содержимое. Уровень истории реализует контроль версии, разрешения, регистрацию событий и такие функции, как присвоение глобальных идентификаторов новым документам. Уровень истории может быть реализован как отдельный журнал или база данных, а может находиться в хранилище. Уровень представления – это пользовательский интерфейс. Помимо предоставления возможностей по взаимодействию с документом, например обзору или редактированию, уровень представления может также реализовывать функции контроля, такие как доступ только для чтения или установление разрешений.

Продвинутые системы wiki обладают многими элементами полной CMS. Многие системы CMS в настоящее время обладают функциями, подобными имеющимся в wiki. Есть две популярные системы CMS с открытым исходным кодом – Drupal и MediaWiki.

9.2.3. Культура отношения

Сайт «живой документации» требует культуры отношения, иначе люди будут сомневаться, стоит ли им что-то писать, или сочтут, что они могут писать только «одобренные» материалы. Такие компромиссы изначально присущи так называемой модерируемой публикации. Не стоит позволять всем и каждому редактировать инструкции по проверке резервного генератора, но ведь даже компетентный автор может, например, что-то упустить или исказить в первоначальной публикации. В большинстве случаев эту проблему можно решить, предоставляя возможность оставлять комментарии к странице и преобразовывать комментарии в содержимое, когда сам автор или достаточное число других комментаторов посчитают их справедливыми. Если случайно будет сделана ошибка, контроль версий может предоставить доступ к неизмененной версии. Когда непонятно, какая версия является правильной, контроль версий, по

крайней мере, может показать список изменений и предоставить какой-то контекст, помогающий принять окончательное решение или сформулировать запрос разъяснений по телефону или электронной почте.

Будьте готовы к тому, что вам придется потратить некоторое время на управление системой wiki, пока люди не освоятся с ней и не поднимутся до уровня вашей культуры. Определите, какая степень детализации будет «правильной» для вашей группы, и, как это бывает с любыми документами, прежде чем все станет выглядеть так, как вы считаете нужным, будут иметь место какие-то разногласия между обеими сторонами. В некоторых группах есть системы документации, которые представляют собой просто скопированные электронные письма без особого упорядочивания по темам, в других группах есть страницы с продуманными инструкциями для каждого важного элемента инфраструктуры. Преимущество использования wiki или похожей системы «живой документации» в качестве временной CMS состоит в том, что по мере накопления документов вы можете перейти от стихийной системы к более формализованной. С течением времени страницы и записи могут быть реорганизованы и очищены и, возможно, переведены в новые разделы или экспортированы в более формальную CMS.

9.2.4. Классификация и структурирование

Системы wiki обычно слабо структурированы. Некоторые просто предоставляют возможность навигации.

Не тратьте много времени на структурирование на начальном этапе. Основным врагом wiki-проектов является введение слишком жесткого структурирования на ранних стадиях. Wiki так широко распространились именно благодаря *принципу низкого уровня ограничений при внесении записей*. Обновление страницы должно быть таким же легким, как отправка электронного письма, иначе люди просто не будут пользоваться этой функцией. Гораздо лучше заниматься доведением некоторых страниц до нужной степени удобочитаемости, чем оставить эту информацию в папках чьей-нибудь почты, где никто не сможет ее найти, когда хозяин в отпуске. Если какой-то тип документа будет многократно создаваться многими людьми – например, предложения по проектированию или запросы на функции, – создайте шаблон, чтобы эти официальные документы изначально записывались в одном формате.

Различайте написание документации и организацию документации. С ростом объемов ваших материалов люди все чаще будут пользоваться поиском, а не категориями, чтобы найти интересующие их данные. Вы всегда можете создать структурированные категории и реорганизовать страницы или ссылки на них с ростом wiki.

9.2.5. Дополнительное применение документации

Приведем еще несколько способов применения системы «живой документации». Во многих системах wiki есть шаблоны или дополнения специально для этих приложений.

9.2.5.1. Служба самостоятельной помощи

Пользователи могут применять раздел службы самостоятельной помощи сайта документации для прямого взаимодействия с сайтом. Возможно, сейчас на ва-

шем сайте есть ссылка Создать новую заявку, которая позволяет пользователям сделать запрос через систему заявок.

Этот раздел – подходящее место для таких объектов, как новости о запланированных отключениях, обновлениях по текущим процессам и явные ссылки на политики и документы How-To[1]. В качестве примера последних можно привести «Как войти в систему удаленно через VPN», «Как настроить синхронизацию с мобильным устройством» и т. д.

Еще одна функция в разделе службы самостоятельной помощи – это доступ пользователей к обзору результатов, например графиков загрузки нескольких маршрутизаторов (Multirouter Traffic Graphics – MRTG), или даже вызываемые скриптом данные о свободном месте на общих дисках. Сайты, которые очень заботятся о лицензиях на совместно используемое программное обеспечение, могут убедиться, что размещение ссылки на средство проверки лицензии на этой странице очень полезно, чтобы избежать вопросов о том, какие лицензии у кого проверены.

9.2.5.2. Внутренние документы группы

Системные администраторы принимают новшества раньше других, и многие группы системных администраторов создали сайт «живой документации» для собственного удобства. Наличие информации о том, как выполнять сложные задачи, с которыми хорошо знакомы лишь один-два человека в группе, может сэкономить день, когда кто-то заболел или не на месте. Создание собственных документов группы является началом формирования «памяти» подразделения, которая является очень важным элементом преемственности в любой группе.

Любая группа или подразделение может получить пользу от создания собственного раздела на сайте, хотя группа системных администраторов может быть первопроходцем. Фактически в некоторых группах есть сайты «живой документации» в форме хранилища исходного кода, в котором помимо кода можно собирать спецификации, списки пользователей, материалы по маркетингу. Поскольку внутренняя документация группы требует бережного отношения, доступ в этот раздел должен быть органичен, чтобы им обладала только эта группа и руководящий персонал.

9.2.5.3. Документы How-To

На многих сайтах имеются короткие пояснительные документы, называемые How-To или HOWTO, которые дают возможность пользователям помочь себе самостоятельно, когда обратиться к системному администратору невозможно. В каждом документе HOWTO рассматривается одна тема, обычно выполнение конкретной задачи, адаптированное под среду сайта. В них обычно включают как вводимые пользователем команды, как и ответы программ, часто со скриншотами. Документ HOWTO создан, скорее, для решения конкретной проблемы, чем для использования в качестве учебного пособия как такового. Информация изложена в очень доступной форме, чтобы привлечь внимание пользователей, которые иначе посчитали бы чтение документации слишком утомительным и позвонили бы вместо этого в службу поддержки.

---

[1] How-To – термин, означающий нечто, передаваемое путем непосредственного практического обучения. – *Примеч. науч. ред.*

Типичными примерами HOWTO являются настройка клиента электронной почты, получение удаленного доступа к сетям или серверами, доступ к принтерам и настройка программ для применения в локальной среде. Сайты университетов, на которых обычно имеется много клиентов системных администраторов, особенно выигрывают от службы самостоятельной помощи и документов How-To. Сайты, документирующие применение службы поддержки и уровни поддержки в своих организациях, могут использовать для мониторинга и отчетности журналы доступа к HOWTO на веб-серверах.

9.2.5.4. Часто задаваемые вопросы

Часто задаваемые вопросы (FAQ – Frequently Asked Question) являются средством, знакомым большинству пользователей Интернета. FAQ – это просто список наиболее распространенных вопросов по конкретной теме, часто организованный в виде разделов и подразделов и обычно развивающийся со временем. Некоторые дополнения для wiki автоматически создают таблицу содержания, выводя список вопросов в виде гиперссылок, ведущих к ответам (такой подход имеет тот недостаток, что затрудняются чтение всех вопросов и ответов по порядку, поиск по списку или его распечатка).

Список FAQ и набор документов HOWTO различаются, главным образом, длиной и форматом. HOWTO – это разбор одной темы, а FAQ – набор вопросов и ответов. Часто ответ может указывать на документ HOWTO или несколько документов на выбор, отвечающих запросу пользователя.

Если на вашем сайте еще нет списка FAQ, хороший способ его создать – ознакомиться с данными системы запросов и посмотреть, какие вопросы поднимаются чаще других. Типы вопросов будут сильно различаться в зависимости от типа вашей организации и степени поддержки пользователей. FAQ небольшой начинающей технической компании может включать, например, вопрос «Где можно загрузить драйверы для видеокарт в системах наших лабораторий разработки?». FAQ в некоммерческих организациях может включать вопросы типа «Где наши добровольцы могут открыть бесплатные блоги или создать сайты сообщества?».

9.2.5.5. Справочные списки

Справочные списки – это списки объектов, которые не используются часто, но служат для конкретной цели. Например, список корпоративных сокращений не является чем-то, требуемым ежедневно, но если вы увидите какое-то сокращение впервые, то сможете посмотреть его в списке.

Вот несколько примеров подобных списков:

- Поставщики и их контактная информация.
- Серийные и инвентарные номера аппаратных средств.
- Лицензионные ключи и количество пользователей для программ.
- Списки совместимости: какие оптические мыши совместимы с какими аппаратными средствами, какие драйверы работают с какими контроллерами.
- Каталог сотрудников: ручной или автоматически создаваемый из корпоративной базы данных.
- Корпоративные сокращения.
- Список местных ресторанов, служб такси и т. д.: одна страница на офис.

- Для каждого удаленного офиса – список советов для командированных: предложения по аэропортам, рекомендации по отелям, работает ли обычный доступ по личным картам и т. д.
- Кого уведомлять о сбоях, предложениях и комментариях о различных продуктах и/или проблемах.

9.2.5.6. Процедуры

Многие организации должны соответствовать международным стандартам ISO (International Organisation for Standardization), нормам техники безопасности и гигиены труда OSHA (Occupational Safety and Health Administration)[1] или положениям закона Сарбейнса–Оксли[2] об управлении. Такие сайты выигрывают от наличия простого способа создания, поддержки и доступа к процедурам, контрольным спискам и скриптам, относящимся к актуальным методикам. Создайте журнал регистрации процедур и записывайте соблюдение процедур.

Документировать процедуры и вести журналы регистрации полезно даже в том случае, если вы не обязаны это делать. Когда нужно отключить генератор после восстановления подачи энергии, описание процедуры, позволяющей правильно это сделать, будет более полезным, чем схема, показывающая все электрические соединения в вычислительном центре.

9.2.5.7. Техническая библиотека или информационный сборник

Документы, полученные от продавцов, поставщиков и клиентов, статьи, которые вы купили или загрузили из других источников, и, возможно, даже руководство по ремонту кухонной раковины – этот раздел хранилища может быть сложным для систематизации. На некоторых сайтах просто создаются списки содержимого в алфавитном порядке, на других назначается библиотекарь, который выполняет подробную классификацию документов. Если классификация будет слишком объемной, это затруднит, а не облегчит поиск документов (в каком разделе искать инструкции по обжатию коннектора для консоли Cisco – «Документы поставщиков», «Кабельные системы» или «Сети»? Документ может быть во всех этих разделах, но кто-то должен поддерживать обновление ссылок).

9.2.6. Ссылки на внешние источники

Интернет содержит огромное количество полезной информации по технической и деловой тематике, от полезных записей в блогах о Linux Documentation Project до совместных сетевых энциклопедий, таких как Википедия. Большую часть этих данных нельзя воспроизвести на вашем сайте из-за авторских прав или

---

[1] В России – нормативам СанПиН и требованиям техники безопасности. – *Примеч. науч. ред.*

[2] Положения закона Сарбейнса–Оксли направлены на обеспечение прозрачности деятельности американских компаний. В соответствии с этим законом компании обязаны внедрять современные формы документооборота, перестраивать системы управления, что в итоге позволяет руководству этих компаний предупреждать риски и преодолевать трудности и в целом повышает эффективность и конкурентоспособность компании. – *Примеч. науч. ред.*

практических соображений, например ограниченности дискового пространства или необходимости своевременного обновления. Однако ссылки на эти данные могут быть очень полезны для ваших пользователей. В качестве примера объектов, на которые разрешается в явном виде дать ссылки с вашего сайта, можно назвать обучающие и HOWTO-статьи по применению инструментов или программ, форумы поддержки разработчиков для коммерческих продуктов или с открытым исходным кодом, используемых в вашей организации, и сетевые публикации, связанные с интересной технической тематикой.

Важно, чтобы для таких ссылок применялась **служба перенаправления с сохранением анонимности**. Большинство броузеров, когда запрашивают страницу, включают в запрос ссылку на страницу, которая направила броузер на запрашиваемую страницу. Это позволяет сайтам отслеживать, кто дает на них ссылки и какие из этих ссылок наиболее удачны. Однако имеется проблема безопасности: если направившая страница находится на внутреннем веб-сайте, то сайт, на который была ссылка, узнает о существовании этого внутреннего сайта. Сайт, на который была дана ссылка, может узнать имя вашего внутреннего веб-сервера, что не должно стать проблемой, если только ваша безопасность не основана на простом сокрытии имен узлов. Однако полный URL может раскрыть секретные условные названия проектов и другую информацию[1]. Например, сайт, который видит ссылки с такого URL, может обнаружить, что вы готовите большой сюрприз в мае. Всего лишь несколько звонков репортерам – и газеты вдруг начинают писать, что в вашей компании есть проект под названием quickfox, а большой сюрприз испорчен. Решение этой проблемы состоит в обеспечении перенаправления хранилищем документов внешних ссылок через службу, которая удаляет заголовки источников ссылок.

9.3. Заключение

Документация предоставляет пользователям нужную информацию, поэтому они реже беспокоят системных администраторов, что приводит к экономии времени последних. Документация позволяет системным администраторам повторять процессы без ошибок и упрощать их, чтобы было легче передавать поддержку процессов другим людям.

Документацию проще создать, применяя шаблон, с которым вы можете использовать скриншоты, сохраненные сеансы работы с терминалом, архивы электронной почты и системы заявок для помощи в создании содержимого документов. Контрольные листы являются хорошим способом документации многошаговых процедур, что поможет вам повторять их в одной и той же последовательности, документировать требования других групп к вам или обеспечить младшим системным администраторам способ отметить выполненные задания и передать этот отчет руководителю.

Процесс документирования является сложным. Однако, как только вы проделаете тяжелую работу по созданию процесса, документацией смогут воспользоваться менее информированные люди. Таким образом, выполнение процесса станет проще поручить кому-то другому. Наличие документации по процедурам упрощает составление должностных инструкций при найме новых сотрудников.

---

[1] Например, *http://secret.example.com/project/quickfox/competitors-to-destroy-may27.html*.

Документы должны находится в хранилище, чтобы их можно было поддерживать и использовать совместно. Очень удобной системой для создания хранилищ являются wiki, потому что они упрощают создание и обновление документов и не требуют знания HTML. При помощи дополнений wiki могут предоставлять дополнительные службы.

Людей может быть трудно привлечь к использованию хранилища документации. Предоставление помощи, обучения и шаблонов снижает этот барьер.

Хранилища могут быть удобны не только для процедур. Они могут стать службами самостоятельной помощи и содержать документы HOWTO, списки FAQ, справочную документацию и инвентарные списки.

Группы системных администраторов с напряженным графиком работы всегда приветствуют документирование процессов и распространение информации. Хорошее хранилище может способствовать этому. Документация экономит время вам и всем остальным, а также позволяет использовать знания всех сотрудников для улучшения системы.

Задания

1. Какие темы чаще всего появляются в запросах пользователей на вашем сайте? Какую их долю можно обработать при помощи службы самостоятельной помощи с несколькими документами HOWTO?
2. Опишите, как вы делитесь информацией с другими членами группы. Что работает лучше всего? Что бы вы изменили?
3. Какие документы в вашей организации больше всего выиграют от наличия шаблона? Создайте шаблон.
4. Какие объекты войдут в шаблон документации в вашей организации? Есть ли среди них необычные или характерные только для вашей группы?
5. Как бы вы оценили простоту использования общей системы документации по десятибалльной шкале? Почему? Как бы вы оценили контроль доступа?
6. Если на вашем сайте или в вашей группе нет хранилища документов, спросите у трех человек, почему они не хотят его использовать. Если на вашем сайте или в вашей группе есть хранилище, но используется мало, спросите у трех человек, что могло бы упростить его использование. Как бы вы решили эти проблемы?
7. Какие из рассмотренных в данной главе решений по созданию общих систем документации лучше всего соответствуют вашим ответам на два предыдущих вопроса?

Глава 10

Аварийное восстановление и целостность данных

План аварийного восстановления рассматривает, какие нештатные ситуации могут затронуть компанию, и предоставляет план реакции на эти ситуации. Планирование аварийного восстановления включает реализацию способов смягчения последствий возможных нештатных ситуаций и подготовку быстрого восстановления основных служб. План определяет эти ключевые службы и указывает, как быстро они должны быть восстановлены.

Определенный уровень планирования аварийного восстановления должен быть на всех сайтах. Проектировщики аварийного восстановления должны рассмотреть, что будет, если с одним из сайтов их организации случится что-то катастрофическое, и как они смогут обеспечить восстановление. Мы уделяем основное внимание аспектам аварийного восстановления, касающимся электронных данных. Однако эта часть плана должна строиться как элемент большой программы, чтобы соблюдать правовые и финансовые обязательства компании. Планированию аварийного восстановления посвящено несколько книг, которые мы рекомендуем для прочтения: Fulmer 2000, Levitt 1997 и Schreider 1998.

При создании плана аварийного восстановления должны приниматься во внимание как риски, с которыми сталкивается ваш сайт, так и правовые и долговые обязательства вашей компании. С этого вы можете начинать свои приготовления. В данной главе рассмотрено, что должно быть включено в план для вашего сайта.

10.1. Основы

Как и любой другой проект, создание плана аварийного восстановления начинается с определения требований: какие нештатные ситуации могут затронуть ваш сайт, какова их вероятность, стоимость для вашей компании и как быстро нужно восстановить различные части вашего бизнеса. Как только вы и ваше руководство поймете, что может случиться, вы сможете получить средства на проект и начать поиск способов выполнения или, что предпочтительнее, перевыполнения этих требований.

10.1.1. Определение нештатной ситуации

Нештатная ситуация – это катастрофическое событие, которое вызывает сильный сбой, влияющий на все здание или сайт. Нештатная ситуация может быть

любой: от стихийного бедствия, например землетрясения, до более распространенной проблемы случайного повреждения ваших кабелей экскаватором. Нештатная ситуация – это все, что может значительно повлиять на возможность вашей компании вести бизнес.

Недостаток планирования может вызвать большие риски

У одного производителя компьютерного оборудования было предприятие на западе Ирландии. В здании начался пожар, и персонал знал, что система пожаротушения была неэффективной, а здание будет очень сильно повреждено. Несколько сотрудников пошли в вычислительный центр и начали выбрасывать аппаратуру из окна, потому что у нее было больше шансов сохранить работоспособность после падения, чем при пожаре. Затем другие сотрудники переносили аппаратуру в соседнее здание. Люди ушли из горящего здания, когда решили, что пожар стал слишком опасен.

Вся аппаратура, выброшенная из окна, действительно сохранила работоспособность, и предприятие снова заработало в рекордные сроки. Однако недостаток планирования аварийного восстановления и подходящих систем защиты привел к тому, что сотрудники рисковали своей жизнью. К счастью, во время этого происшествия никто не получил серьезных повреждений. Но действия сотрудников противоречили правилам противопожарной безопасности и были очень рискованными, потому что никто из них не имел соответствующей квалификации, чтобы определить, когда пожар стал слишком опасным.

10.1.2. Анализ рисков

Первый шаг в построении плана аварийного восстановления – проведение анализа рисков. Управление рисками является подходящей областью для привлечения сторонних консультантов, потому что их специализированные навыки требуются лишь время от времени, а не каждый день. Крупная компания может нанимать сторонних специалистов, имея штатного сотрудника, ответственного за управление рисками.

Анализ рисков включает определение того, с какими нештатными ситуациями может столкнуться компания и какова вероятность их возникновения. Аналитик определяет возможные издержки компании в случае возникновения каждого типа нештатной ситуации. Затем компания использует эту информацию, чтобы определить приблизительную сумму денег, которую можно потратить на попытку смягчить последствия каждого типа нештатной ситуации.

Приблизительный бюджет предупреждения риска определяется по формуле:

$$\left(\begin{array}{l}\text{возможные издержки}\\ \text{в случае нештатной}\\ \text{ситуации}\end{array} - \begin{array}{l}\text{возможные издержки}\\ \text{после предупреждения}\\ \text{последствий}\end{array}\right) \times \begin{array}{l}\text{вероятность}\\ \text{нештатной}\\ \text{ситуации}\end{array}$$

Например, если есть один шанс из миллиона, что здания компании пострадают от наводнения, и если наводнение обойдется компании в 10 млн долларов, бюд-

жет на предупреждение последствий наводнения должен будет находиться в пределах 10 долларов. Иными словами, не стоит даже запасаться мешками с песком, готовясь к наводнению. С другой стороны, если у компании есть один шанс из 3000 оказаться в радиусе 10 миль от эпицентра землетрясения силой в 5 баллов по шкале Рихтера, которое вызовет убытки в 60 млн долларов, бюджет снижения или предотвращения этого ущерба должен быть в пределах 20 тыс. долларов.

В качестве более простого и менее масштабного примера можно привести большой сайт, который имеет одну потенциальную точку сбоя, где все локальные сети связываются одним маршрутизатором. Если он откажет, то для его ремонта потребуется один день, и есть 70-процентный шанс, что сбой случится один раз в 24 месяца. Авария приведет к невозможности работы 1000 человек в течение суток. Компания оценивает потерю производительности в 68 тыс. долларов. При выборе резервного маршрутизатора системные администраторы будут располагать бюджетом, равным приблизительно 23,8 тыс. долларов. Также системным администраторам нужно определить стоимость снижения времени неработоспособности до 4 ч – например, за счет повышения уровня контракта на обслуживания. Если цена будет разумной, это еще сильнее снизит объемы возможных убытков компании, а следовательно, и сумму, которую она должна будет потратить на полное восстановление.

Такой взгляд на процесс является в определенной мере упрощенным. Каждая нештатная ситуация может произойти в различном масштабе с разной вероятностью и широким диапазоном факторов, влияющих на издержки. Предотвращение ущерба для одного уровня конкретной нештатной ситуации, скорее всего, снизит уровень ущерба, полученного на более высоком уровне той же нештатной ситуации. Все эти сложности учитываются профессиональным аналитиком рисков, когда он рекомендует бюджет для подготовленности к различным типам нештатных ситуаций.

10.1.3. Правовые обязательства

Помимо собственно издержек компании, в качестве элементов процесса планирования аварийного восстановления нужно учитывать дополнительные факторы. У коммерческих организаций есть правовые обязательства перед поставщиками, клиентами и акционерами, касающиеся выполнения контрактных обязательств. Открытые акционерные общества должны соблюдать нормы фондовых рынков, на которых ведется торговля их акциями. Университеты имеют контрактные обязательства перед своими студентами. Кроме того, необходимо соблюдать строительные нормы и правила, а также правила техники безопасности.

Юридический отдел должен уметь детально разъяснить эти обязательства. Обычно они имеют вид «Компания должна иметь возможность возобновить доставку продукта в течение недели» или «В таких обстоятельствах компания может задержать подачу квартальной отчетности не более чем на 3 дня». Эти обязательства переводятся в требования для плана аварийного восстановления. Они определяют, как быстро должна быть восстановлена работоспособность различных элементов физической и электронной инфраструктуры. Восстановление работоспособности отдельных составных частей компании до полного восстановления всей инфраструктуры требует глубокого понимания того, на какие элементы инфраструктуры полагаются эти части, и подробного плана их

возвращения в рабочее состояние. Соблюдение временных рамок также требует понимания того, какое время займет восстановление этих компонентов. Мы рассмотрим это далее в разделе 10.1.5.

10.1.4. Ограничение ущерба

Ограничение ущерба касается снижения издержек в результате нештатных ситуаций. Некоторое ограничение ущерба может быть достигнуто бесплатно или с небольшими затратами за счет планирования и хорошей организации процессов. Бóльшая часть ограничения ущерба предполагает дополнительные затраты компании и является предметом анализа прибыли и издержек, который проводится аналитиком риска.

Существуют способы снизить риск нанесения большого ущерба в случае нештатной ситуации или ограничить этот ущерб бесплатно либо с небольшими затратами. Например, если местность подвержена небольшому затоплению, размещение основных структур на некоторой высоте может незначительно увеличить расходы на строительство и перемещение, но позволит избежать проблем в будущем. Выбор оборудования, устанавливаемого в стойках, и применение для его установки достаточно прочных стоек вместо размещения аппаратуры на полках может значительно снизить влияние небольшого землетрясения бесплатно или с небольшими дополнительными затратами. Применение громоотводов при строительстве зданий в местности, где часто бывает гроза, также является недорогим способом ограничения ущерба. Эти шаги особенно экономичны, потому что они решают проблему один раз и не требуют постоянных расходов.

Ограничение ущерба, вызванного серьезной аварией, дороже и всегда должно быть предметом анализа прибыли и издержек. Например, вычислительный центр может быть построен в подземном бункере, аналогичном военному, для защиты от торнадо и бомбардировок. На сейсмоопасных территориях применяют дорогие механизмы, обеспечивающие взаимное перемещение элементов стойки, чтобы снизить риск повреждения панелей компьютеров, что является основной проблемой жестко закрепленных стоек при сильных землетрясениях. Эти механизмы ограничения ущерба настолько дороги, что, скорее всего, их применение может быть оправданным только в крупнейших компаниях.

Большинство механизмов ограничения ущерба находятся где-то между «совершенно бесплатными» и «очень дорогими». Системы пожаротушения обычно относятся к последней категории. Разумно рассмотреть возможность применения системы пожаротушения, спроектированной для ограничения ущерба оборудованию вычислительного центра при активации. Местные законы и требования техники безопасности ограничивают возможности в этой области, но на момент написания книги наиболее популярными были системы на основе инертных газов и выборочные, с ограниченным радиусом действия, системы на основе воды с механизмами раннего предупреждения, которые позволяют оператору обнаружить и решить проблему, например, при возгорании диска или источника питания, прежде чем активировать систему пожаротушения. Системы, отслеживающие влажность под фальшполами вычислительных центров или в редко посещаемых помещениях с источниками бесперебойного питания либо генераторами, также являются средствами ограничения ущерба средней стоимости.

Еще одна область, часто заслуживающая внимания, – это отключение питания в здании или комплексе зданий. С короткими перебоями в подаче электроэнергии, скачками или падением напряжения можно справиться при помощи источника бесперебойного питания, для более долгих перерывов потребуется генератор. Чем больше аппаратуры требует защищенного питания – рефрижераторы в биотехнологических компаниях, центры обработки вызовов в компаниях по работе с клиентами – и чем дольше потребуется поддерживать их работу, тем дороже это будет стоить. Создание вычислительных центров с аварийной защитой рассмотрено в главе 6, особенно в разделе 6.1.1, где обсуждается выбор правильного размещения, и в разделе 6.1.4, где объясняются вопросы, связанные с электропитанием.

10.1.5. Подготовка

Даже при наличии достаточных мер по контролю ущерба ваша компания может столкнуться с нештатной ситуацией. Часть вашего планирования аварийного восстановления должна представлять собой подготовку к этой возможности. Подготовленность к нештатной ситуации означает возможность восстановить работоспособность основных систем в сжатые сроки, определенные вашими правовыми обязательствами.

Восстановление служб после аварии может потребовать перестройки необходимых данных и служб на новом оборудовании, если старое оборудование неработоспособно. Таким образом, вам нужно заранее определить источник замены оборудования из компаний, которые предоставляют эту услугу. Вам также потребуется наличие другого помещения, куда можно будет переместить это оборудование, если основное помещение нельзя использовать по соображениям безопасности, из-за недостатка электроэнергии или плохой связи. Убедитесь, что компания, предоставляющая рабочее оборудование, знает, куда его нужно отправлять в случае аварии. Убедитесь, что у вас есть временные обязательства по замене от поставщика и что вы знаете, какое оборудование компания сможет поставить по первому требованию. Не забудьте учесть время замены этого оборудования при подсчете общих затрат времени на процесс. Если нештатная ситуация достаточно серьезна и требует обращения к услугам компании, вполне возможно, что у нее будут другие клиенты, которые также пострадают. Узнайте, как компания планирует справиться с ситуацией, при которой как вы, так и ваш сосед будете иметь право на единственный крупный сервер Sun, который был зарезервирован.

Как только у вас будут машины, вам потребуется восстановить систему. Обычно сначала вы реконструируете систему, а затем восстанавливаете данные. Это требует наличия резервных копий данных вне сайта – обычно в коммерческой службе хранения. Вам также потребуется возможность легко определить, какие кассеты потребуются для восстановления основных служб. Этот этап базовой подготовки строится на инфраструктуре, которая уже должна быть на вашем сайте. Следующий этап подготовки к нештатной ситуации – попробовать получить кассеты у сторонней компании, которая занимается хранением, в общем порядке и посмотреть, сколько это займет времени. Это время вычитается из общего количества времени, которое отведено на полное восстановление работоспособности важнейших систем. Если получение кассет занимает слишком много времени, полное восстановление в приемлемые сроки может быть невоз-

можным. Более подробно эти вопросы рассмотрены в главе 26, особенно в разделе 26.2.2.

Обычно сайту требуется безопасное сохранение важных документов в хранилище. Такие хранилища специализируются на сценариях аварийного восстановления. Если в вашей компании есть такое хранилище, вы можете применять его для хранения кассет с резервными копиями данных.

Помните, что в качестве элемента восстановления служб вам могут понадобиться электропитание, телефон и сетевое соединение. Проработайте эти вопросы с группой обеспечения. Может быть, разумно назначить резервное местоположение офиса для выполнения важнейших функций в качестве элемента аварийного плана.

Хорошая подготовка к чрезвычайной ситуации

У компании был центр обработки вызовов в Калифорнии, который использовался ее клиентами, в основном крупными финансовыми структурами. В компании имелся хорошо отработанный план действия в случае чрезвычайной ситуации, которая затронет здание центра обработки вызовов. У компании были внешние источники обеспечения электропитания и телефонных служб центра обработки вызовов, а также соответствующие кабели и готовое оборудование, в том числе палатки и складные столы и стулья. Когда в 1991 году произошло сильное землетрясение, центр обработки вызовов был быстро перемещен из здания и снова заработал через несколько минут. Спустя некоторое время после его восстановления поступило много звонков от клиентов из Нью-Йорка, которые хотели убедиться в том, что услуги доступны. Персонал центра обработки вызовов спокойно сообщал клиентам, что все службы работают в нормальном режиме. Клиенты даже представить не могли, что разговаривали с людьми, которые сидели на стульях на траве вне здания. Центр обработки вызов был вынужден оставаться на улице несколько дней, пока не была подтверждена безопасность здания. Но для клиентов он оставался работоспособным все время.

План перемещения центра обработки вызовов из здания в случае чрезвычайной ситуации сработал хорошо, потому что землетрясение было наиболее вероятной чрезвычайной ситуацией и погода была сухой, по крайней мере в то время, которое потребовалось для того, чтобы поставить палатки. Компания хорошо подготовилась к наиболее вероятному сценарию чрезвычайной ситуации.

10.1.6. Целостность данных

Целостность данных означает обеспечение неизменности данных под действием внешних источников. Данные могут быть повреждены злоумышленно при помощи вирусов или вручную. Также они могут быть повреждены случайно в результате действий людей, багов в программах и не обнаруженных вовремя сбоев оборудования. Целостность важных данных необходимо обеспечивать путем определенных операций и ежедневного резервного копирования и архи-

вации. Например, данные, которые не должны изменяться, можно проверять по неизменяемой контрольной сумме данных. Базы данных, в которых предусмотрены лишь небольшие изменения или только добавление данных, могут проверяться на неожиданно большие изменения или удаления. В качестве примеров можно назвать системы контроля исходного кода и базы данных генетических последовательностей. Учитывайте известные вам особенности данных в ваших системах при создании автоматизации проверки целостности.

Аварийное планирование также включает обеспечение возможности воспроизводства и восстановления в системах полной и достоверной копии корпоративных данных. Для аварийного восстановления это должна быть недавняя, согласованная копия данных с синхронизацией всех баз данных. Аварийное восстановление должно обеспечивать целостность данных.

Промышленный шпионаж и кража интеллектуальной собственности довольно распространены, и может получиться так, что компании необходимо будет защищать свои права на интеллектуальную собственность в суде. Возможность быстрого восстановления данных в виде, существовавшем на определенную дату, может быть использована для доказательства владения интеллектуальной собственностью. Для применения в качестве доказательства дата полученной информации должна быть точно известной, а данные должны быть в целостном состоянии. Как для задач аварийного восстановления, так и для использования в качестве доказательства в суде системные администраторы должны знать, что данные не были искажены.

Важно, чтобы при реализации использовались те механизмы обеспечения целостности данных, которые рекомендовали проектировщики системы. Вы не можете быть уверены, что готовы к нештатной ситуации, пока не подтверждена надежность этих систем.

10.2. Тонкости

Полная подготовка к нештатной ситуации заключается в наличии резервных версий всего, что может взять работу на себя, когда основная версия откажет. Другими словами, должен иметься резервный сайт с резервными системами. В этом разделе мы рассмотрим наличие резервного сайта и некоторые способы, которые компания может использовать, чтобы сделать этот сайт более рентабельным.

Несмотря на высокие затраты, в крупных компаниях, особенно в банках, наличие резервного сайта является необходимостью. Фактически крупные компании перестали использовать термин «*аварийное восстановление*» и вместо него пользуются термином «*планирование резервных вариантов*» или «*планирование непрерывности бизнеса*».

10.2.1. Резервный сайт

Для компаний, которым требуется высокая доступность, следующим уровнем аварийного планирования является наличие полного резервного сайта, расположенного в месте, которое не будет затронуто той же самой чрезвычайной ситуацией. Для большинства компаний это дорогостоящая мечта. Однако, если у компании есть два помещения с вычислительными центрами, есть возможность продублировать некоторые критические службы в обоих вычислительных

центрах, чтобы единственной проблемой, которую останется решить, было обеспечение доступа пользователей служб к резервному сайту.

Вместо того чтобы постоянно хранить резервное оборудование во втором помещении, его можно использовать в качестве альтернативного варианта для восстановления служб. Если у компании есть контракт на поставку оборудования в случае чрезвычайной ситуации, это оборудование может быть отправлено в помещение альтернативного вычислительного центра. Если помещение, затронутое чрезвычайной ситуацией, было серьезно повреждено, это может быть самым быстрым способом восстановить работоспособность служб. Другой вариант – обозначить некоторые службы каждого сайта как менее важные и использовать оборудование этих служб для восстановления важнейших служб поврежденного сайта. В некоторых случаях у вас может быть структура, разделенная на отдельные элементы, что упрощает проектирование резервного сайта.

10.2.2. Нарушения безопасности

Нарушения безопасности являются растущей проблемой. Кто-то взламывает веб-сайт корпорации и изменяет логотип на непристойное изображение. Кто-то похищает базу данных номеров кредитных карт с вашего сайта электронной коммерции. Вирус удаляет все файлы, к которым может получить доступ. В отличие от природных чрезвычайных ситуаций, физический ущерб не наносится, а атака может осуществляться не с физически локального объекта.

Для определения типов мер по защите данных можно провести аналогичный анализ рисков. В архитектурных решениях есть элемент риска. Можно справиться с риском несколькими способами – за счет построения барьеров вокруг системы или с помощью мониторинга системы, чтобы можно было быстро ее отключить в случае атаки.

Мы постоянно видим сайты, которые покупают крупные готовые системы, не требуя объяснения рисков безопасности этих систем. Хотя ни одна система не является абсолютно безопасной, продавец должен уметь объяснить структуру безопасности продукта, факторы риска и восстановление в случае потери данных. В главе 11 рассмотрено создание политик и процедур безопасности, которые учитывают планы по аварийному восстановлению.

10.2.3. Отношения с прессой

Когда произойдет чрезвычайная ситуация, журналисты, скорее всего, захотят узнать, что случилось, как это повлияло на компанию и когда службы будут восстановлены. К сожалению, обычно вы можете дать лишь один ответ на все три вопроса: «Мы не знаем». Это, пожалуй, является наихудшим ответом, который можно дать репортеру. Невнимательное отношение к прессе во время чрезвычайной ситуации может вызвать больше проблем, чем собственно сама ситуация.

По этому вопросу у нас есть две простых рекомендации. Во-первых, заключите соглашение с компанией по связям с общественностью (PR – Public Relations) заблаговременно, чтобы вы не пытались привлечь ее к сотрудничеству во время чрезвычайной ситуации. Некоторые PR-компании специализируются на чрезвычайных ситуациях, другие являются экспертами в области нарушений безопасности. Во-вторых, заблаговременно планируйте, как вы будете общаться

с прессой. Этот план должен включать следующее: кто будет общаться с прессой, что будет и что не будет сказано и каков порядок цепочки управления при отсутствии ответственных за принятие решений. Все, кто будет общаться с прессой, должны пройти подготовку в вашей PR-компании.

Обратите внимание, что у этих рекомендаций есть одна общая черта: они требуют заблаговременного планирования. Никогда не позволяйте себе попасть в чрезвычайную ситуацию без плана отношений с прессой и не пытайтесь создать его во время этой ситуации.

10.3. Заключение

Самый важный аспект аварийного планирования – понимание того, какие службы являются наиболее важными для бизнеса и каковы временные рамки восстановления этих служб. Ответственному за аварийное планирование также нужно знать, какие чрезвычайные ситуации могут произойти и какие расходы они вызовут, прежде чем завершить анализ рисков и определить бюджет компании на ограничение ущерба.

Аварийный план должен строиться с учетом этих критериев. Он должен учитывать время, необходимое для получения нового оборудования, внешних резервных копий и восстановления всей системы с нуля. Это требует заблаговременного планирования для получения нужного оборудования и возможности быстро определить, какие резервные кассеты необходимы для восстановления критических систем.

Ответственный за аварийное планирование должен искать как простые способы ограничения ущерба, так и более сложные и дорогие. Наиболее эффективными являются средства автоматического действия, включенные в инфраструктуру. К этой категории относятся системы пожаротушения, обнаружения воды, сейсмоустойчивые опоры и подходящее оборудование, монтируемое в стойках. Ответственный за аварийное планирование также должен подготовить план действий людей в случае чрезвычайной ситуации. Простые планы часто наиболее эффективны. Члены группы должны знать свои персональные обязанности и проходить практикум несколько раз в год.

Полное резервирование, включающее резервный сайт, является идеалом, который большинство компаний не могут себе позволить. Однако, если у компании есть второй вычислительный центр, существуют способы включить его в аварийный план с разумными расходами.

Задания

1. Какие подразделения бизнеса вашей компании потребуется восстановить после чрезвычайной ситуации в первую очередь и в какие сроки необходимо сделать их работоспособными?
2. Какие обязательства есть у вашей компании перед клиентами и как эти обязательства влияют на ваше аварийное планирование?
3. Какие чрезвычайные ситуации наиболее вероятны для каждого из ваших сайтов? Какую территорию может затронуть эта чрезвычайная ситуация и сколько зданий вашей компании может быть затронуто?

4. Каковы будут расходы вашей компании, если чрезвычайная ситуация средней силы затронет одно из помещений?
5. Какие формы ограничения воздействия чрезвычайных ситуаций вы сейчас используете?
6. Какие формы ограничения воздействия чрезвычайных ситуаций вы хотели бы внедрить? Сколько стоит каждая из них?
7. Как бы вы восстановили обслуживание, если бы работоспособность вычислительного центра нарушилась из-за чрезвычайной ситуации?
8. Каковы ваши планы по общению с прессой в случае чрезвычайной ситуации? Как называется PR-компания, которую вы привлечете для помощи?

Глава 11

Политика безопасности

Безопасность – это гораздо больше, чем межсетевые экраны, обнаружение вторжений и схемы аутентификации. Эти компоненты являются ключевыми в программе безопасности, но администраторам безопасности также необходимо выполнять множество других задач, требующих различных знаний. В данной главе мы рассмотрим все аспекты безопасности и опишем основные элементы, необходимые компании для реализации успешной программы безопасности, а также некоторые руководящие принципы и общие требования безопасности. Кроме того, мы кратко обсудим, как описанные здесь подходы применяются в компаниях различного размера, и покажем некоторые возможные отличия применяемых вами подходов к безопасности от идеального случая.

Безопасность – это широкая тема, по которой написано много хороших книг. Цвики, Чепмэн и Купер (Zwicky, Chapman and Cooper 2000) и Белловин, Чесуик и Рубин (Bellovin, Cheswik and Rubin 2003) написали отличные книги о межсетевых экранах. В книгах Гарфинкеля и Спэффорда (Garfinkel and Spafford 1996, 1997) рассмотрены вопросы безопасности UNIX и Интернета, а также веб-безопасности и безопасности электронной коммерции. Норберг и Рассел (Norberg and Russel 2000), а также Шелдон и Кокс (Sheldon and Cox 2000) предоставляют подробный обзор безопасности Windows. Книга Miller and Davis 2000 охватывает область интеллектуальной собственности. Вуд (Wood 1999) хорошо известен своими образцами политик безопасности. Ковачич (Kovacich 1998) рассматривает тему создания программы для защиты информации. Нойманн (Neumann 1997) и Деннинг (Denning 1999) рассматривают тему рисков и информационного противоборства.

Безопасность должна быть задачей каждого. Однако важно, чтобы в компании были сотрудники, которые специализируются на потребностях организации, касающихся безопасности, и уделяют им основное внимание. Безопасность – это широкая, быстро изменяющаяся область знаний, и, чтобы идти в ногу со временем, системные администраторы, отвечающие за безопасность, должны уделять все свое внимание области безопасности. Хорошими кандидатами для обучения в этой области и работы в группе безопасности являются старшие системные администраторы с подходящим образом мышления.

Безопасность данных требует больше навыков общения и связей в компании, чем любая другая область системного администрирования. Во многих компаниях люди считают компьютерную безопасность препятствием для своей работы. Для достижения успеха вы должны разрушить этот стереотип и на максимально ранней стадии принимать участие во всех проектах, которые затрагивают электронную безопасность компании.

Мы надеемся, что из этой главы вы усвоите в первую очередь следующее: политика, которую легко и приятно соблюдать, – самая удобная для пользователя. Если вы хотите, чтобы люди соблюдали правила, убедитесь, что это самый простой для них вариант. Например, если вы хотите, чтобы люди пользовались шифрованием электронной почты, убедитесь, что приложение, которое вы предлагаете, позволяет отправлять ее так же просто, как и обычную электронную почту, иначе люди не будут им пользоваться. Доведение политики или технологии до точки, в которой она будет проще всех остальных вариантов, потребует от вас серьезных усилий. Однако это лучше, чем тратить свое время на борьбу с проблемами безопасности.

С течением времени использование компьютера эволюционировало от необходимости непосредственного физического присутствия до возможности удаленного доступа из любой точки мира. В соответствии с этим развивались и средства и методы безопасности. Как изменятся модели доступа к компьютерам и сетям в будущем и как это изменение повлияет на безопасность? В настоящее время наблюдается тенденция к более широкому применению шифрования и строгой аутентификации в противоположность физической безопасности или доверительным отношениям. Каждая новая модель доступа требует все больше планирования, обучения, тестирования и применения прогрессивных технологий.

11.1. Основы

Две основные схемы политики безопасности – это *безопасность периметра* и *глубокая защита*.

1. **Безопасность периметра** – это что-то вроде крепости с высокими стенами. Постройте хорошую стену – и вы сможете делать внутри что угодно. Поставьте хороший межсетевой экран на входе в вашу сеть – и вам не придется беспокоиться о том, что будет внутри. В книге Bellovin, Cheswick and Rubin 2003 данный подход рассматривается как «твердый леденец с мягкой начинкой», или политика, при которой «все яйца складываются в одну корзину, а затем обеспечивается защищенность этой корзины». Проблема безопасности периметра в том, что «твердая оболочка» исчезает с распространением беспроводных сетей и соединением сетей организации и партнеров.
2. **Глубокая защита** предполагает размещение средств безопасности во всех точках сети. Например, межсетевой экран защищает организацию от атак из Интернета, антивирусная система сканирует каждое сообщение электронной почты, на каждом отдельном компьютере установлены программы для борьбы с вредоносными программами, а при передаче данных между компьютерами используются шифрование и аутентификациая.

Как и в случае с проектированием других компонентов инфраструктуры, проектирование системы безопасности должно быть основано на простоте, возможности нормального использования и минимализме. Сложность повышает риск появления ошибок или уязвимостей в вашей защите. Слишком сложная система будет негибкой, неудобной в использовании и поддержке, тем самым вынуждая людей всячески обходить ее ограничения, чтобы эффективно работать. Кроме того, в эффективной архитектуре безопасности элементы обеспечения безопасности встроены в систему, а не являются поверхностными надстройками. Хорошая система безопасности предполагает глубокий подход с элементами обеспечения безопасности на всех уровнях системы. Если этих элементов нет

с самого начала, их может быть очень трудно добавить и интегрировать в дальнейшем.

Некоторые считают, что безопасность обратно пропорциональна удобству. То есть обеспечение большей безопасности какого-либо объекта затрудняет его использование. Это, конечно, было справедливо для ряда продуктов по обеспечению безопасности. Мы полагаем, что, когда обеспечение безопасности осуществляется правильно, учитывается и простота работы пользователей. Проблема в том, что часто технологии требуется несколько лет, чтобы дойти до данного уровня развития. Например, пароли являются хорошей практикой, но установка паролей на каждое приложение становится головной болью для людей, которые в ежедневной работе используют много приложений. Однако при повышении безопасности за счет развертывания системы единой авторизации увеличивается и удобство в результате усиленной безопасности при практически полном отсутствии необходимости введения пользователями паролей.

Когда система безопасности неудобна, ваши пользователи найдут способы ее обхода. Однако при достаточном развитии технологий безопасности система становится более безопасной *и* простой в применении.

Безопасность и надежность

Безопасность и надежность тесно связаны между собой. Небезопасная система открыта для атак, что делает ее ненадежной. Злоумышленники могут вывести ненадежную систему из строя за счет использования уязвимостей, что представляет собой атаку «отказ в обслуживании» (Denial-of-Service, DoS-атака). Если руководство не интересуется проблемой безопасности, разберитесь, важна ли для него надежность, и если да, представляйте все вопросы безопасности как вопросы надежности.

11.1.1. Задавайте правильные вопросы

Прежде чем реализовать успешную программу безопасности, вы должны определить, что вы пытаетесь защитить, от кого, каковы риски и расходы компании. Эти деловые решения должны быть приняты в результате серьезного обсуждения с руководством компании. Задокументируйте решения, принятые в ходе этого процесса, и рассмотрите окончательный документ с руководством. Этот документ должен будет развиваться вместе с компанией, но его не следует изменять слишком сильно или часто.

11.1.1.1. Защита информации

Корпоративная безопасность касается защиты активов. Чаще всего информация является активом, наиболее важным для компании. Информация, подлежащая защите, может принадлежать к нескольким категориям. Развитая программа безопасности определяет набор категорий и классифицирует информацию в них.

Классификация информации определяет, какой уровень безопасности к ней применяется. Например, информация может быть категорирована как публичная, конфиденциальная и строго конфиденциальная информация компании.

Публичная информация может включать литературу по маркетингу, руководства пользователей и публикации в журналах или на конференциях. Конфиденциальная информация компании может включать схемы организации, телефонные справочники, внутренние новости с финансовыми результатами, направление коммерческой деятельности, статьи по продуктам в разработке, исходный код или политики безопасности. Строго конфиденциальная информация должна очень серьезно отслеживаться и быть доступной только тем, кому она действительно необходима. Она может включать переговоры по контрактам, информацию о сотрудниках, особо секретные подробности разработки продукции или интеллектуальную собственность клиента.

Другой аспект защиты информации – защита от злонамеренного изменения, умышленной или случайной утечки информации, ее кражи или уничтожения.

Пример: защита от злонамеренного изменения

Сотрудники ведущей нью-йоркской газеты рассказали консультанту по безопасности, что, несмотря на свое беспокойство о возможной краже информации, их главной проблемой была возможность необнаруженной модификации информации. Что произойдет, если отчет о компании будет намеренно искажен? Что случится, если заголовок будет заменен неприличным выражением? Фраза «Сегодня [вставьте название вашей любимой ведущей газеты] сообщила...» имеет очень большую ценность, которая была бы дискредитирована, если бы злоумышленники могли изменять содержимое газеты.

11.1.1.2. Доступность обслуживания

В большинстве случаев компании требуется защищать доступность обслуживания. Если компания в ведении бизнеса полагается на доступность определенных электронных ресурсов, то одной из задач группы безопасности будет предотвращение DoS-атак против этих ресурсов. Часто компании не думают об этом, пока не начинают предоставлять интернет-услуги, потому что сотрудники обычно не склонны проводить такие атаки против своей собственной компании.

11.1.1.3. Кража ресурсов

Иногда компания хочет защититься от кражи ресурсов. Например, если производственная линия обслуживается компьютерным оборудованием практически при полной загрузке, потому что часть вычислительных циклов компьютера используется для других задач, компании потребуется снизить вероятность применения вычислительных циклов этой машины злоумышленниками. То же самое касается больничного оборудования с компьютерным управлением, где от доступности вычислительных ресурсов при первом требовании может зависеть жизнь человека. Сайты электронной коммерции также могут подвергнуться краже ресурсов. Их системы могут быть замедлены пиратами, скрывающими в инфраструктуре FTP- или чат-серверы, что приводит к потере клиентуры.

11.1.1.4. Выводы

Совместно с вашей руководящей группой решите, что вам нужно защищать и от кого, сколько это будет стоить компании и каковы риски. Определите категории информации и допустимые для них уровни защиты. Задокументируйте эти решения и используйте полученный документ как основу для своей программы безопасности. С развитием компании не забывайте периодически переоценивать решения в этом документе совместно с руководящей группой.

Пример: решите, что важно, а затем защищайте это

Любому консультанту часто приходится слышать различные ответы на вопрос «Что вы хотите защитить?». Обычно (но не всегда) ответ предсказуем.

Компания среднего размера, занимавшая автоматизацией проектирования электроники, где имелась комиссия по защите информации, в которую входили специалисты различного профиля, считала наиболее важным объектом защиты интеллектуальную собственность клиентов и бизнес-партнеров, а следующим по значимости – свою собственную интеллектуальную собственность. Клиенты отправляли этой компании свои проекты чипов в случае наличия проблем с инструментами или если у них было совместное соглашение по оптимизации программного обеспечения для проектов клиентов. Компания также работала с бизнес-партнерами над совместными проектами, которые предполагали двусторонний обмен информацией. Информация третьих сторон всегда сопровождалась контрактными соглашениями о мерах безопасности и ограничения доступа. Компания понимала, что, если клиенты или бизнес-партнеры потеряют доверие к ее безопасности, особенно в плане несанкционированного доступа к этой информации, компания никогда больше не будет иметь доступа к информации, которая сделала ее лидером в своей области, и в конце концов клиенты уйдут к конкурентам. Если бы кто-то получил доступ к интеллектуальной собственности самой компании, это не принесло бы такого ущерба, как потеря доверия клиентов.

Для компании, занимающейся лишь электронной коммерцией, наиболее важной была доступность ее сайта электронной коммерции, а вторым приоритетом – защита доступа к кредитным картам клиентам. Эта компания совсем не беспокоилась о доступе к своей интеллектуальной собственности.

Подразделение по производству оборудования в большой транснациональной компании в области электроники имело другой приоритет. В данном случае наиболее важны были доступность систем контроля производства и доступ к ним.

Для большой компании в области сетевого оборудования и программного обеспечения наиболее важными были финансовая система и система обработки заказов. Удивительно, но ни интеллектуальная собственность компании, ни интеллектуальная собственность клиентов упомянуты не были.

11.1.2. Документируйте политики безопасности компании

Политики – это основа всего, что делает группа обеспечения безопасности. Формальные политики должны создаваться в сотрудничестве с людьми из многих других отделов. В создание определенных политик должен быть вовлечен отдел кадров, особенно при определении политик допустимого использования, политик мониторинга и неприкосновенности частной информации, а также при определении и реализации санкций за любые нарушения политики. Юридический отдел должен быть вовлечен в создание политик, определяющих необходимость отслеживания и преследования нарушителей, а также того, как и когда привлекать правоохранительные органы при совершении незаконных действий. Естественно, все политики должны быть одобрены высшим руководством.

Решения, принимаемые группой обеспечения безопасности, должны поддерживаться политикой, чтобы обеспечить соблюдение решений, одобренных руководством, в этой очень щекотливой области. Эти политики должны быть задокументированы и формально одобрены соответствующими людьми. Группу обеспечения безопасности будут просить обосновать свои решения во многих областях, и она должна иметь возможность принимать решения с уверенностью в том, что они находятся в полном соответствии с интересами компании, определенными руководством компании, а не группой безопасности, инженерного обеспечения или какой-либо другой.

В разных случаях требуются различные наборы политик, и до какой-то степени эти наборы политик будут постоянно развиваться и обновляться с возникновением новых ситуаций. Однако для начала можно взять следующий набор общих политик.

- **Политика допустимого использования (**Acceptable Use Policy – AUP) определяет правомочных пользователей компьютерных и сетевых ресурсов, а также то, для чего им разрешено использовать эти ресурсы. AUP также может включать некоторые явные примеры недопустимого использования. Правомочные пользователи компьютерных и сетевых ресурсов перед получением доступа к ним должны подписать экземпляр этой политики, подтверждая, что они прочли ее и согласились с ней. При наличии в компании нескольких зон безопасности может применяться несколько AUP.
- **Политика мониторинга и неприкосновенности личной информации** описывает мониторинг компьютерных и сетевых ресурсов компании, в том числе мониторинг деятельности на отдельных компьютерах, сетевого трафика, электронной почты, обзора веб-страниц, журналов регистрации событий и логов. Поскольку мониторинг может расцениваться как посягательство на личную информацию, в политике должно быть в явном виде указано, на какой уровень неприкосновенности личной информации может рассчитывать человек при использовании этих ресурсов, если он вообще есть. Иногда местные законы устанавливают, что может и что не может входить в эту политику, особенно в Европе. Опять же, каждый человек должен прочитать и подписать экземпляр этой политики, прежде чем получить доступ к ресурсам.
- **Политика удаленного доступа** должна объяснять риски, связанные с получением доступа к сети людьми, не имеющими на это права, описывать необходимые меры предосторожности для «секретных» данных человека – пароля, персонального идентификационного номера (Personal Identification

Number – PIN) и т. д. – и обеспечивать способ оповещения об утерянных или украденных данных для удаленного доступа, чтобы их использование можно было быстро запретить. Эта политика также должна содержать некоторые вопросы личного характера – например, о размере обуви и любимом цвете, – при помощи которых люди могут быть идентифицированы по телефону. Каждый должен заполнить и подписать копию этой политики перед разрешением удаленного доступа.

- **Политика сетевых соединений** описывает, как компания устанавливает сетевые соединения для других субъектов или некоторых общих ресурсов для доступа третьих сторон. Каждой компании в определенный момент потребуется установить деловые отношения с другой компанией, что потребует более простого доступа к сети и, может быть, наличия некоторых общих ресурсов: расширенной интрасети. Вы должны заранее подготовиться к этому. Политика должна быть распространена по всем уровням руководства и предусматривать участие группы обеспечения безопасности на максимально ранней стадии. В политике должны быть перечислены различные поддерживаемые типы соединений и общих ресурсов, офисы, которые могут поддерживать соединение с третьими сторонами, и типы поддерживаемых соединений.
- **Политика ведения журналов** (или логов) описывает, что заносится в журналы и на какой срок. Журналы полезны для отслеживания нарушений безопасности после того, как они произошли, но могут занимать большие объемы дискового пространства при отсутствии временных ограничений. Также важно знать, существуют ли логи определенной даты, в случае вызова в суд по уголовному делу.

Пример: применение лучших технологий упрощает политику

Самая легкая для соблюдения политика – максимально упрощенная. Например, в политики использования паролей часто включают руководства по созданию подходящих паролей и указывают, с какой периодичностью они должны меняться на машинах различных классов. Эти подробности могут быть сокращены или исключены за счет применения лучших технологий. Например, инфраструктура Bell Labs включает систему электронных удостоверений (HandHeld Authenticator – HHA), которая вообще не требует использования паролей. Что может быть проще?

Электронные удостоверения

Для удостоверения личности людей используется HHA, устройство размером с калькулятор или толстую кредитную карту. Для идентификации пользователя HHA генерирует одноразовый пароль (OTP – One-Time Password). Один класс HHA отображает новую комбинацию из 7 цифр каждые 30 с. Часы синхронизированы, поэтому узел знает, какие цифры должны быть введены конкретным пользователем. Вместо пароля пользователь вводит цифры (HHA защищено PIN-кодом). Таким образом,

компьютер может знать, что пользователь – действительно тот, за кого себя выдает, или, по крайней мере, держит в руках соответствующее HHA и знает PIN-код этого человека. Это более безопасно, чем пароль, который никогда не меняется или меняется очень редко.

HHA могут использоваться для авторизации на узлах, получения удаленного доступа – UNIX-команда `su` – и даже получения доступа к вебсайтам. С такой инфраструктурой политики использования паролей становятся гораздо проще. Узлы за пределами межсетевого экрана больше не требуют политик использования паролей, потому что здесь не применяются жесткие пароли. Получение безопасного `root`-доступа к UNIX-системам, которое ранее было затруднено из-за опасений по поводу перехвата паролей, стало более реальным за счет преимуществ HHA в сочетании с шифрованием[1]. Этот пример показывает, как правильно организованное усиление безопасности делает систему более удобной.

Недостаток политик затрудняет работу группы безопасности

Кристина была привлечена к работе в качестве консультанта в крупной транснациональной компании, производящей компьютеры, у которой не было формально утвержденной письменной политики безопасности. В частности, в компании не было политики сетевых соединений. В результате у многих офисов были небезопасные соединения с третьими сторонами, во многих случаях корпоративное IT-подразделение и группа безопасности даже не знали, что эти соединения существуют, потому что у удаленных офисов не было никаких обязательств сообщать об этих соединениях.

Кристину попросили работать над централизацией доступа третьих сторон к корпоративной сети на трех сайтах в США, двух сайтах в Европе, одном сайте в Австралии и одном сайте в Азии. В процессе обнаружения всех существующих соединений оценка количества соединений с третьими сторонами увеличилась примерно с 50 до 80.

Группа безопасности провела беседу с людьми, ответственными за соединения, и описала новую архитектуру и ее преимущества для компании. Затем группа обсудила с пользователями, какие услуги в этой новой архитектуре им требуются. Уверив себя и пользователей в том, что все услуги будут доступны, группа начала обсуждение перехода на новую архитектуру. В большинстве случаев на этом этапе процесс останавливался. Поскольку новая архитектура была сосредоточена на нескольких сайтах-концентраторах, соединения с небольшими офисами продаж, ближайшими к третьим сторонам, пришлось переносить дальше, что привело к росту расходов. За неимением не только политики с явным указанием разрешенных способов подключения третьих сторон к сети, но и денег, выделенных на оплату дополнительных расходов на связь, группе безо-

[1] SSH предоставляет зашифрованную систему, аналогичную rsh/telnet (Yben 1996, см. также Farrow 1997 и Thorpe 1998b).

пасности некуда было обратиться за помощью, когда пользователи отказались оплачивать дополнительные расходы на перенесение соединений или добавление элементов безопасности в существующие соединения.

Несмотря на завершение построения в главном офисе, начальная инфраструктура соединений с третьими сторонами принималась очень неохотно, в результате чего другие центры соединений не были созданы. При наличии разумной и поддерживаемой руководством политики сетевых соединений результат мог бы кардинально отличаться. Руководству нужно было поддерживать проект как материально, так и за счет создания формальной политики, которую группы должны были бы соблюдать.

В качестве противоположного примера можно привести работу Кристины на сайте, на котором уделялось большое внимание безопасности, где имелись политики и группа защиты информации. На этом сайте она установила похожую централизованную область для соединений с третьими сторонами, где предоставлялся доступ людям из других компаний, которые работали на сайте. Эта область использовалась для большинства соединений третьих сторон. У остальных соединений третьих сторон была своя инфраструктура безопасности, разрешенная политикой сетевых соединений. Относительно расходов не было никаких вопросов, потому что такого порядка требовала политика компании и все понимали и принимали причины.

Управление сетевыми соединениями с партнерами

Федеральное авиационное агентство США (Federal Aviation Administration – FAA) имеет сетевые соединения с аналогичными организациями практически каждой страны мира, а также со многими авиакомпаниями, поставщиками и партнерами. Однако в FAA не было универсальной политики по управлению этими соединениями и обеспечению их безопасности. Фактически в FAA не было списка соединений. Без списка эти соединения нельзя было проверять. Без проверки не было безопасности.

В FAA очень удачно подошли к составлению списка, который позволил бы начать проверку и обеспечение безопасности. Сначала список был составлен на основании всей информации, которая была в наличии и могла быть получена при анализе сети различными средствами.

Как только в сетевой группе посчитали, что сделали все возможное, пришла пора объявить новую политику проверки всем IT-организациям в FAA. Сначала группа хотела объявить, что за все сетевые соединения, которые не входят в список и, следовательно, не являются проверенными и безопасными, будут применяться санкции к людям, ответственным за сетевые соединения. Однако группа поняла, что это просто заставит людей тщательнее скрывать такие соединения. Фактически это заставило бы людей с незарегистрированными соединениями «уйти в подполье».

Вместо этого группа объявила о программе амнистии. В течение нескольких месяцев любой мог сообщить о неофициальных сетевых соединениях и не понести наказания, а получить помощь в проверке соединения и обеспечении его безопасности. Однако всем, кто не откликнулся до определенного срока, грозили неприятности.

Люди признавались массово, иногда по электронной почте, иногда очень испуганный человек приходил в офис директора, чтобы признаться лично. Но программа работала. Многие люди пришли в группу за помощью, никто не был наказан. Фактически даже после окончания программы амнистии один человек, который пришел в офис директора практически в слезах, признался и не понес наказания. Целью было обеспечение безопасности сети, а не увольнение людей, и максимальная открытость и снисхождение были лучшей политикой.

В то же время у сетевой группы было много своих недокументированных соединений, которые требовали анализа для определения того, к чему они были подключены. Иногда для помощи в идентификации линий обращались к биллинговым записям. Иногда разъем имел пометку и недолгий поиск позволял определить владельца сети, что приводило к более серьезному поиску, который определял линию. В других случаях группе везло меньше.

В конце концов несколько соединений не удалось идентифицировать. После того как все предпринятые попытки оказались безрезультатными, группа просто выбрала день и время, когда в воздухе было меньше всего самолетов, и отключила эти соединения. В некоторых случаях до того, как отключенная страна замечала это и жаловалась, проходили месяцы. Оставшиеся линии так и не были идентифицированы и остались отключенными. Мы не знаем, что является более шокирующим: соединения, которые так и не были определены, или тот факт, что некоторые страны месяцами осуществляли полеты и не жаловались.

11.1.2.1. Получите поддержку высшего руководства

Для того чтобы быть успешной, программа безопасности должна получить поддержку высшего руководства. Руководство компании должно быть вовлечено в создание политик и правил в программе безопасности, чтобы принимались правильные для бизнеса решения и чтобы руководство понимало, какие решения были приняты и почему. Если вы хотите приобрести авторитет как представитель группы обеспечения безопасности, вам потребуется умение ясно объяснить возможности, риски и преимущества, и это нужно будет сделать на деловом языке, а не техническом жаргоне.

В некоторых случаях сотрудники, обеспечивающие безопасность, могут не согласиться с решениями, принятыми руководством компании. Если это случится с вами, попробуйте понять, почему были приняты такие решения. Помните, что у вас может не быть доступа к той же информации или такого знания бизнеса, как у руководящей группы. В деловых решениях принимаются во внимание как технические, так и нетехнические потребности. Если вы хороший представитель группы обеспечения безопасности[1], вы должны понимать, что руководство принимает решения, которые считает лучшими для компании,

[1] Если вы считаете себя недостаточно хорошим представителем группы безопасности, попытайтесь понять, что вы не смогли донести и как лучше всего это объяснить, а затем найдите еще одну возможность обсудить это. Но лучше сделать все правильно с первого раза!

и соглашаться с ними. Люди, обеспечивающие безопасность, склонны строить настолько безопасную систему, что ее невозможно будет завершить, если бизнес не откажется от благоприятной возможности на рынке или не станет таким безопасным, что его невозможно будет развивать. Важно найти баланс между построением совершенной системы и поддержанием развития бизнеса.

Как только корпоративное решение по безопасности было согласовано, оно должно быть задокументировано и одобрено руководством, а затем опубликовано в компании. В идеале директор по безопасности, который не входит в IT-отдел компании, должен находиться на высоком уровне в иерархии руководства. Этот человек должен иметь как навыки ведения бизнеса, так и опыт в области защиты информации. Директор по безопасности должен возглавлять многофункциональную группу защиты информации с представителями из юридических, кадровых, IT-, инженерных отделов, а также отделов службы поддержки и продаж или любых, имеющихся в компании. Директор по безопасности отвечает за обеспечение своевременной разработки, одобрения и исполнения адекватных политик и ведет деятельность группы обеспечения безопасности и защиты информации в необходимом для компании направлении.

Отсутствие поддержки руководства

Когда Кристина приехала в компьютерную компанию, описанную в предыдущем примере, она спросила о политике безопасности компании. За два года до этого многофункциональная группа написала политику безопасности в соответствии с неофициальной политикой компании и отправила его руководству для формального одобрения. Политика застревала на различных уровнях иерархии IT-руководства на месяцы. Никто из старшего руководства не был заинтересован в ее продвижении. Руководитель группы обеспечения безопасности периодически пытался продвигать ее снизу, но это было почти безуспешно.

Безуспешность попыток была обусловлена слабым интересом к вопросам безопасности в компании вообще. Персонал компании, ответственный за безопасность, не задерживался надолго из-за слабой поддержки, и в конце концов компания была вынуждена обратиться для обеспечения безопасности к консалтинговой фирме.

Если группа обеспечения безопасности не может полагаться на поддержку руководителей высокого уровня, программа безопасности неизбежно потерпит неудачу. В группе безопасности будет большая текучка кадров, а выделенные на безопасность деньги будут потрачены впустую. Поддержка высшего руководства жизненно важна.

Обучение вашего начальника

Иметь начальника, понимающего вашу работу, – роскошь. Однако иногда вам может очень пригодиться способность обучать своего начальника.

В одной финансовой компании человек, ответственный за безопасность, должен был отчитываться перед вице-президентом, почти не имеющим опыта работы с компьютером. Кошмар, правда? Нет.

Они организовали сотрудничество. Человек, ответственный за безопасность, взял на себя выполнение задач по обеспечению безопасности и контроль всех технических аспектов при условии, что вице-президент будет предоставлять необходимые ресурсы. Вице-президент обеспечивал необходимое финансирование на каждом этапе, ответственный за безопасность предоставлял вице-президенту нужную информацию перед каждым собранием по разработке бюджета, иначе ему пришлось бы строить систему безопасности компании в одиночку.

Их совместная деятельность оказалась очень успешной.

11.1.2.2. Централизуйте полномочия

Появляются вопросы. Возникают новые ситуации. Имея одно место для разрешения этих проблем, легче поддерживать программу безопасности единой и эффективной. Должен быть совет по политике безопасности, или **центральный орган для решений**, связанных с безопасностью: деловых решений, решений в области создания политики, архитектуры, реализации, реакции на происшествия и проверки.

Невозможно реализовать стандарты безопасности и обеспечивать эффективную реакцию на происшествия без центрального органа, который поддерживает и проверяет безопасность. В некоторых компаниях есть центральный орган для каждого автономного подразделения бизнеса и центральный орган более высокого уровня для установления общих стандартов. В других случаях мы видели орган безопасности корпоративного масштаба с одним отдельным подразделением вне его контроля, который принадлежал недавно приобретенной компании. Если компания полагает, что какие-то автономные подразделения бизнеса должны иметь контроль над созданием своей политики, архитектуры и т. д., компьютерные и сетевые ресурсы таких подразделений должны быть четко отделены от ресурсов остальной компании. Взаимосвязи должны рассматриваться как соединения с третьими сторонами, и каждая сторона должна применять к этим соединениям свои политики и архитектурные стандарты.

Несколькими автономными сетями в одной компании может быть очень трудно управлять. Например, если у двух частей компании различные политики мониторинга без четкого разделения ресурсов подразделений бизнеса, то может оказаться так, что одна группа безопасности будет непреднамеренно просматривать трафик сотрудника другого подразделения бизнеса, что будет противоречить его ожиданиям относительно неприкосновенности личной информации. Это может привести к судебному делу и негативному общественному мнению, а также отчуждению персонала.

На техническом уровне эффективность вашей безопасности равна эффективности ее самого слабого звена. Если к вашей сети открыт доступ из другой сети, над которой у вас нет контроля, вы не знаете, какая связь является слабейшей, и у вас нет над ней контроля. Вы также можете испытывать затруднения в отслеживании нарушителя, воспользовавшегося такой открытой связью.

Пример: отсутствие центрального органа

В одной крупной компании каждое подразделение использовало свои собственные (недокументированные) политики, но сеть была единой. Многие подразделения подключали к сети третьи стороны без каких-либо мер безопасности. В результате подозрения на нарушения безопасности в одном из офисов возникали каждые несколько недель и группе обеспечения безопасности приходилось тратить несколько дней на поиск ответственных людей в подразделении, чтобы узнать, что случилось, если что-то случилось вообще. Иногда группу безопасности вызывали среди ночи, чтобы разобраться с нарушением безопасности, но она не имела доступа к месту, где, скорее всего, произошло нарушение, и возможности связаться с людьми, ответственными за него, до следующего дня. Напротив, там, где имелись центральный орган и политики, подобных подозрений и нарушений не было.

11.1.3. Основы для технического персонала

Как технический сотрудник группы обеспечения безопасности вы должны иметь в виду несколько других принципов, наиболее важный из которых – обеспечение ежедневных рабочих потребностей людей, которые будут пользоваться спроектированными вами системами. У этих людей должна быть возможность выполнять свою работу. Вы также должны быть в курсе того, что происходит в области уязвимостей и атак, чтобы при появлении новой уязвимости или нового способа атаки ваш сайт был адекватно защищен. Критическим элементом инфраструктуры, который вам потребуется и за выбор которого вы будете отвечать, – это система аутентификации и авторизации. Мы дадим несколько советов по выбору правильных продуктов для задач, в которых важна безопасность.

Состояние безопасности

Хотя эта глава о том, как помочь вам построить правильную политику для своей организации и создать на основе этой политики хорошую инфраструктуру безопасности, следующие технологии обязательны к использованию во *всех* сетях:

- *Межсетевые экраны* (брандмауэр, firewall). Сеть организации должна быть отделена от Интернета при помощи межсетевого экрана.
- *Фильтрация электронной почты*. Электронная почта, приходящая в вашу организацию, должна проходить через фильтр, защищающий от спама – нежелательной коммерческой электронной почты, – и вирусов.
- *Защита от вредоносных программ*. На каждом компьютере должно быть программное обеспечение для обнаружения и уничтожения вредоносных программ, которые включают в себя вирусы[1], шпионские

[1] Вирус – это программа, которая распространяется с одного компьютера на другой и вызывает какие-либо сбои или повреждения.

программы[1] и червей[2]. Эти защитные программы всегда требуют обновления баз данных с образцами. Программы должны автоматически загружать эти обновления, и должен существовать способ проверить, какие компьютеры в вашей организации не обновляли свои базы в последнее время, чтобы эту ситуацию можно было исправить.

- *Виртуальные частные сети* (Virtual Private Network – VPN). Если офисные сети вашей организации соединяются друг с другом через Интернет или если удаленные пользователи подключаются через Интернет к сети вашей организации, для этих соединений должны обеспечиваться аутентификация и шифрование при помощи какой-либо технологии VPN.

Нас удивляет, сколько посещаемых нами организаций не пользуются этими четырьмя основными технологиями. «Кому нужно нас атаковать?» Просто имейте в виду: если у вас есть компьютеры, то вы являетесь целью. Если нарушителям не нужны ваши данные, им может понадобиться ваша связь для распространения спама. Нам встречаются компьютеры, на которых используются антивирусы без автоматического обновления баз. Интересно, почему такие продукты еще есть на рынке? Мы часто видим фрагментарные подходы к фильтрации электронной почты, использование программ для фильтрации электронной почты только на некоторых машинах вместо централизованной полной фильтрации на сервере. Мы проверяли много сетей, где якобы использовались VPN, но простое тестирование показывало, что пакеты на самом деле не шифровались. Мы называем это «VPN без V или P».

Хотя программа безопасности вашей организации должна основываться на хорошей политике и проработанном процессе, на начальном этапе наличие вышеуказанных четырех технологий является минимальной точкой отсчета.

11.1.3.1. Обеспечивайте потребности бизнеса

При проектировании системы безопасности вы всегда должны знать потребности бизнеса и стремиться обеспечить их. Помните, что нет смысла в обеспечении безопасности компании до уровня, на котором она не может вести свой бизнес. Также помните, что другие люди в компании тоже не глупые. Если они не смогут эффективно работать, пользуясь вашей системой безопасности, они найдут способ взломать ее или обойти. Этот факт нельзя недооценивать: *обходной путь, который найдут люди, будет менее безопасен, чем система, которую вы создали.* Таким образом, лучше использовать чуть менее безопасную систему, чем такую, которую будут обходить.

---

[1] Шпионская программа – это программа, которая наблюдает за действиями пользователя и реагирует на них, например, вставляя платную рекламу при просмотре веб-сайтов.

[2] Червь – это программа, которая распространяется на большое количество компьютеров и позволяет злоумышленнику удаленно программировать компьютер для выполнения своих задач.

Для эффективного выполнения потребностей бизнеса в плане безопасности вам потребуется понять, что сотрудники пытаются делать, как они пытаются это делать и как выглядит их рабочий процесс. Прежде чем вы сможете принять верное решение, вам также потребуется найти все разумные технологические реализации и очень подробно разобраться, как они работают. Верное решение имеет следующие черты:

- Позволяет людям эффективно работать.
- Обеспечивает умеренный уровень безопасности.
- Максимально просто и ясно.
- Может быть реализовано в умеренные сроки.

Пример: позвольте людям работать эффективно

На одном из сайтов электронной коммерции группа безопасности решила, что требуется снизить число сотрудников, имеющих доступ к машинам привилегированного пользователя, и что группам системных администраторов больше не будет разрешен доступ к машинам других групп с правами привилегированного пользователя. Хотя идея определения четких границ между зонами ответственности групп, в принципе, выглядела хорошо, она не учитывала общей ответственности за машины, которая требовалась, например, для работы баз данных и сложных систем электронной почты. По новой политике системные администраторы баз данных и системные администраторы почты находились в различных группах и не могли одновременно иметь доступ к одной машине с правами привилегированных пользователей. В результате обработка от 10 до 15% запросов на устранение неисправностей стала занимать в 2–3 раза больше времени, потому что нужно было задействовать несколько групп и для решения проблемы одной группе приходилось давать устные указания другой по телефону.

Как системные администраторы, так и группа безопасности хотели политики, лишавшей прав привилегированных пользователей около 100 разработчиков, которым эти права не требовались для работы и которые случайно создавали проблемы, когда совершали некоторые действия с правами привилегированных пользователей. Однако реализованная политика лишила системных администраторов возможности эффективно работать и создала враждебные отношения между системными администраторами и группой безопасности.

Лишение людей возможности эффективно работать – не лучший способ защищать интересы компании. Любая политика, которая к этому приводит, не может быть хорошей. Группа обеспечения безопасности должна была проконсультироваться с системными администраторами и инженерами, чтобы понять, как они работают и для чего им нужны права привилегированных пользователей, и создать подходящую политику.

Пример: проектирование общей среды разработки

Кристина работала в группе, которой требовалось спроектировать такую среду разработки программного обеспечения, где подразделение одной

компании трудилось бы совместно с подразделением другой компании над разработкой программного продукта. Две компании конкурировали друг с другом в других областях, поэтому им нужно было изолировать этот совместный проект от других разработок.

Первый заданный вопрос был таким: «Что нужно будет делать инженерам?» Ответ на него был следующим: им потребуется проверять код и проекты в общей системе контроля исходного кода и вне ее, писать и исполнять код, получать доступ в Интернет, отправлять и получать электронную почту и иметь доступ к внутренним ресурсам своей компании. Некоторым инженерам также потребуется возможность работать над программным обеспечением, которое не является общим с другой компанией. Инженеры одной компании будут проводить время в другой компании, работая там несколько недель или месяцев. Инженерной группе выпуска нужен был способ получения полной версии программы, когда она была готова к выпуску. Инженерам поддержки также требовался доступ к общему коду для поддержки пользователей.

Затем был задан такой вопрос: «Обеспечат ли два компьютера, один из которых будет подключен к общей сети, а второй – к частной сети компании, приемлемую модель работы для разработчиков программы?» После обсуждения с различными инженерами стало ясно, что это простое решение не будет работать с точки зрения рабочего потока. Скорее всего, если бы группа безопасности продолжила двигаться по этому пути, некоторые инженеры в конце концов подключили бы свои компьютеры к обеим сетям, чтобы работать эффективно, обходя таким образом все средства безопасности, которые обеспечила группа обеспечения безопасности. Инженерам требовалась возможность делать все на одном компьютере.

На основании полученной группой безопасности информации появилось несколько технологических решений. Каждое из них имело различные характеристики в плане скорости реализации, производительности с точки зрения пользователей и различий в рабочем потоке каждой группы. В конце концов было реализовано краткосрочное решение, которое было развернуто максимально близко к тому дню, когда компании хотели начать работать вместе, но не имело производительности, требуемой группе. Группа безопасности правильно учла ожидания и начала работать над другим решением, которое имело бы приемлемую производительность, но не могло быть реализовано в течение нескольких месяцев из-за ряда внешних факторов.

Потребовалась дополнительная работа, и первая реализация решения не была идеальной, но она удовлетворяла потребности бизнеса в предоставлении людям возможности начать проект вовремя. Кроме того, имелся план улучшения производительности и рабочей среды, поэтому в дальнейшем инженеры должны были получить возможность работать более эффективно.

11.1.3.2. Стройте безопасность при помощи жесткой инфраструктуры

Создание эффективной программы безопасности требует жесткой компьютерной и сетевой инфраструктуры, построенной с учетом безопасности. Эффективная реализация безопасности требует наличия известных, стандартных конфигураций, умения быстро и недорого строить и перестраивать безопасные системы, умения быстро устанавливать новые программы и патчи, а также способности хорошо отслеживать уровни патчей и версии. Постоянный процесс установки и модернизации машин означает наличие возможности постоянно поднимать планку защиты против атак.

Другой элемент инфраструктуры, необходимый для хорошей программы безопасности, – это процесс увольнения сотрудников из компании. Процесс увольнения обычно включает уведомление отдела кадров, который, в свою очередь, уведомляет другие отделы, например фонд заработной платы, хозяйственный отдел и отдел информационных технологий. Наиболее полезным средством в процессе увольнения является контрольный список для руководителя уходящего сотрудника. Он должен напомнить руководителю попросить вернуть ключи, карты доступа, удостоверение личности, средства аутентификации, домашнее оборудование, телефонную карту компании, мобильный телефон, пейджер, рацию и любое другое оборудование, которое может быть у человека. Контрольный список также должен напоминать руководителю о необходимости связаться с IT-подразделением в приемлемые сроки. В IT-подразделении должен быть эффективный, максимально автоматизированный процесс отключения доступа сотруднику. Эффективное отключение доступа особенно важно при увольнении сотрудника, который считает себя обиженным компанией. Более подробно этот процесс рассмотрен в главе 36.

Пример: безопасность за счет хорошей инфраструктуры

Эту историю мы чаще всего рассказываем, когда пытаемся объяснить, как можно снова и снова максимально эффективно использовать методы, представленные в предыдущих главах, и как недостаточное внимание к этим основным принципам делает реализацию безопасности очень дорогой или невозможной.

Небольшая группа консультантов по безопасности была привлечена на успешный сайт интернет-коммерции, который подвергся взлому. Консультанты начали по очереди восстанавливать машины. Однако сайт рос так быстро, что вокруг них постоянно устанавливались новые машины. Каждую из них взламывали быстрее, чем группа могла восстановить ее и заблокировать доступ новых злоумышленников. Ситуация становилась безвыходной.

После некоторого анализа консультанты поняли, что принципиальной проблемой было отсутствие в компании системы для автоматизации за-

грузки, модернизации или обновления операционной системы. Все делалось вручную, машины обслуживались последовательно, а не одновременно, не имелось даже какой-либо документации на процедуры или контрольного списка. Естественно, было невозможно выполнить единообразно все процессы на всех машинах.

Для обеспечения безопасности этого сайта консультантам пришлось воспользоваться совершенно другой стратегией: перестать исправлять отдельные проблемы, а вместо этого построить инфраструктуру, обеспечивающую автоматическую загрузку операционной системы, модернизацию и установку обновлений. Хотя эти системы обычно не считаются объектом ответственности группы безопасности, консультанты поняли, что, если они не построят ее, этого не сделает никто. Когда инфраструктура была создана, компания могла перезагрузить все машины, обслуживающие сайт интернет-коммерции, устраняя таким образом нарушителей и обеспечивая правильные безопасные конфигурации всех машин и блокировку новых злоумышленников.

В компании также не хватало других элементов инфраструктуры – в том числе централизованной системы регистрации событий, синхронизации времени и консольных серверов, – что затрудняло быстрое развертывание инфраструктуры безопасности. Фактически консультанты по безопасности стали группой создания инфраструктуры, потому что они не могли установить системы безопасности без полной инфраструктуры.

Когда группа обеспечения безопасности завершила работу, в компании была практически новая, безопасная и надежная коммерческая инфраструктура. И хотя казалось, что это сделало стоимость первоначального запроса («обеспечить безопасность сайта») очень высокой, крупный выигрыш в эффективности и надежности принес компании большую выгоду.

Реализация новых политик безопасности не была бы такой дорогой, если бы у компании уже имелась базовая инфраструктура сайта.

Важно построить базовую системную и сетевую инфраструктуру, и сделать это правильно, потому что от нее зависят другие аспекты, например безопасность.

В предыдущих главах этой книги подробно рассмотрена базовая инфраструктура, которая обеспечивает простоту обслуживания, воспроизводимость и высокую эффективность. Эти элементы являются опорными. Без них окажется, что вы бесполезно тратите время и силы, решая одни и те же проблемы.

11.1.3.3. Знайте об актуальных атаках

Профессионал в области безопасности должен уметь справляться с распространенными типами атак и знать способы защиты систем компании от этих атак. Это предполагает ежедневное чтение нескольких рассылок электронной почты и информации на соответствующих веб-сайтах. Вам нужно отслеживать бюл-

летени безопасности поставщиков и сводки данных организаций, исследующих вопросы безопасности, таких как:

- *Bugtraq*: *http://www.securityfocus.com* (Levy, нет даты)
- *CERT/CC*[1]: *http://www.cert.org*
- *Отдел наблюдения компьютерных инцидентов (Computer Incident Advisory Capability – CIAC)*: *http://www.ciac.org*
- *Австралийская группа реагирования на компьютерные происшествия (Australian Computer Emergency Response Team, AUSCERT)*: *http://www.auscert.org.au*

Информационные рассылки по электронной почте обычно предоставляют эксплойты, которые вы можете протестировать на своих системах, чтобы оценить, являются ли они уязвимыми. Эти рассылки часто информируют о новой уязвимости быстрее других, потому что в этом случае не нужно разрабатывать и тестировать патч, прежде чем опубликовать новость. Профессионал в области безопасности должен стараться максимально быстро узнавать о новых уязвимостях, чтобы оценить, как лучше всего защитить системы компании и как проверять наличие атак, использующих эту уязвимость.

Среднее время до проведения атаки

Средства для сканирования узлов или целых сетей широко используются потенциальными злоумышленниками с конца 1990-х годов. Узел, впервые подключенный к Интернету, будет сканирован и атакован в течение нескольких минут. Прошли времена, когда злоумышленники в один день сканировали сеть и возвращались, чтобы ее атаковать, через несколько недель.

В 1998 году друг Кристины провел в свой дом новое DSL-соединение и посмотрел, сколько времени пройдет, прежде чем его небольшая сеть будет просканирована. Прошло менее двух часов. К счастью, прежде чем подключаться, он обеспечил безопасность своих машин и установил все самые свежие патчи, потому что прочел много информации в рассылках по вопросам безопасности.

Теперь машины атакуют в течение нескольких минут. Если учесть, сколько времени занимает установка средств обеспечения безопасности, машина, только что введенная в действие, будет атакована до того, как эти средства будут загружены.

Новые машины должны вводиться в эксплуатацию в сетях, отделенных межсетевым экраном от Интернета и по возможности от больших корпоративных сетей. Никогда не используйте небезопасную сеть для подключения новой машины.

[1] Организация, ранее известная как Группа реагирования на компьютерные происшествия/Координационный центр, теперь известна как CERT/CC, зарегистрированная услуга университета Карнеги Меллон.

Обеспечьте безопасность узлов перед выходом в сеть

Издательская компания, которая выпускала как бумажный, так и сетевой вариант своего еженедельного журнала, работала над новым веб-сайтом. На следующий день ждали консультанта по безопасности, который должен был обеспечить безопасность машин, используемых для веб-серверов. Одна сотрудница группы разработчиков была нетерпелива и, не дожидаясь консультанта, подключила машины напрямую к Интернету. Через несколько часов она заметила, что на одной из машин происходит что-то странное, и поняла, что та была взломана. Она не могла понять, как кто-то мог найти машину, потому что она даже еще не имела имени на внешнем DNS-сервере компании. Машина была просканирована, а уязвимости в операционной системе и конфигурации были определены и использованы в течение нескольких часов после подключения. Использованные уязвимости были хорошо известны, и этого легко можно было избежать. Так как сотрудница не имела отношения к безопасности, не получала бюллетеней безопасности и не читала соответствующей информации, она не имела представления ни о том, какие уязвимости существуют и насколько они опасны, ни о том, как широко распространено автоматическое сканирование и использование после определения уязвимостей пакетов для взлома.

11.1.3.4. Применяйте аутентификацию и авторизацию

Один из важнейших элементов системы безопасности – это мощная система аутентификации с уникальным идентификатором для каждого человека и без учетных записей, используемых несколькими людьми одновременно. Совместно с системой аутентификации работает система авторизации, которая указывает уровень доступа, разрешенный пользователю. **Аутентификация** дает человеку идентификатор, а **авторизация** определяет, что ему разрешено делать.

Ролевая учетная запись – это учетная запись, которая предоставляет людям права на выполнение одной или более задач, недоступных для выполнения с правами обычной учетной записи. Типичные примеры включают роли системного администратора, администратора базы данных и администратора веб-сайта. Общие учетные записи, даже общие ролевые учетные записи, нужно исключить. Например, ролевая учетная запись может называться `dbadmin` и любой человек, которому нужно управлять записями баз данных, способен воспользоваться для этого данной учетной записью. Пароль известен всем, кому нужен доступ. Общие учетные записи затрудняют отчетность, если не делают ее вообще невозможной. В случае возникновения проблем может оказаться, что невозможно найти виновного. Также в этом случае может быть гораздо труднее полностью отключить доступ человеку, уходящему из компании. Системные администраторы вынуждены проверять, к каким ролевым учетным записям человек имел доступ, и причинять неудобства другим, меняя пароли на этих учетных записях.

В большинстве операционных систем есть другие механизмы обеспечения одного уровня доступа нескольким людям, которые идентифицируются как отдельные субъекты. Проверьте возможности своей системы, прежде чем принять решение воспользоваться общей учетной записью. Например, людей, которым

нужен доступ к учетной записи `dbadmin`, можно вместо этого добавить в группу `dbadmin`, которая позволяет им действовать в качестве администратора базы данных. Учетная запись `root` в UNIX – ролевая учетная запись, как и `Администратор` в Windows. Лучше дать кому-то права `PowerUser` в Windows на необходимых машинах или права `Администратор домена`, если человеку нужен привилегированный доступ на всех мащинах. Системы жесткой аутентификации обычно затрудняют создание общих учетных записей.

Система жесткой аутентификации предоставляет вам бóльшую степень уверенности, что человек, которого компьютер считает прошедшим аутентификацию, действительно этот человек, а не просто кто-то, использующий его учетные данные (пароль). Например, система жесткой аутентификации может быть биометрическим механизмом, таким как сканер отпечатка пальца или глаза, или системой, основанной на карманных устройствах, для которой человеку нужно физическое устройство (идентификатор), а также секретные данные, например PIN-код, который он помнит. Человек, который передает кому-то свое физическое устройство, больше не имеет доступа, что часто является достаточным затруднением для совместного использования. Если устройство будет похищено, то похититель не будет знать секретный PIN-код. Другими словами, система карманных идентификаторов требует чего-то, что у вас есть, и чего-то, что вы знаете.

Карманный идентификатор проще носить, если у него есть другие функции. Другими словами, если это еще и брелок, люди будут носить его с собой, потому что он будет полезен им не только для загрузки компьютеров. Это также привязывает его к чему-то, что важно для человека лично, к дому или машине, снижая таким образом вероятность передачи другому лицу.

Пример: более жесткая безопасность выявляет плохое поведение

После перехода с паролей на HHA в одной компании начались жалобы в группе продаж. Многие люди были недовольны тем, что они больше не могут давать свои имя пользователя и пароль клиентам и потенциальным клиентам, чтобы те могли опробовать продукцию компании в корпоративной сети, прежде чем принять решение ее купить. Любой, кто передавал другому человеку HHA, не мог отправлять и получать электронную почту до его возвращения.

Группе обеспечения безопасности пришлось рассказать людям о проблемах с передачей другим лицам доступа к корпоративной сети и помочь им организовать лучшие способы для пробных версий клиентов, например передачу оборудования или специальный ограниченный VPN-доступ для клиентов.

Системы жесткой аутентификации обычно не являются гибкими. Но иногда в экстренных случаях требуется небольшая гибкость. Время от времени в механизме жесткой аутентификации что-то может работать неправильно и вам понадобится способ аутентификации людей по телефону, особенно если они путешествуют. Например, кто-то может потерять или сломать физическое устройство – HHA или переносное биометрическое устройство, – необходимое для аутен-

тификации. Вам нужно подготовиться к такой возможности при первоначальной установке системы жесткой аутентификации.

При создании учетной записи дайте человеку заполнить форму, содержащую вопросы об информации, которая может быть использована для аутентификации по телефону. Например, человек может назвать свой размер обуви, любимый фрукт, магазин, в котором была сделана конкретная покупка, место, где он встречал новый 2000 год, любимый предмет в школе или что-то, что может быть проверено в компании, например кто находится в соседнем офисе или за соседним столом. Для человека, который может таким образом обеспечить успешную аутентификацию по телефону, должен быть доступен другой механизм, дающий ему временный доступ к системам, пока проблема не будет решена. Например, многие системы позволяют пользоваться обычным паролем в течение 24 ч или достаточно долгое время до замены HHA.

Общая голосовая почта

В одной быстрорастущей компании потребительского рынка группа сотрудников совместно использовала один телефон и голосовой почтовый ящик. Однажды этим телефоном и голосовым почтовым ящиком начал пользоваться новый сотрудник и спросил пароль к голосовой почте. В ответ один из других сотрудников этой группы перевернул трубку и показал на номер, наклеенный на другой стороне трубки. Таким образом, любой мог найти пароль и прослушивать потенциально конфиденциальную информацию, оставленную на голосовой почте. Многие компании считают голосовую почту безопасным способом передачи важной информации, такой как новости о потенциальном новом клиенте, первоначальные пароли, объявления для персонала, ориентацию продукции и другую информацию, попадание которой к ненужным людям может принести компании ущерб.

В той же компании вместо установки соответствия уровней авторизации с прошедшими аутентификацию сотрудниками использовались общие учетные записи для административного доступа. Конечным результатом была книга с именами учетных записей и паролями администратора для каждого узла. Кто-нибудь с правами доступа к паролю для одного узла мог легко просмотреть пароли для других узлов, а затем получить анонимный доступ к другим машинам, используя административные учетные записи. Недостаток отчетности из-за общих учетных записей – это плохо, как и наличие книги с паролями, при помощи которой люди легко могут получить больший уровень доступа, чем им положено.

Данная компания пострадала от нескольких взломов, и применение общих ролевых учетных записей затрудняло определение и отслеживание нарушителей. Также эта система была не так проста в применении, как система, предоставлявшая бóльшие права доступа на основе уникального личного маркера аутентификации, потому что каждому требовалось периодически заглядывать в книгу паролей. Авторизация, основанная на аутентификации каждого сотрудника, была бы проще в использовании и безопаснее.

Общие ролевые учетные записи затрудняют идентификацию

Компания, в которой применялась общая учетная запись с правами привилегированного пользователя, пострадала от нескольких взломов, когда главный системный администратор долго отсутствовал и вместо него работал неопытный системный администратор. Главный системный администратор был практически недоступен через удаленное соединение, и компания обратилась к помощи опытного системного администратора, который работал на другой должности.

В определенный момент главный системный администратор испугался, что учетная запись привилегированного пользователя была взломана, когда увидел логи доступа к этой учетной записи через SSH с неизвестной машины. Оказалось, что с неизвестной машины этой учетной записью пользовался системный администратор, который оказывал помощь. Если бы группа системных администраторов была гораздо больше, было бы трудно обнаружить подозрительный доступ и отследить его до источника, если вообще возможно. Отсутствие возможности обнаружить подозрительный доступ может привести к тому, что машины останутся взломанными, когда проблема, казалось бы, уже решена. Отсутствие возможности отследить этот доступ до его (правомерных) источников может привести к большой трате сил и бесполезным расходам на перестройку ключевых машин, которые не были взломаны. Такой ситуации лучше избегать и не использовать общие ролевые учетные записи.

В этих примерах применялись общие учетные записи, поскольку казалось, что это проще. Однако в результате система оказывалась менее безопасной и более сложной в использовании, особенно когда людям приходилось специально заходить под своими ролевыми учетными записями для выполнения большого количества действий. Ценой очень малых усилий индивидуальные учетные записи могли бы предоставить доступ к ресурсам в соответствии с требованиями, повышая безопасность системы и возможность отслеживать деятельность в ней, а также упрощая доступ системным администраторам, которым он был необходим. Безопаснее и проще в использовании – и все ценой небольших заблаговременных усилий.

11.1.3.5. Матрица авторизации

Аутентификация подтверждает личность. Авторизация – это то, что позволено делать человеку. Например, обычному пользователю нужна возможность читать его собственную электронную почту, но не почту других людей. Некоторые люди должны иметь возможность чтения конкретной базы данных, меньшее их число – обновлять данные, и только у нескольких администраторов должна быть возможность изменять схему базы данных.

Использование **матрицы авторизации**, основанной на функциях подразделений компании, категориях системы и классах доступа (табл. 11.1), более удобно, чем определение этой политики в текстовой форме. Матрица авторизации описывает уровень доступа данной группы людей к определенному классу машин.

Таблица 11.1 Матрица авторизации

Подразделение	Машины							
	Разр	ВИ	Фин	Рес	Кадр	Эксп	Инф	Без
Разработчики	W	R		R				
Выпускающие инженеры	R	W		R				
Финансовое			W	R				
Кадровое				R	W			
Эксплуатационное				R		W		
Системные администраторы	A	A	A	A	A	A	A	
Безопасность	A	A	A	A	A	A	A	A

Разр – разработчики; ВИ – выпускающие инженеры; Фин – финансы; Рес – корпоративные ресурсы (внутренняя сеть и т. д.); Кадр – отдел кадров; Эксп – эксплуатация/производство; Инф – инфраструктура (почтовые серверы, серверы авторизации и т. д.); Без – безопасность (межсетевые экраны, обнаружение вторжений, жесткая аутентификация); A – административный доступ, R – доступ на чтение, W – доступ на запись.

Такая политика должна разрабатываться совместно с руководством и представителями всех подразделений компании. После того как это будет сделано, система авторизации должна быть связана с системой аутентификации, которая реализует политику. Набор идентификаторов и информация, записанная в системах аутентификации и авторизации, являются одним из пространств имен. Управление этим и другими пространствами имен рассмотрено более подробно в главе 8.

Матрица авторизации экономит время

Том устроился в компанию, в которой велись продолжительные дискуссии о повышении безопасности определенных сетей. В течение предыдущих двух месяцев компания не могла принять решение о том, какие сети должны иметь доступ к определенным службам.

До этого момента обсуждение велось устно и не приближалось к консенсусу. Том выслушал мнения людей и подумал, что в них много общего, но, так как дискуссия развивалась и позиции менялись, он не мог точно сказать, где было согласие, а где – разногласия.

На одном собрании Том сказал: «О, у меня есть средство, которое решит эту проблему». Люди подумали, что он достанет бейсбольную биту. Вместо этого он открыл программу электронных таблиц и нарисовал таблицу.

В строках он написал сети, а в столбцах – различные службы. Он начал заполнять отдельные ячейки там, где, как он думал, мнения были согласованными. Затем он спросил у группы, все ли он понял правильно. Группа предложила заполнить еще несколько ячеек. Оказалось, что лишь несколько ячеек оказались незаполненными, потому что по ним не было достигнуто соглашение.

Том предложил начать с имеющейся политики, а не держать очень дорогие аппаратные межсетевые экраны в коробках еще два месяца. В незаполненных ячейках до заполнения таблицы решено было указать «Нет доступа».

В течение недели, которая потребовалась на установку оборудования, руководство просмотрело таблицу и разрешило установить политику. Эти люди не очень хорошо разбирались в технике, но матрица позволила им принять решение без необходимости разбираться в технологиях, и они смогли разрешить противоречие между системными администраторами.

К тому времени, как было готово оборудование, таблица была заполнена. Инженер, который устанавливал межсетевой экран, должен был лишь убедиться, что конфигурация точно отражала таблицу. Затем различные системные администраторы могли проверять межсетевой экран, сравнивая конфигурацию с таблицей.

После двух месяцев дискуссий весь проект был завершен за неделю, потому что использовалось правильное средство.

11.1.3.6. Выбирайте правильные продукты и поставщиков

При выборе продукта для любой задачи, в которой важна безопасность, вы должны действовать правильно. Оценка продукта с точки зрения безопасности отличается от оценки продукта, для которого безопасность не является приоритетной.

Продукт, **чувствительный к безопасности**, обладает по крайней мере одной из следующих характеристик:

- Используется любой третьей стороной, имеющей ограниченный уровень доступа к этой системе или к сети (сетям), к которой она подключена.
- Является частью системы аутентификации, авторизации или контроля доступа.
- Доступен из Интернета или любой небезопасной сети.
- Имеет доступ в Интернет или любую небезопасную сеть.
- Предоставляет доступ с аутентификацией к важным данным или системам, например к данным о выплатах.

При оценке чувствительного к безопасности продукта вам также нужно учитывать несколько дополнительных факторов. Например, вам требуется некоторая степень уверенности в безопасности продукта. Вы должны учитывать несколько критериев простоты использования, влияющих на безопасность. Кроме того, вам нужно иметь в виду вопросы текущего обслуживания и направленность поставщика, а также ряд менее специфичных факторов, например вопросы функциональности и интеграции.

- *Простота.* Простые системы обычно более надежны и безопасны, чем сложные. Например, система электронной почты, лишь отправляющая и получающая сообщения, не так сложна, как система, которая также хранит адресные книги и записи и, возможно, имеет встроенный календарь. Более простая система электронной почты может быть улучшена при помощи других программ, которые предоставляют дополнительную функцио-

нальность, если она нужна. Несколько небольших, простых компонентов, взаимодействующих друг с другом, скорее всего, будут иметь меньше проблем с безопасностью, чем одна крупная, сложная система. Чем сложнее система, тем труднее детально ее протестировать и тем выше вероятность, что она будет иметь непредвиденные проблемы, которые могут быть использованы злоумышленником.

- *Безопасность.* Почему вы считаете, что этот продукт достаточно безопасен? Ознакомьтесь с продуктом и узнайте, кто его ведущие дизайнеры и программисты. Вы знаете их (о них)? Являются ли они авторитетными людьми в отрасли? Насколько хорошо работали их предыдущие продукты и насколько они были безопасны? Как продукт решает известные проблемы? Например, вы можете спросить, как межсетевой экран организует доставку почты, которая представляет собой область с традиционно большим количеством проблем безопасности. Еще одна служба, традиционно подверженная проблемам с безопасностью, – это FTP, и не только реализации FTP-серверов, но и то, как межсетевые экраны работают с протоколом. Просмотрите информационные бюллетени по безопасности за пару лет и изучите область, где проблемы постоянно повторяются.
- *Открытый исходный код.* Является ли данный продукт продуктом с открытым исходным кодом? В двух словах, дебаты об открытом исходном коде сводятся к следующему: если исходный код доступен, злоумышленники могут найти уязвимости и воспользоваться ими, но, с другой стороны, он постоянно проверяется многими людьми, проблемы находятся быстрее, патчи появляются раньше и вы всегда можете сами изменить его, если это необходимо. Безопасность закрытого исходного кода за счет его неизвестности сомнительна: это лишь кажется, что сохранение метода в тайне делает его безопасным, даже когда он принципиально небезопасен. Безопасность за счет неизвестности не работает, злоумышленники находят уязвимости в любом случае.
- *Простота использования.* Легко ли понять и проверить конфигурацию? Насколько легко случайно настроить приложение так, что оно станет небезопасным? Как взаимодействуют компоненты? Как изменение конфигурации в одной области влияет на другие области. Например, если в межсетевом экране, который имеет и прокси, и фильтры пакетов, отдельные правила конфигурации пытаются управлять чем-то как на сетевом уровне (фильтр пакетов), так и на уровне приложения (прокси), правила какого уровня применяются первыми и к чему это приведет? Обнаруживает ли приложение конфликты конфигурации? Сколько времени занимает обучение новых сотрудников работе с продуктом?
- *Функциональность.* Продукт должен предоставлять только те функции, которые вам нужны. Избыточная функциональность может быть источником проблем, особенно если ее нельзя отключить.
- *Связь с поставщиком.* Для продукта, чувствительного к безопасности, очень важны патчи и обновления. В большинстве случаев вам также потребуется возможность сообщать о проблемах поставщику и иметь все основания ожидать быстрого устранения или временного решения проблемы. Если у поставщика есть бесплатная версия коммерческого продукта, то вы, скорее всего, получите лучшее обслуживание при пользовании коммерческой версией. Насколько поставщик уделяет внимание безопасности? Выпускает ли он патчи для устранения проблем его продуктов с безопасно-

стью? Каков его механизм уведомления пользователей о проблемах безопасности?

- *Интеграция.* Насколько хорошо этот продукт сочетается с вашей остальной сетевой инфраструктурой?
  - Будет ли он использовать имеющуюся систему аутентификации?
  - Как он загружает сеть и остальные ключевые системы?
  - Если ему нужно связываться с другими системами или людьми через межсетевой экран, то есть ли у межсетевого экрана нормальная поддержка его протоколов? Открытые протоколы обычно поддерживаются, собственные протоколы разработчиков часто не поддерживаются.
  - Использует ли продукт другие протоколы для связи, например направляет протокол мгновенных сообщений через HTTP? Это может затруднить контроль доступа к новому приложению вне зависимости от того, используется ли на самом деле этот протокол[1]. Новые службы должны иметь собственные порты.
  - Можно ли отправлять его логи на центральный узел?
  - Наличие каких сетевых служб ему требуется и предоставляете ли вы их?
  - Работает ли он под операционной системой, которая уже поддерживается и хорошо изучена в компании?
- *Расходы на содержание.* Сколько времени занимает настройка этой программы? Имеет ли она возможность автоматической загрузки, которая может помочь в стандартизации настроек и ускорить время установки? Какие объемы ежедневного обслуживания требуются системе, требует ли она серьезной доработки? Знакомы ли люди в вашей организации с этой системой? Высока ли вероятность, что люди, которых вы нанимаете, будут знакомы с ней, или вам придется их обучать? Насколько трудно будет обеспечить удобную работу нового сотрудника с вашей конфигурацией?
- *Перспективы.* Насколько масштабируем продукт и каковы возможности масштабирования при достижении максимальной загрузки? В каком направлении разработчик развивает продукт и соответствует ли оно направлению вашей компании? Например, если в вашей компании все основано на UNIX и вы практически не имеете дела с Windows и вряд ли будете двигаться в этом направлении, то продукт компании, ориентированной главным образом на Windows, – не лучший выбор. Возможно ли прекращение разработки продукта в скором времени? Как долго поддерживаются версии? Как часто выходят новые релизы? Как продукт принимается рынком? Выживет ли он под давлением рынка? Распространенность продукта на рынке также упрощает наем людей, которые знают продукт.

11.1.3.7. Внутренние проверки

Проверка, проводимая группой, входящей в компанию, называется **внутренней проверкой**. Мы считаем, что нужно использовать как внутренние, так и сторон-

[1] Веб-продукт или продукт с веб-интерфейсом, очевидно, должен использовать HTTP для связи. Однако продукт, отправляющий информацию между клиентом, который не является веб-броузером, и сервером, который не является веб-сервером, не должен использовать HTTP и порт 80.

ние проверяющие группы; внешние проверки будут рассмотрены далее в разделе 11.1.4.3.

Мы определяем **проверку** в очень широком смысле, чтобы охватить все перечисленные вопросы:

- Проверка соответствия систем безопасности политикам и структуре.
- Проверка списков сотрудников и подрядчиков по базам данных аутентификации и авторизации.
- Физические проверки серверных, кабельных и телекоммуникационных шкафов на наличие инородных устройств.
- Проверка наличия последних обновлений по безопасности на важнейших машинах.
- Сканирование важнейших сетей с целью проверки предоставляемых услуг.
- Запуск сложных, глубинных атак против конкретных областей инфраструктуры с четко определенными критериями успеха и ограничениями.

Мы рекомендуем, чтобы группа внутренней проверки выполняла эти задачи, и они могут быть выполнены более тщательно и легко при использовании внутренней информации компании:

- *Ведение и обработка логов.* Логи, особенно логи чувствительных к безопасности машин и приложений, являются важным источником информации о безопасности. Логи могут помочь группе безопасности отследить, что случилось во время атаки. Их можно анализировать для помощи в обнаружении атак и определения масштабов и серьезности атаки. С точки зрения безопасности логов не может быть слишком много. С практической точки зрения бесконечные логи требуют бесконечного дискового пространства и в них невозможно искать важную информацию. Логи должны обрабатываться компьютером для извлечения полезной информации и архивироваться на определенный период, чтобы обеспечить возможность повторного просмотра в случае обнаружения происшествия. Все логи, важные с точки зрения безопасности, должны собираться в одной централизованной точке, чтобы их можно было совместно обрабатывать и сравнивать информацию с различных машин. Логи, важные с точки зрения безопасности, не должны оставаться на чувствительных к безопасности машинах, потому что они могут быть удалены или изменены злоумышленником, атакующим эти машины. Центральный узел логов должен быть очень хорошо защищен, чтобы обеспечить целостность логов.
- *Проверка структуры.* Рассмотрите все способы, при помощи которых вы можете проверить ваши сети и важные системы на наличие аномалий. Видите ли вы в сети какие-либо странные маршруты, например идущие в непонятном направлении или трафик из неожиданных источников? Попробуйте использовать метод war-dialing по всем телефонным номерам вашей компании, чтобы посмотреть, нет ли ответов модема с каких-либо неожиданных номеров[1]. Проверьте, какие машины и службы видны из публич-

[1] Метод war-dialing предполагает наличие программы, которая набирает все номера в заданном списке, что может включать полный обмен данными, и записывает все номера, которые отвечают звуком работы модема. War-dialing также может выполнять запись приветствия машины на другом конце или попытку загрузки с определенными комбинациями имен пользователя и паролей с записью результатов.

ных сетей, чтобы убедиться, что не появилось ничего нового или неожиданного. Нет ли активного удаленного доступа к сети со стороны кого-то, находящегося в офисе? Системы обнаружения вторжений (IDS – Intrusion Detection System) упрощают обнаружение некоторых аномалий этого типа, а также других типов атак.

- *Проверка каждого проекта.* Периодически проверяйте каждый реализованный проект в области безопасности, чтобы убедиться, что конфигурация не была существенно изменена. Убедитесь, что она соответствует проектным спецификациям и согласована с соответствующими политиками. Также воспользуйтесь этой возможностью, чтобы пообщаться с людьми, которые применяют эту систему безопасности, чтобы узнать, удовлетворяет ли она их потребности и нет ли каких-то новых требований.
- *Физические проверки.* Проверяйте объекты, которые являются ключевыми точками в компьютерной, сетевой или телекоммуникационной инфраструктуре. Ищите дополнительные устройства, возможно скрытые, которые могут перехватывать и записывать или передавать данных. Такими объектами являются вычислительные центры, шкафы с сетевым и телекоммуникационным оборудованием, помещения для видеоконференций, кабели между такими помещениями, а также проводные и беспроводные соединения между зданиями.

Нарушения физической безопасности

Группа безопасности в крупной транснациональной корпорации не проводила регулярных физических проверок вычислительных центров и шкафов с коммуникационным оборудованием. Однажды из компании, которая поставляла и обслуживала телефонную станцию, пришел сотрудник для проведения каких-то работ на станции и обнаружил подключенное к ней устройство. Дальнейшее расследование показало, что устройство перехватывало всю телефонную связь в здании и по внешним линиям и передавало информацию за пределы компании. Оказалось, что кто-то, одетый в форму сотрудника телефонной компании, пришел в здание и сказал, что ему нужно подключить какие-то новые линии к телефонной станции. Никто не связался ни с телекоммуникационным, ни с сетевым отделом, чтобы узнать, ждали ли сотрудника телефонной компании. После этого происшествия группа безопасности пересмотрела свою политику и больше никто не допускался в эти помещения без сопровождения и разрешения телекоммуникационного либо сетевого отдела. Кроме того, стали проводиться регулярные физические проверки всех компьютерных и коммуникационных помещений и кабелей между ними.

11.1.4. Вопросы руководства и организации

Есть ряд областей, в которых группе безопасности особенно нужна поддержка руководства. Поддержание достаточного для размера компании уровня обеспечения персоналом с соответствующими функциями в группе – одна из таких областей. Руководитель группы безопасности также может помочь в координации с другими руководителями системных администраторов для создания

группы реагирования на происшествия, подготовленной к экстренным ситуациям. Установление отношений с внешней проверяющей компанией и создание графика ее работы, соответствующего потребностям остальной компании, – еще одна задача, которую обычно выполняет руководитель группы безопасности. Мы рассмотрим несколько подходов для успешной организации безопасности в других подразделениях компании.

11.1.4.1. Ресурсы

Группе безопасности нужен доступ к различным ресурсам. Один из ключей к успешной программе безопасности – наличие большого количества связей в отрасли, а следовательно, информированность о действиях других компаний и мнениях других людей о совершенных системах. За счет своих связей профессионалы в области безопасности также узнают о происхождении атак раньше других, что позволяет им быть на шаг впереди и максимально подготовиться. Это также позволяет профессионалам в области безопасности оценивать работу компании в сравнении с другими. Тратит ли компания на безопасность слишком много или слишком мало? Испытывает ли она нехватку некоторых важных политик? Группа безопасности также может узнать, с чем столкнулись другие компании, пытаясь внедрить некоторые новые технологии, и какова была рентабельность инвестиций. Был ли у кого-то особенно позитивный или негативный опыт в работе с новым продуктом, рассматриваемым группой безопасности?

Связи устанавливаются за счет регулярного посещения конференций и участия в деятельности специальных межфирменных рабочих групп по безопасности. Профессионалы в области безопасности должны иметь известность и доверие среди своих коллег, чтобы быть в курсе дел в отрасли.

Группе безопасности требуются люди с разными навыками. В небольшой компании всю работу может выполнять один человек, возможно, с небольшой помощью руководства. Однако в более крупной компании руководитель группы безопасности должен нанимать людей на ряд должностей. Некоторые из этих должностей требуют особых навыков и личностных качеств. Эти должности включают разработчика политик, архитектора безопасности, конструктора, операторов, аудитора, менеджера рисков и специалистов по реакции на происшествия.

- *Разработчик политик* отвечает за написание корпоративных политик и, следовательно, должен иметь связи в ключевых подразделениях компании и входить в некоторые многофункциональные группы, чтобы обсуждать политики с руководителями, юридическим отделом и отделом кадров. Разработчик политик должен уметь определять, какие политики требуются компании, и обеспечивать в компании их поддержку, особенно на уровне высшего руководства. Разработчик политик должен знать, как обстоят дела с политиками у других компаний, особенно той же отрасли, и что считается наилучшим. Он должен быть в курсе ситуации в бизнесе и знать дух компании, чтобы определить, что приемлемо для компании.
- *Архитектор безопасности* является представителем группы безопасности перед другими сотрудниками компании и должен входить в многофункциональные группы в компании. Этот человек отвечает за то, чтобы группа безопасности была в курсе происходящего в компании, за выявление проектов, в которых группе потребуется участие, а также за выяснение требований, нужд бизнеса и ключевых людей. Кроме того, архитектор безопасности проектирует систему безопасности и наблюдает за ситуацией с безопасно-

стью в компании, в том числе за тем, какая инфраструктура может помочь группе и компании. Этот человек должен заниматься связями с поставщиками, отслеживанием технологий, продуктов и перспектив, а также решать, когда компания должна переходить на новую технологию и должна ли вообще.

- *Конструктор* реализует проекты архитектора и работает вместе с ним над оценкой продуктов. Конструктор должен вступать в многофункциональные группы по проектам, когда он будет заниматься построением конкретной среды для этого проекта. Также конструктор должен понимать требования бизнеса, выносить на обсуждение проблемы и предлагать альтернативные решения. Этот человек документирует вопросы установки и эксплуатации созданных систем и обучает операторов работе с ними. Конструктор находится на ступень выше оператора и должен обсуждать перспективы, технологии и продукты с архитектором, а также доводить до него любые требования, которые могут появиться в будущем.
- *Операторы* обеспечивают ежедневную работу инфраструктуры безопасности. Этих людей обучает конструктор, и они обращаются к нему по вопросам, которые не могут решить самостоятельно. В крупных компаниях оператор, обеспечивающий работу в режиме 24/7, может выполнять двойную функцию, работая также в качестве оператора безопасности, отвечая на уведомления и отчеты системы мониторинга логов или других IDS. Операторы имеют дело с ежедневными задачами системы аутентификации и авторизации, например с потерянными или сломанными маркерами, новыми сотрудниками или подрядчиками и увольнениями из компании. С этими людьми беседуют остальные системные администраторы в случае подозрений о проблемах в элементах инфраструктуры безопасности. По возможности операторы должны помогать конструктору в построении инфраструктуры.
- *Аудитор* может быть сотрудником компании или членом сторонней консалтинговой группы. Компания может использовать аудиторов обоих типов в различных целях. Аудитор строит программу[1] проверки безопасности компании на предмет ее соответствия требованиям, тесно работая вместе с группой безопасности и руководством, чтобы определить, какие конкретные области должны быть протестированы глубоко. Такое тестирование может включать социальную инженерию, которая обычно является наиболее слабым звеном в защите любой компании. Задачи аудиторов, особенно внешних, рассмотрены далее в этом разделе.
- *Менеджер рисков* осуществляет техническое руководство со стороны бизнеса. Менеджер рисков оценивает технические требования с целью подсчета рисков для компании, связанных с отклонением от стандартов политики, определяет, позволять ли такие отклонения или требовать перестройки решения, чтобы их не допускать, а затем объясняет приемлемые риски аудиторам (внутренним или внешним). Таким требованием может быть предоставление анонимного FTP-доступа к серверу, разрешение сторонним провайдерам доступа к конкретному внутреннему ресурсу тем или иным способом или установление менее жесткой политики использования паролей на определенном устройстве. В крупных компаниях может быть много менеджеров рисков, ориентированных на различные подразделения компании, с поддержкой большой структуры управления рисками.

---

[1] Здесь термин «программа» означает систему проектов и служб для выполнения требований, а не компьютерную программу.

Социальная инженерия

Социальная инженерия – это искусство убеждения людей предоставить вам доступ к какому-либо объекту, к которому вам доступ не положен, обычно используя некоторые данные, собранные заранее. Например, вы узнаете имя нового инженера по сбыту и обращаетесь в службу поддержки от имени этого инженера с целью узнать номер телефона. Затем вы звоните в службу поддержки от имени того же или другого человека, говорите, что потеряли свой HHA, но вам нужен доступ, и просите службу поддержки предоставить вам какой-либо другой способ аутентификации, например пароль. Большинство людей охотно соглашаются помочь новому сотруднику, социальная инженерия пользуется людской отзывчивостью.

- *Группа реагирования* на происшествия вступает в дело, когда происходит реальное вторжение или есть подозрение на него. Кроме того, эта группа периодически собирается для обсуждения процедур реагирования на происшествия. В зависимости от размера компании и группы безопасности эта группа, скорее всего, будет состоять из системных администраторов компании, как и группа безопасности. В оставшееся время у этой группы есть другая функция в отделе системных администраторов, иногда в рамках группы безопасности, а иногда и вне ее.

11.1.4.2. Реагирование на происшествия

В данном разделе мы рассмотрим создание процесса урегулирования инцидентов в области безопасности за счет подготовки эффективной реакции на происшествия и выяснения, как политики различных компаний, связанные с реагированием на происшествия, влияют на работу группы.

Чтобы справиться с происшествием, люди должны быть подготовлены. Нельзя формировать группу во время кризиса. Парадоксально, но лучшее время для создания группы и процессов – когда вы считаете, что они вам не нужны.

«На первой полосе»

Чем крупнее становится компания, тем выше вероятность, что она будет обеспокоена скорее ударом по репутации от происшествия, чем потерей данных или производительности в результате инцидента. Удар по репутации связан с недостаточно эффективным урегулированием инцидента. Если происшествие будет урегулировано нормально, то оно приведет к появлению небольшой заметки в газете. Если же урегулирование будет неправильным, то вы попадете на первые полосы газет. Это может повлиять на курс акций компании и доверие клиентов.

При организации группы реагирования на происшествия вам сначала нужно решить, как вы будете предавать группе сообщения о возможных инцидентах. Для этого вам нужно обратить внимание на ваши механизмы сообщения о про-

блемах (см. раздел 14.1.2). Кому человек сообщает о потенциальном происшествии и как оно урегулируется? Сообщают ли об инцидентах какие-либо электронные устройства, если да, куда идут эти сообщения и как они обрабатываются? В какое время вы хотите реагировать на потенциальные инциденты в области безопасности и как это влияет на механизмы сообщения? Например, если вы обеспечиваете поддержку внутренних пользователей только в рабочее время, но хотите иметь возможность реагировать на происшествия круглосуточно, как человек может сообщить о потенциальном инциденте в области безопасности в нерабочее время?

Первый этап процесса должен быть интегрирован в ваши стандартные процедуры сообщения о проблемах. Нельзя ожидать от пользователей, что они в состоянии аффекта вспомнят, что сетевые или системные сбои должны урегулироваться одним способом, а потенциальные инциденты в области безопасности – другим. Пользователи обычно не имеют достаточных знаний, чтобы определить, является ли происшествие инцидентом в области безопасности.

Человек, получающий сообщение, должен знать последовательность действий по обработке сообщения, связанного с потенциальным происшествием в области безопасности, и определению того, нужно ли передавать это сообщение сотруднику группы реагирования на происшествия. В группе должен быть один или несколько сотрудников, имеющих связи с теми, кому изначально поступают сообщения, и эти сотрудники должны уметь определять, является ли происшествие серьезным инцидентом, на который группа должна реагировать. Также эти сотрудники должны входить в группу обеспечения безопасности. Человек, первым получающий сообщение, должен уметь определить, действительно ли происшествие является потенциальным инцидентом в области безопасности, а если он не уверен – сообщать о нем соответствующему сотруднику группы реагирования на инциденты. Если информация об инциденте в области безопасности не будет передана соответствующим людям – это плохо.

Механизм сообщения о происшествиях

В одной компании, производящей компьютеры, не было формальной группы реагирования на происшествия. Этим занималась группа обеспечения безопасности, у которой был достаточный набор хорошо отработанных процедур. Кроме того, в компании имелась внутренняя компьютерная помощь в режиме 24/7.

Как-то один инженер в веб-группе заработался допоздна и заметил что-то странное на одной из машин в веб-кластере. Он решил разобраться получше и обнаружил, что машина была взломана и что злоумышленник уже активно изменял внешний вид веб-страниц. Инженер попытался сделать все, чтобы злоумышленник покинул машину и не смог вторгнуться в дальнейшем, но понял, что не в силах противостоять, потому что не знал точно, как злоумышленник проник на машину. Он позвонил в круглосуточную внутреннюю группу поддержки около 2 ч ночи и объяснил, что случилось.

Не зная, как действовать в таких случаях, и не имея контактов службы поддержки группы безопасности для нерабочего времени, он просто написал заявку на устранение неисправности и отправил ее кому-то в груп-

пе безопасности. Когда в 8 ч утра пришел администратор безопасности, он обнаружил эту заявку в своей электронной почте и запустил процессы реагирования на инцидент. На этом этапе как инженер, так и злоумышленник устали и ушли спать, что затруднило получение всех подробностей и отслеживание злоумышленника. Инженер чувствовал себя покинутым системными администраторами, потому что он небезосновательно ожидал, что кто-то поможет ему справиться с атакой.

И системные администраторы, и отдел безопасности поступили неправильно, но по-разному. Отдел безопасности поступило неправильно, потому что не предоставил группе внутренней поддержки четких инструкций по сообщению о происшествии в области безопасности. Системные администраторы поступили неправильно, потому что не предприняли попыток сообщить о происшествии, хотя о нем следовало бы сообщить по крайней мере внутри подразделения, если было неизвестно, куда сообщать за его пределами.

После этого происшествия группа безопасности позаботилась о том, чтобы системные администраторы знали, куда сообщать об инцидентах с безопасностью. (Кстати, злоумышленника нашли и успешно наказали за ряд взломов и изменений внешнего вида веб-сайтов, в том числе правительственных.)

После того как вы разработаете схему получения сотрудниками группы реагирования на происшествия сообщений о потенциальных происшествиях в области безопасности, вам нужно определить, какие действия группа должна предпринять. Это зависит от подготовки и решений компании, принятых заблаговременно.

- *Политика реагирования* определяет, на какие происшествия вы реагируете и на каком уровне. Например, вся группа реагирования на происшествия мобилизуется при крупномасштабной атаке на большое количество машин. Однако при небольшой атаке только на одну машину может быть привлечена меньшая группа людей.

  Как вы станете реагировать, если вашу сеть будут сканировать? Вы можете решить записать это или попытаться отследить злоумышленника. На основе различных способов сообщения о происшествиях и уровня фильтрации до получения сотрудником группы реагирования на происшествия сообщения об инциденте вы должны построить список общих сценариев и определить, как реагировать на каждый из них. Вне зависимости от того, планируете ли вы преследовать злоумышленника, группа безопасности должна вести подробные и снабженные временными метками журналы событий, действий и обнаруженных объектов. Вы также должны задокументировать, какой должна быть ваша реакция, если причина происшествия носит, скорее всего, внутренний характер. То, как вы отреагируете, частично будет определяться политикой преследования, политикой отключения и политиками связи компании, описанными ниже.
- *Политика преследования* должна быть создана высшим руководством и юридическим отделом. В какой момент компания начинает преследовать злоумышленников? Ответ может быть от «никогда» до «только когда был

причинен значительный ущерб», «только в случае успешного взлома» или «всегда, даже в случае сканирования». Компания может выбрать вариант «никогда» из-за возможных негативных отзывов в прессе и рисков сбора доказательств. После определения критериев преследования вам также нужно определить, на каком этапе вы будете связываться с правоохранительными органами. Для успеха любого преследования необходимо научить всех сотрудников группы реагирования на происшествия, как и когда собирать доказательства, принимаемые в суде.

- *Политика отключения* определяет, когда вы должны отключать связь между атакуемыми машинами – и, возможно, другими сетями компании – и злоумышленником, если такое вообще допускается. В некоторых случаях это может означать отключение сетевых соединений, возможно соединения с Интернетом, блокировку какой-либо формы удаленного доступа, отключение питания на одной или более машинах, разрыв некоторых сеансов TCP, остановку определенной службы или добавление нескольких правил по фильтрации в межсетевом экране на устройстве, обеспечивающем безопасность периметра. Вы заранее должны определить, какие виды соединений вам может понадобиться отключить, как вы будете это делать и как это повлияет на работу компании. Вам также требуется определить риски отказа от отключения этих соединений в различных ситуациях. Не забывайте принимать во внимание, что ваша сеть в дальнейшем может быть использована для атаки на другие сети. Когда эти данные будут ясны и хорошо организованы, руководство компании должно решить, как и в каких случаях соединения должны быть отключены, когда они не должны отключаться, когда они могут отключаться или не отключаться и кто должен сделать запрос. Также нужно указать, когда соединение может быть восстановлено и кто может принять такое решение.

Использование вашей сети для новых атак

Если ваша сеть используется в качестве базы для атаки других сетей, компания может быть вовлечена в судебное дело против злоумышленника. Даже если ваша компания предпочитает не преследовать его, чтобы избежать негативной реакции общественности, следующая атакованная компания может иметь другую политику. Чтобы защитить свою сеть от использования в качестве базы для атак на другие сети, важно использовать выходную фильтрацию, ограничивающую трафик, который может выходить из вашей сети.

- Высшее руководство должно определить *политику связи* внутри и вне компании для различных типов происшествий в области безопасности. В зависимости от принятых решений эта политика может предполагать связь с маркетинговым подразделением или подразделением по связям с прессой, которые с самого начала должны быть в курсе происходящего. Компания может принять решение максимально избегать огласки инцидентов, чтобы предотвратить появление негативных отзывов в прессе. Такая политика может предполагать отсутствие внутренних сообщений об инциденте в целях не допустить случайной утечки информации в прессу. Политика связи будет влиять на структуру группы. Действует ли кто-то как ответственный

за такие связи? Старается ли группа работать незаметно? Ограничивает ли она число людей, вовлеченных в урегулирование инцидента?

Политика связи может влиять на политику отключения, потому что отключение может привлечь внимание к инциденту. Политика преследования также влияет на политику отключения, потому что отключение может затруднить отслеживание злоумышленника или активировать автоматическую очистку атакованной системы, уничтожая таким образом доказательства. С другой стороны, подключенный злоумышленник может уничтожить доказательства сам.

Реагирование на происшествие в области безопасности – процесс, где очень важны подробности. Он хорошо описан в брошюре SANS (System Administration Networking and Security – Организация по системному и сетевому администрированию и безопасности) «*Computer Security Incident Handling: Step-by-Step*» (Northcutt 1999). Процесс разделен на шесть фаз: подготовка, идентификация, сдерживание, устранение, восстановление и дальнейшие мероприятия. Эти фазы содержат 90 действий в 31 этапах, большая часть которых входит в фазу подготовки. Подготовленность – важнейший элемент эффективного реагирования на происшествие.

11.1.4.3. Внешние проверки

Мы рекомендуем привлечение сторонних консультантов по безопасности в качестве аудиторов. Они должны быть людьми, которых может рекомендовать и с которыми может работать технический персонал, иначе компания не получит максимальной выгоды от сотрудничества. Использование сторонних аудиторов имеет ряд преимуществ. Оно предоставляет группе безопасности независимое мнение о том, как она работает, и свежий взгляд на безопасность компании. Консультанты имеют преимущество в отстраненности от идущей работы, и их подход не будет подвержен влиянию ожиданий и предубеждений. В идеале проверяющая группа не должна быть вовлечена в проектирование или обслуживание систем безопасности компании. Высшее руководство обычно выигрывает от получения стороннего обзора безопасности компании: если консультанты по безопасности имеют опыт в этой области, то они могут предоставить высшему руководству гораздо больше данных о последних новинках отрасли, ресурсах, которые тратят на безопасность похожие компании, и рисках, связанных с любыми недостатками, которые они нашли или о которых узнали от группы безопасности. Сторонняя группа может помочь внутренней группе безопасности получить больше ресурсов, если это допустимо, и у нее может быть больше идей в плане возможных подходов или советов по применению программного и аппаратного обеспечения.

Такие задачи внешней проверки не заменяют задач внутренней проверки. Мы рекомендуем различные функции и задачи внутренних и внешних групп проверки. Задача внешней группы рассмотрена здесь, задача внутренней группы – в разделе 11.1.3.7. Говоря коротко, мы рекомендуем разделение функций проверки, при котором внутренняя группа проверки занимается постоянными проверками, а внешняя группа привлекается периодически для более масштабных проверок и получения полезных результатов, обусловленных ее сторонней точкой зрения.

Мы считаем, что сторонняя проверяющая группа должна оценивать безопасность компании извне, что включает глубокие атаки против определенных областей и сканирование доступных сетей и точек удаленного доступа. Что мы

имеем в виду под фразой «глубокие атаки» против определенной области? Мы имеем в виду задание внешней проверяющей группе, например получение доступа к финансовой или клиентской базе данных компании, а не такое задание, как «пройти через межсетевой экран», которое ориентировано на конкретный механизм безопасности. Глубокая атака предполагает более целостный подход к проверке безопасности сети. Внешняя проверяющая группа может продумать способы атаки, которые не учла группа обеспечения безопасности. Указание в качестве цели атаки инфраструктуры безопасности ограничивает подход консультантов, тогда как у реального злоумышленника этих ограничений не будет. Глубокая атака – это более реалистичная проверка прочности безопасности сети против преднамеренной атаки.

Из некоторых таких проверок группа безопасности может захотеть намеренно исключить социальную инженерию. Социальная инженерия предполагает, что злоумышленник убеждает людей раскрыть ему определенную информацию или предоставить доступ, обычно выдавая себя за другого человека, например нового сотрудника или подрядчика. Социальная инженерия обычно является самым слабым звеном. Важно иметь программу по информированию в этом направлении. Ее успешность можно периодически проверять, разрешая атаки при помощи социальной инженерии. Когда социальная инженерия больше не будет проблемой, нужно разрешить ее как метод.

Сканирование доступных сетей и точек удаленного доступа – другая область, которую можно передать внешней проверяющей группе. Она может стать хорошим источником статистики для использования в общении с высшим руководством при обсуждении деятельности группы безопасности. Кроме того, эта задача является трудоемкой и часто у консультантов есть лучшие средства для ее выполнения. К тому же внешняя группа будет осуществлять свою работу из сети или местоположения, которое не будет обладать очень высоким уровнем привилегий из-за принадлежности компании или сотруднику.

Внешняя проверка должна включать тестирование на проникновение, если в вашей компании это допустимо. Если консультанты осуществляют для вас проверку на проникновение, то необходимо наличие письменного графика тестируемых областей и установленных пределов объема тестирования. Убедитесь, что вы четко определили задачи и ограничения для группы. Например, вы можете указать, что группа должна остановиться сразу же, как только она проникнет в пределы вашего периметра безопасности, получит доступ к конкретной базе данных, получит права привилегированного пользователя на любой из целевых машин или покажет, что атака «отказа в обслуживании» работает на одной или двух машинах. В процессе проверки консультанты должны тщательно координировать свои действия с одним-двумя сотрудниками компании, которые в любой момент должны иметь возможность приказать им остановиться, если они начали наносить непредвиденный ущерб. Убедитесь, что у вас есть одобрение самого высокого руководства на проведение таких проверок.

Проверка на проникновение должна координироваться

Один консультант был привлечен для проведения проверки на проникновения в крупной транснациональной компании по компьютерным сетям. В очень подробном контракте и перечне работ были описаны даты, содержание и ограничения тестирования. Одним из элементов проверки

на проникновение была проверка на DoS-уязвимости. Консультант обнаружил многоуровневую DoS-уязвимость, которая вывела из строя все европейские соединения, прежде чем он смог прекратить проверку. Естественно, такой большой сбой в сети привлек очень серьезное внимание высшего руководства. К счастью, консультант тщательно соблюдал контракт и перечень работ, поэтому инцидент вызвал гораздо меньше расходов, чем могло быть, если бы эту уязвимость обнаружил злоумышленник или компания не смогла бы быстро разобраться в том, что произошло. Как только высшее руководство разобралось, что и почему произошло, они с пониманием отнеслись к расходам на нахождение этой уязвимости прежде, чем она могла быть использована против них.

11.1.4.4. Многофункциональные группы

Группа обеспечения безопасности не может работать в изоляции. Ей нужно максимально быстро узнавать о любой новой разработке бизнеса, которая может повлиять на безопасность. Группа должна знать об особенностях компании и ключевых игроках при разработке политик безопасности. Группе нужны сильные связи с остальными сотрудниками группы системных администраторов, чтобы обеспечить понимание и поддержку того, что она реализует, и она должна быть уверена, что другие администраторы не сделают ничего, что повредит безопасности. Группа должна быть в курсе того, как работают другие люди в компании и как изменения в области безопасности повлияют на этих людей, особенно в периферийных офисах.

- Сильная связь с *юридическим отделом* компании приносит большую пользу. Нужный человек или люди в этом подразделении, скорее всего, будут рады крепким связям с группой безопасности, потому что у них найдутся вопросы и проблемы, которые эта группа сможет решить. Нужный человек в данной группе – это обычно сотрудник, ответственный за интеллектуальную собственность, который чаще всего называется менеджером по интеллектуальной собственности, или IP-менеджером (Intellectual Property, не путать с IP-протоколом – Internet Protocol).

  IP-менеджер – подходящий человек для того, чтобы возглавить группу защиты информации, в которую обычно входят представители всех подразделений компании для обсуждения того, как в компании лучше всего защищать интеллектуальную собственность и как предлагаемые изменения повлияют на каждое подразделение. В этой группе должны присутствовать представители следующих отделов: юридического, управления рисками и аварийного планирования, эксплуатационного, безопасности (данных), системного администрирования, кадров, маркетинга и связей с общественностью, инженерного и отдела сбыта.

  IP-менеджер в юридическом отделе заинтересован в безопасности данных, хранимых в электронном виде, потому что защита компанией своей информации связана с тем, как она может защищать свои права на эту информацию в сети. IP-менеджер также, скорее всего, будет вовлечен во все партнерские переговоры с другими компаниями, слияния и приобретения или, по крайней мере, будет в курсе текущей ситуации, потому что в этих случаях будет иметь место обсуждение вопросов интеллектуальной собственности. Если у вас хорошие отношения с этим человеком, он может предоставить вам

информацию о планируемых проектах, которая потребуется вам для своего планирования, и привлечет вас к работе с группами этих проектов на начальном этапе. Также он сможет предоставить вам базу для модели безопасности, основанную на контрактном соглашении между двумя компаниями, и помочь с политиками, необходимыми для поддержки соглашения, и с обучением людей, которые будут работать с компанией-партнером.

Пример: важность связей с юридическим отделом

Одно подразделение транснациональной компании по автоматизации проектирования электроники (Electronic Design Automation – EDA) заключило соглашение с EDA-подразделением IBM. Соглашение предполагало совместную разработку программного продукта, а это означало, что обеим группам нужен был полный доступ к исходному коду продукта и пригодная для работы среда разработки. Однако другие группы в EDA-подразделении IBM напрямую конкурировали с другими группами в EDA-компании, а другие части IBM – с клиентами EDA-компании. Компания часто получала от своих клиентов конфиденциальную информацию, которая обычно была связана со следующим поколением чипов, разрабатываемых клиентом. Это была очень важная и чрезвычайно ценная информация. Следовательно, EDA-компании требовалось тщательно ограничить информацию, которую она использовала совместно с IBM.

Сотрудник юридического отдела EDA-компании, с которым контактировала группа безопасности, обеспечил создание группы проектирования общей среды разработки задолго до подписания контракта, и группа обеспечения безопасности входила в ее состав. Среди других сотрудников были люди, ответственные за средства разработки, группа управления выпуском, служба технической поддержки и аналогичные сотрудники IBM. Для работы по другим направлениям соглашения было сформировано несколько других групп, и работа отслеживалась и координировалась людьми, ответственными за выполнение соглашения. Кроме того, IP-менеджер управлял группой, разрабатывающей обучающие материалы для инженеров, которым предстояло трудиться над совместным продуктом. Эти материалы включали руководство по контрактным обязательствам и ограничениям, политики, реализованные в соответствии с этим проектом, и технический обзор использования области совместной разработки. Обе стороны получили одинаковые обучающие материалы.

В проекте такого масштаба, в который было включено так много различных отделов компании, группа безопасности потерпела бы неудачу, если бы не была к нему привлечена с самого начала. Кроме того, деятельность группы не имела бы успеха без четких указаний от юридического отдела относительно того, что должно быть открыто для общего доступа, а что защищено. Другим важнейшим залогом успеха группы безопасности был дух сотрудничества в многофункциональной группе, которая разрабатывала среду.

Казалось бы, очевидно, что именно так и должно все выполняться, но мы снова и снова слышим о тайно заключенных деловых соглашениях, о которых IT-подразделение узнает последним.

- Безопасность должна быть общим делом компании вообще и группы системных администраторов в частности. Системные администраторы часто узнают о том, что происходит или будет происходить в их подразделениях бизнеса, до того, как решают привлечь группу безопасности. Системные администраторы могут помочь привлечь группу безопасности на начальном этапе, что существенно повысит успешность проектов. Кроме того, группа системных администраторов может помочь за счет наблюдения за необычными действиями, которые могут быть признаком атаки, знания того, что нужно делать при обнаружении таких действий, и, возможно, вхождения в состав группы реагирования на происшествия.

  В некоторых компаниях группа поддержки бизнес-приложений (иногда называемая MIS – Management of Information Systems – управление информационными системами) является частью групп системных администраторов, в других нет. Сотрудники этой группы отвечают за определенный набор бизнес-приложений: системы отдела кадров, расчета зарплат, отслеживания заказов, финансовые системы. Очень важно, чтобы группа безопасности имела поддержку этой группы и знала, что в ней происходит. Если группа поддержки приложений не понимает модель и политику безопасности, она может выбрать и установить программную систему, которая поддерживает удаленный модемный доступ поставщика или соединение с поставщиком и не обеспечивает возможности создания приемлемой модели безопасности. Группа может установить приложение, чувствительное к безопасности, не понимая этого или не используя при его выборе соответствующие инструкции по безопасности. Если группа безопасности будет эффективно работать совместно с этой группой, подобных ошибок можно избежать.

- *Группа разработки продукта* – это главный источник прибыли для компании. В консалтинговой компании это консультанты, в университете – преподаватели и студенты, в некоммерческой организации – люди, выполняющие главные функции организации. Если эти люди не могут эффективно выполнять свою работу, вся компания будет подвержена негативному влиянию, поэтому так важно работать с ними в тесной связи, чтобы понимать их требования. Кроме того, именно группе разработки продукта, скорее всего, потребуется взаимодействие с деловыми партнерами и она будет иметь сложные требования к безопасности. Хорошее знание этих людей и получение информации о новых проектах до того, как они станут официальными, позволяют группе безопасности быть более подготовленной. Группа разработки продукта, скорее всего, будет использовать системы безопасности регулярно. Следовательно, мнения группы о том, насколько система проста в использовании, как выглядит рабочий процесс и какими она видит будущие требования, очень важны.

- Функционирование безопасности обычно основано на одном или нескольких *основных филиалах* компании. Менее крупные филиалы часто считают, что их требования игнорируются или упускаются, поскольку нередко их набор требований отличается от требований людей в более крупных филиалах и они практически не имеют прямой связи с группой безопасности, если имеют какую-либо связь вообще. В филиалах часто размещается персонал сбыта и поддержки, который нередко выезжает к клиентам и которому может понадобиться доступ к корпоративной информации в пути или у клиента. В компании клиента возможные типы доступа к компании обычно ограничены из-за политик и прав клиента. Если филиалы не способны

использовать один из официально разрешенных методов, они могут установить в своих офисах что-то для себя, чтобы выполнять свою работу. Из-за недостаточного количества системных администраторов или отсутствия связи группы безопасности с офисом может быть очень трудно обнаружить, что в удаленном офисе появился такой доступ. Очень важно, чтобы люди в таких офисах знали, что их голос слышат и их требования выполняются группой безопасности. Также важно, чтобы они понимали, что делает группа безопасности и почему действия, выполняемые в обход группы безопасности, вредны для компании.

11.1.4.5. Продавайте безопасность эффективно

Продажа безопасности аналогична продаже страхования. В трате денег нет очевидной мгновенной пользы, за исключением душевного спокойствия. Но в случае со страхованием клиенты, по крайней мере, могут из года в год и из десятилетия в десятилетие оценивать, как они живут, и видеть потенциальные издержки в случае отсутствия страховки, даже если риски трудно представить среднестатистическому человеку. В случае с безопасностью пользу увидеть сложнее, если группа безопасности не может предоставить больше данных о неудавшихся атаках, глобальных тенденциях в области атак и потенциальных убытках компании.

Вам требуется продавать безопасность высшему руководству, людям, использующим системы, и системным администраторам, которым придется эти системы устанавливать, обслуживать и поддерживать их пользователей. Каждая из этих групп имеет свои задачи, и при разработке и реализации программы безопасности нужно учесть все их пожелания.

Чтобы продать безопасность высшему руководству, вы должны показать, как обеспеченная вами безопасность помогает компании выполнять обязательства перед акционерами и клиентами, а также как безопасность может рассматриваться в качестве конкурентного преимущества. У всех организаций есть эквивалент клиентов и акционеров. Клиентами университета являются студенты и финансирующие организации, в некоммерческой или правительственной организации клиентами являются субъекты, которых она обслуживает.

Пытаясь продать безопасность другим, важно показать им, что ее покупка отвечает их важнейшим интересам, а не вашим. Юридический отдел должен иметь возможность помочь с информацией по правовым обязательствам. Если компания получает от клиентов конфиденциальную информацию, хорошая безопасность является активом, который может обеспечить развитие бизнеса. Университеты смогут получить более серьезную спонсорскую поддержку, если они смогут показать, что способны безопасно хранить конфиденциальную информацию. Компании сферы услуг или поддержки за счет демонстрации своего внимания к безопасности также могут повысить доверие клиентов. Подумайте, чего вы, человек, заинтересованный в безопасности, хотели бы от своей компании, если бы были ее клиентом. Если вы можете это предоставить и продать, то это является конкурентным преимуществом.

Кроме того, соберите данные о том, что делают конкуренты компании в плане вложений в безопасность, или, по крайней мере, данные о других компаниях такого же размера в достаточно похожих отраслях. Высшему руководству потребуется возможность оценить, тратится ли на безопасность слишком много, слишком мало или достаточно средств. Если возможно, создайте метрику для

измерения работы, выполняемой группой безопасности. Мертики будут рассмотрены далее в разделе 11.2.3. Также рассмотрите возможность привлечения сторонней группы для выполнения анализа рисков вашей компании. Высшее руководство любит, когда есть серьезные данные, на основании которых можно принимать решения.

Пример: используйте безопасность как конкурентное преимущество

Компания по автоматизации проектирования электроники по различным причинам регулярно получала от своих клиентов проекты чипов. Компания должна была обращаться очень внимательно с этой ценной интеллектуальной собственностью третьих сторон. Компания очень заботилась о безопасности и имела хорошие средства безопасности и группу защиты информации, которая считала свою программу безопасности конкурентным преимуществом и именно в таком свете представляла ее клиентам и руководству. Это помогало обеспечивать высокий уровень поддержки безопасности в компании.

Чтобы продать безопасность, вы должны обеспечить людям, которые будут пользоваться системами, возможность эффективно работать в среде, которая удобна для них. Вам также понадобится показать им, что безопасность отвечает их важнейшим интересам или важнейшим интересам компании. Если вы сможете предоставить им систему, которая не влияет на их работу, но предоставляет больший уровень безопасности, пользователи будут рады с ней работать. Однако вы должны быть особенно внимательны, чтобы не потерять доверие этих клиентов. Если вы будете предоставлять медленные, громоздкие или назойливые системы, пользователи потеряют веру в вашу способность создать систему безопасности, которая не влияет негативно на их работу, и не захотят использовать ваши системы безопасности в дальнейшем. Доверие очень важно для успешной продажи.

Чтобы продать безопасность системным администраторам, которые будут обслуживать системы, следить за людьми, пользующимися этими системами, и, возможно, устанавливать системы, вы должны обеспечить, чтобы системы, которые вы проектируете, были просты в применении и реализации, имели простую и понятную установку, а также были надежны и не вызывали бы проблем у пользователей. Вам также потребуется обеспечить их средствами и способами отладки. В идеальном случае поддержка системы безопасности не должна затруднять людей больше, чем поддержка любой другой системы.

11.2. Тонкости

В данном разделе рассмотрены идеальные реализации программы безопасности. Чтобы достичь такого уровня, вам потребуется надежная инфраструктура и программа безопасности. В идеале группы безопасности и защиты информации должны сделать безопасность предметом внимания всех в компании. Кроме того, группа безопасности обязана быть в курсе новинок отрасли, что предполагает поддержание контактов и отслеживание новых технологий и направле-

ний. И наконец, группа безопасности может создать метрику, позволяющую дать представление о том, как работает группа, и показать пользу от программы безопасности.

11.2.1. Сделайте безопасность предметом общего внимания

Хорошая программа защиты информации предполагает осведомленность каждого сотрудника в вопросах безопасности и интеллектуальной собственности. Например, в одной компании, где работала Кристина, группы защиты информации и маркетинга вели просветительскую деятельность, которая включала создание плакатов с комиксами, где были показаны распространенные способы кражи информации и подчеркивалась необходимость опасаться воров ноутбуков в аэропортах.

Если вы можете сделать безопасность частью образа мыслей и работы людей, работа группы безопасности станет гораздо проще. Люди будут автоматически привлекать группу обеспечения безопасности на ранних этапах проектов, замечать странное поведение, которое может быть признаком взлома, и внимательно следить за важной информацией.

Пример: сделайте безопасность предметом общего внимания

В IBM политика «чистого рабочего стола» (Clean Desk Policy) предписывала, чтобы все бумаги, вне зависимости от степени их конфиденциальности, запирались в столе сотрудника каждый вечер, а конфиденциальные документы должны быть под замком все время. Обычно результатом нарушения являлась записка, которую оставлял на столе либо охранник, либо сотрудник IT- или хозяйственного отдела – в зависимости от того, кто отвечал за проверку конкретного офиса. С многократными нарушениями разбирались по-другому, в зависимости от ситуации, но существовал ряд критериев наказания. По крайней мере один человек был уволен за оставление на своем столе строго конфиденциальной информации.

В IBM целые блоки офисов и залы для конференций не имеют окон для предотвращения возможности подсматривать через окна с помощью оптических приборов. Безопасность в компании важна для всех и является серьезной частью корпоративной культуры.

Пример: просвещайте сотрудников в вопросах безопасности

Motorola запустила программу защиты патентованной информации POPI (Protection of Proprietary Information). Эта программа информирования о безопасности включала информационные плакаты, напоминающие людям о том, что они должны быть внимательны с патентованной информацией, даже в пределах зданий компании. Напоминания на принтерах

указывали, что все распечатки должны быть убраны вечером в определенное время, поэтому люди не оставляли никаких распечаток, чтобы никто не мог их просмотреть или забрать. Маленькие таблички на столах напоминали: «Пожалуйста, не оставляйте патентованную информацию на моем столе, когда меня нет». В каждом подразделении была «полиция POPI», которая периодически совершала обходы и проверяла столы и доски на наличие важной информации. После проверки полиция оставляла на каждом столе либо зеленую карточку «Все хорошо», либо красную «Вы сделали неправильно следующее...».

Люди обычно хотят поступать правильно. Если вы будете постоянно напоминать им, что правильно, а они будут стараться так поступать, это войдет в привычку. Очень важно уважительное отношение, чтобы напоминания не заставляли людей чувствовать, что к ним придираются, их опекают, или, иначе говоря, не воспринимают как разумных взрослых людей. Снисхождение и придирки вызывают возмущение и не способствуют созданию полезных для безопасности привычек.

11.2.2. Будьте всегда в курсе: связи и технологии

Связи в отрасли безопасности могут быть хорошим источником информации по актуальным атакам и уязвимостям, различным мнениям о продуктах и развивающихся технологиях. Посещение конференций по безопасности является хорошим способом завести такие связи и позволяет вам на несколько месяцев опережать своих конкурентов в отрасли. Профессионалы в области безопасности обычно излишне осторожны и практически не делятся своим опытом с людьми, которых они плохо знают, поэтому важно посещать большое количество конференций, войти в сообщество и стать там известным и построить хорошие отношения с другими участниками конференций.

Вы также должны стремиться быть в курсе всех новых разрабатываемых технологий, их предполагаемых преимуществ, принципа работы и требований для их внедрения и эксплуатации. В этом процессе вам потребуется развить навык отличать «панацеи» от полезных продуктов. Советы можно найти в книге Мэтта Кертина «*Snake Oil Warning Signs: Encryption Software to Avoid*» (Curtin 1999a, b).

В рамках любой идеи нового продукта разработчики обычно применяют несколько принципиально различных подходов, и часто трудно сказать, насколько успешным будет любой из них. Однако отслеживание развития различных подходов, понимание их значения для работы и знание людей, которые стоят за различными подходами, поможет вам предсказать, какие продукты и технологии окажутся успешными.

11.2.3. Создайте метрику

Метрика в безопасности – это очень сложный элемент. Как было упомянуто выше, продажа безопасности аналогична продаже страхования. Если вы сможете предоставить какую-либо форму метрики, убедительно характеризующую качество работы группы безопасности и выгоду, которую она приносит компании

за ее деньги, будет проще убедить руководство финансировать проекты по инфраструктуре безопасности.

Наличие сторонней проверяющей группы может быть полезным источником метрики. Например, вы можете описать область, которая была проверена или атакована, уровень успешности и возможные расходы в случае взлома безопасности этой области. Если в данной области были обнаружены проблемы, вы сможете подготовить информацию о том, сколько будет стоить их устранение, а затем держать начальство в курсе хода улучшений.

Если у вас есть четкий периметр безопасности, то вы можете – например, при помощи системы обнаружения вторжений, – собрать данные по количеству предпринятых или потенциальных атак, обнаруженных вне периметра безопасности и в его пределах, и построить таким образом график уровня защиты, который обеспечивается вашим периметром. Вы можете начать с простых графиков количества машин, которые видны людям вне компании, статистики по количеству служб, доступных на каждой из них, и количества уязвимостей. Вы также можете отобразить на графике количество патчей для операционных систем и приложений, которые потребовалось установить с целью обеспечения безопасности.

Хорошая метрика должна помочь руководству и другим далеким от безопасности людям в компании ясно понять, что вы делаете и насколько хорошо. Хорошая метрика помогает обеспечить доверие остальной компании к группе обеспечения безопасности. По крайней мере, она демонстрирует, какая работа сделана и в каких областях постоянно присутствуют проблемы.

11.3. Профили организаций

В данном разделе мы представим краткий обзор этапов разработки адекватной программы безопасности компании в зависимости от размера и назначения компании. Данный раздел является лишь руководством, предназначенным для того, чтобы создать у вас представление о том, отстаете ли вы от основной тенденции или опережаете ее и как должна развиваться ваша программа безопасности с ростом вашей компании.

Мы рассмотрим простую программу безопасности для малой, средней и крупной компаний, сайта электронной коммерции и университета. В этих примерах предполагается, что наиболее типичное количество сотрудников для малой компании – от 20 до 100, для средней – от 1000 до 3000, а для крупной – более 20 тыс.

11.3.1. Малая компания

В малой компании с одним или двумя системными администраторами обеспечение безопасности не потребует больших усилий. В компании должна быть политика допустимого использования, также стоит подумать о создании политики мониторинга и неприкосновенности личной информации. Системные администраторы, скорее всего, будут знать практически все, что происходит в компании, и поэтому им вряд ли понадобится участие в каких-либо формальных многофункциональных группах. Для компании в первую очередь будет важна безопасность периметра, особенно если это начинающая компания. Системные администраторы должны продумать механизм жесткой аутентифика-

ции, поставить руководство в известность о его необходимости и решить, когда компании лучше всего сделать в него вложения.

Если малая компания только начинает свою деятельность, особенно в компьютерной отрасли, инженерному отделу может потребоваться открытый доступ в Интернет для получения самой свежей информации о новых технологиях, как только она появится. В данном случае компания должна определить, справится ли с этим среда разработки, и если нет, как максимально защитить инженерный отдел, не вмешиваясь в его работу, и как защитить от инженерного отдела остальную компанию.

11.3.2. Средняя компания

В средней компании должна быть небольшая группа постоянно работающих системных администраторов. Основной функцией одного из этих системных администраторов должно быть выполнение работы архитектора безопасности. Остальные системные администраторы должны быть, главным образом, конструкторами и играть второстепенные роли в безопасности. Ответственность за безопасность должна быть централизована, даже если системные администраторы выполняют в числе прочего какую-то работу по обеспечению безопасности в удаленных офисах. Удаленные системные администраторы должны отчитываться перед группой обеспечения безопасности об этом аспекте своей работы.

Архитектор безопасности будет выполнять большую работу по реализации, а конструкторы станут также выполнять обязанности операторов. За политики будет отвечать архитектор и, возможно, руководитель группы. Проверки могут проводиться конструктором или архитектором, также для создания программы проверки они могут работать с какими-нибудь сторонними консультантами. В компании должны быть все основные политики, рассмотренные в разделе 11.1.2, и по крайней мере простейшая программа проверки. Должна быть группа защиты информации с представителями из юридического, хозяйственного, информационного отделов, а также отделов кадров и сбыта и основных групп бизнеса. Компании необходима программа информирования о безопасности, проводимого группой защиты информации.

В компании должны быть серьезная инфраструктура безопасности и централизованная, надежная и тщательно установленная система жесткой аутентификации. Скорее всего, в компании будет много механизмов удаленного доступа, которые должны быть связаны с системой аутентификации. Компании почти наверняка потребуются соединения с третьими сторонами по различным причинам, связанным с бизнесом. В таких соединениях по возможности должны использоваться стандартные механизмы обеспечения безопасности и общая инфраструктура. В компании могут быть области, которые требуют более высокого уровня безопасности и дополнительной защиты от остальных сотрудников компании. В ней также могут быть системы разработки, которые более доступны извне, но от которых защищена остальная компания.

11.3.3. Крупная компания

Самые серьезные проблемы, с которыми сталкиваются крупные компании, связаны с их размером. Затрудняются реагирование на происшествия, согласованность политик и отслеживание изменений.

В крупной компании должно быть несколько выделенных сотрудников для выполнения каждой функции обеспечения безопасности. Скорее всего, компания будет разделена на административные подразделения бизнеса, в каждом из которых будут свои политики и периметр безопасности, с четко описанными методами обмена информацией между подразделениями. В каждом подразделении бизнеса должны быть все политики, описанные в разделе 11.1.2, а в случае необходимости – и другие.

В компании должна быть широкая инфраструктура безопасности с всесторонней программой проверки. В каждом подразделении бизнеса должно быть достаточно много групп, созданных из представителей различных подразделений, которые занимаются программами безопасности и информирования о безопасности.

Во многих областях требования по физической и электронной безопасности будут гораздо выше, чем в остальных. Фактически крупные компании обычно меньше доверяют всем сотрудникам. Просто есть больше возможностей для случайного или злонамеренного раскрытия важной информации.

Наверняка потребуются соединения с третьими сторонами с большим количеством ограничений и контрактов, связанных с их использованием. Кроме того, могут быть в наличии системы разработки, более доступные из внешних сетей.

Слияния и поглощения приносят новые проблемы. Важнейшими задачами крупных компаний становятся урегулирование различий в политиках безопасности, культуре и отношении, а также интеграция сетевого оборудования (сетевое обнаружение).

11.3.4. Компания электронной коммерции

Компания, которая ведет свой бизнес в основном через Интернет, имеет особые требования, помимо уже рассмотренных. В частности, в компании электронной коммерции должно быть четкое разделение между «корпоративными» машинами и машинами «сетевого обслуживания». Последние применяются для ведения бизнеса через Интернет, а корпоративные машины используются для всего остального.

Вне зависимости от размера, в компании электронной коммерции должен быть по крайней мере один постоянный сотрудник-профессионал в области безопасности. Из-за особенностей бизнеса компании потребуется расширять свой персонал безопасности гораздо быстрее, чем другим компаниям такого же размера. Кроме того, компании потребуется разрабатывать политики, связанные, например, с защитой информации клиентов, быстрее других компаний такого же размера.

Для управления доступом к корпоративным машинам и машинам сетевого обслуживания компании электронной коммерции требуются отдельные политики. Вне зависимости от размера, в компании должна быть матрица авторизации, которая определяет уровень доступа к каждому типу машин сетевого обслуживания. Кроме того, компания должна уделять особое внимание платежной информации клиентов, в том числе сведениям о кредитных картах, адресам и номерам телефонов. Для бизнеса компании электронной коммерции жизненно необходимо уделять особое внимание предотвращению DoS-атак на ее инфраструктуру сетевого обслуживания.

11.3.5. Университет

Среда университета обычно значительно отличается от среды бизнеса. В бизнесе людям с правомочным доступом к сети, как правило, можно доверять по определению[1]. Обычно компания предполагает, что все сотрудники работают в интересах компании[2]. Однако в университете люди, имеющие доступ к сети, не являются доверенными по умолчанию, частично из-за того, что физический доступ является довольно свободным.

Обычно в университете есть административные сети и компьютеры с ограниченным доступом и жестким контролем безопасности, а также учебные сети, которые являются довольно открытыми. Часто в университете есть открытый доступ в Интернет и из него, потому что исследовательская среда предполагает тесную взаимосвязь открытости и обучения.

Обычно университеты могут позволить себе тратить меньше денег на компьютерные системы вообще и на безопасность в частности, и в некотором смысле в этом они аналогичны малым компаниям. В университете должна быть политика допустимого использования и политика мониторинга и неприкосновенности личной информации, которые каждый пользователь компьютера должен подписать перед получением доступа к компьютерным системам.

Помните, что первые вопросы, которые вы должны задать, – это что вы должны защитить, от кого и сколько это будет стоить. Обычно университеты открыто публикуют свои исследования, поэтому ценность этих исследований не так велика, как проектирование нового компьютерного процессора или подробности о новом лекарстве. В случае с учебными сетями руководство университета может быть заинтересовано в предотвращении серьезных потерь данных или утраты работоспособности, а также может указать, что есть люди с правомочным доступом к сети, которые должны рассматриваться как угроза.

В системе университета вам потребуется глубокая безопасность на ключевых серверах и дополнительные меры безопасности для административных сетей. Для машин с открытым доступом в лабораториях вам потребуется хорошая система автоматической установки и обновления, рассмотренная в главе 3, и поиск баланса между требованиями безопасности, исследований и обучения.

11.4. Заключение

Безопасность – это широкая, сложная область, которая требует даже больше навыков общения, чем другие области системного администрирования, и должна быть совместной задачей нескольких административных отделов. Безопасность должна строиться на жестких основаниях политик, одобренных и поддерживаемых высшим руководством. Построение систем безопасности основано на инфраструктуре других систем.

---

[1] Часто существуют различные уровни доступа и защиты даже в пределах одной компании, но обычно в компании все имеют доступ ко всей информации, кроме наиболее важной, если это не очень крупная компания, разделенная на подразделения меньшего размера.

[2] С точки зрения безопасности это может быть неразумно, но это является оправданным деловым компромиссом, на который идет большинство руководителей.

Есть ряд областей, на которых должен сосредоточиться технический персонал, а также другие области, где может помочь руководство. Технический персонал должен обеспечивать потребности бизнеса, удобство для пользователей, информированность об актуальных атаках и уязвимостях, построение жесткой системы аутентификации и авторизации и выбор хорошего программного обеспечения безопасности. В идеальном случае технический персонал также должен заводить хорошие связи в отрасли и постоянно следить за новыми технологиями, прилагая все усилия, чтобы быть в курсе всего происходящего в мире безопасности.

Руководство группы безопасности может помочь с ресурсами и персоналом, созданием группы реагирования на происшествия, привлечением сторонних аудиторов и «продажей» безопасности другим подразделениям компании. В идеальном случае безопасность должна быть неотъемлемой частью культуры компании. Чтобы привить этот вид корпоративной культуры, требуется много времени и сил, и она будет успешной, только если инициатива исходит от высшего руководства. Один из лучших способов получить поддержку руководства – подготовить убедительную метрику работы, которой занимается группа обеспечения безопасности.

Задания

1. Какие политики безопасности у вас есть? Какие из них нужно обновить? Какие политики, рассмотренные в данной главе, отсутствуют? Какие проблемы это вызывает?
2. Как вы считаете, почему мы рекомендуем, чтобы в политике сетевых соединений были оговорены все поддерживаемые формы соединений с третьими сторонами?
3. Какие соединения с третьими сторонами есть в ваших структурах? Можете ли вы с полной уверенностью сказать, что других соединений нет? Что можно сказать о небольших удаленных офисах? Можете ли вы классифицировать эти соединения по типам доступа?
4. Есть ли у вас инфраструктура для простой организации нового соединения с третьими сторонами? Если нет, попытайтесь разработать такую инфраструктуру, после чего посмотрите, сможете ли вы включить в нее имеющиеся соединения с третьими сторонами.
5. Какие три изменения в области безопасности вы порекомендовали бы прямо сейчас своему руководству?
6. В разделе 11.1.3.6 есть определение «продуктов, чувствительных к безопасности». Определите, какие устройства вашей сети являются чувствительными и нечувствительными к безопасности.

Глава 12

Этика

Какие политики, связанные с этикой, должны быть в компании? Какова дополнительная моральная ответственность системных администраторов и других сотрудников с привилегированным техническим доступом? В данной главе рассматриваются оба вопроса.

Этика, принципы поведения, которыми руководствуется группа людей, отличается от морали. **Мораль** – это провозглашение того, что хорошо и правильно, и она не входит в число вопросов, обсуждаемых в данной книге.

Вне зависимости от того, привлекает ли вас ваша организация к созданию этических руководств для всех пользователей сети или только для системных администраторов, ознакомьтесь с этой главой. Мы хотим предоставить вам средства, необходимые для выполнения этой работы.

12.1. Основы

Обычно в организациях есть различные политики, связанные с этикой, для своих сотрудников и других филиалов. Этические нормы, связанные с применением сетей, делятся на две категории: нормы, применяемые ко всем пользователям, и нормы, применяемые только к привилегированным пользователям, например руководителям, системным администраторам и администраторам баз данных. В принципе, системный администратор должен тщательно соблюдать политики компании, а также быть примером для подражания. У вас есть доступ к конфиденциальной информации, которую не может видеть большинство других сотрудников, поэтому на вас лежит особая ответственность.

В последнее время появилось много американских и европейских правовых нормативных документов, утвердивших более широкую ответственность корпораций за соблюдение этических норм и правил в сфере IT. Такие документы, как закон Сарбейнса–Оксли (Sarbanes-Oxley Act), Закон о правах семьи на образование и неприкосновенность частной жизни (Family Educational Rights and Privacy Act), Закон об отчетности и безопасности медицинского страхования (Health Insurance Portability and Accountability Act – HIPAA) изменили образ мыслей компаний относительно этих проблем. Профессия системного администратора была затронута напрямую.

12.1.1. Согласие, основанное на полученной информации

Принцип согласия, основанного на полученной информации, изначально сформулированный специалистами по врачебной этике, справедлив в отношении системных администраторов точно так же, как и в отношении врачей. Во врачебной этике согласие, основанное на полученной информации, складывается из двух частей. Сначала пациент должен быть полностью информирован о вариантах лечения, всех возможных достоинствах и недостатках этих вариантов и степени вероятности успеха. Информация должна быть представлена так, чтобы человек ее понял, и у пациента должна быть возможность решиться на лечение или отказаться от него без какого-либо принуждения – в этом заключается элемент согласия.

Такое согласие невозможно, если кто-то не информирован должным образом – неспособен понять последствия – или не имеет возможности дать согласие, например человек находится в коме и у него нет близких родственников. В таких случаях общепринятым стандартом является полное соблюдение трех следующих условий. Во-первых, у процедуры должна быть высокая вероятность успеха. Во-вторых, должны учитываться прежде всего интересы *пациента*, чтобы в случае успешного проведения операции человек скорее всего был бы благодарен впоследствии. В-третьих, сначала должны быть использованы все возможности получить согласие, основанное на полученной информации. Другими словами, нарушение принципа согласия, основанного на полученной информации, является крайней мерой.

Эти принципы могут быть применены ко многим задачам системных администраторов. Люди должны понимать правила, по которым они живут. Например, в соглашении об уровне обслуживания (Service-Level Agreement – SLA) может быть указано, что обслуживание будет осуществляться только в определенные часы, и ваши клиенты должны их знать. Компьютерный сервер может быть предназначен для выполнения долговременных задач, например симуляций. Если у программы симуляции нет функции сохранения на контрольных точках, из-за перезагрузки можно потерять дни и недели работы. Если перезагрузка совершенно неизбежна, в SLA может быть указано, что текущие пользователи машины будут уведомлены об этом, – согласие, основанное на полученной информации. С другой стороны, вычислительные серверы для задач с меньшими затратами времени могут иметь SLA общего характера, в котором будет указано только предупреждение за 15 мин. SLA информирует ваших клиентов о том, как вы будете работать в различных ситуациях.

12.1.2. Профессиональный кодекс поведения

Гильдия системных администраторов (System Administrators' Guild – SAGE) и Лига профессиональных системных администраторов (League of Professional System Administrators – LOPSA) разрешили нам напечатать последнюю редакцию Этического кодекса системных администраторов[1]. Мы делаем это, поскольку

[1] SAGE – *www.sage.org*. LOPSA – *http://lopsa.org*.

ку считаем, что он является отличным словесным выражением наших мыслей относительно того, что системные администраторы должны поддерживать очень высокий уровень профессионализма. Этот документ является хорошей основой для написания ваших собственных корпоративных правил поведения. Он намеренно *не* является сводом законов, обязательных для принудительного исполнения, перечислением процедур, всеобъемлющим списком предполагаемых ответных действий в различных ситуациях или перечислением санкций и наказаний.

Этический кодекс системного администратора

Профессионализм

- Я буду соблюдать профессиональные нормы на рабочем месте и не позволю личным чувствам или убеждениям заставлять меня относиться к людям несправедливо или непрофессионально.

Личная сознательность

- Я буду честным в своей профессиональной деятельности и стану позитивно воспринимать критику относительно моей компетенции и последствий моих ошибок. Когда потребуется, я обращусь за помощью к другим.
- Я буду по возможности избегать конфликтов интересов и убеждений. Когда у меня попросят совет и при этом имеется конфликт интересов и убеждений, я сообщу о последнем, если это уместно, и при необходимости откажусь от участия.

Неприкосновенность личной информации

- Я буду осуществлять доступ к личной информации в компьютерных системах, только когда это необходимо для выполнения моих технических обязанностей. Я буду поддерживать и защищать конфиденциальность любой информации, к которой у меня может быть доступ, вне зависимости от способа, которым я ее узнал.

Законы и политики

- Я буду изучать актуальные законы, нормы и политики, касающиеся выполнения моих обязанностей, и обучать им других.

Общение

- Я стану обсуждать с руководством, пользователями и коллегами компьютерные вопросы, если это будет в наших общих интересах.
- Я буду стараться выслушать и понять потребности всех сторон.

Целостность системы

- Я буду стараться обеспечить необходимую целостность, надежность и доступность систем, за которые отвечаю.
- Я буду разрабатывать и обслуживать каждую систему так, чтобы это максимально соответствовало ее назначению в организации.

Образование

- Я буду улучшать и расширять свои технические знания и другие навыки, связанные с работой.
- Я буду делиться своими знаниями и опытом с другими.

Ответственность перед компьютерным сообществом

- Я буду сотрудничать с более крупным компьютерным сообществом, чтобы поддерживать целостность сетевых и компьютерных ресурсов.

Социальная ответственность

- Как информированный профессионал я буду способствовать написанию и принятию актуальных политик и правил, согласующихся с перечисляемыми здесь этическими принципами.

Нравственная ответственность

- Я постараюсь создать и поддерживать спокойную, здоровую и продуктивную рабочую обстановку.
- Я приложу все усилия для того, чтобы мои решения согласовывались с безопасностью, неприкосновенностью личной информации и благополучием моего сообщества и общества в целом, и буду оперативно выявлять факторы, которые могут представлять собой неизвестные риски или опасности.
- Я буду принимать честную критику моей технической работы и честно критиковать других, а также должным образом сообщать о заслугах других людей.
- Я буду следовать примеру, поддерживая высокие нравственный стандарт и степень профессионализма в выполнении всех своих обязанностей. Я буду поощрять коллег и сослуживцев следовать этому этическому кодексу.

12.1.3. Руководства пользователя

В каждой организации должен быть набор руководств по допустимому использованию компьютеров организации[1]. Эти руководства могут касаться некоторых из следующих вопросов. При каких обстоятельствах допускается использование оборудования работодателя в личных целях? Какие типы использования в личных целях запрещены? Может ли сотрудник посещать обычный интернет-магазин со своего рабочего места? Может ли сотрудник писать в свой блог с работы? Как насчет использования рабочего компьютера для просмотра вебсайтов «для взрослых»? Как меняются правила, если сотрудник пользуется оборудованием компании дома?

---

[1] Интернет-провайдеры часто называют эти соглашения политикой допустимого использования (Acceptable Use Policy – AUP); в учебных заведениях они нередко называются правилами поведения пользователей (User Code of Conduct – UCC). Эти термины взаимозаменяемы.

Правила поведения должны определять и запрещать опасные или мешающие связи, объяснять, как сообщать о них и как обрабатываются эти сообщения. Иногда эти указания являются частью политики допустимого использования, рассмотренной в главе 11.

Правила поведения в учебных заведениях обычно сильно отличаются от таковых в бизнесе. Различия связаны с требованиями свободы обучения и тем, что для многих студентов университетский комплекс *является* домом.

Образцы политик можно найти через различные деловые и учебные ассоциации, у которых часто есть веб-сайты с набором политик различных организаций. Одним из таких архивов является Dijker 1999. Лучший способ написать политику – это найти архив и политику, философия которой наиболее близка к вашей, и использовать ее в качестве базового документа.

12.1.4. Правила поведения привилегированных пользователей

Некоторым пользователям для выполнения работы нужен привилегированный доступ. Возможности писать и отлаживать драйверы устройств, устанавливать программы для других людей и выполнять многие другие задачи требуют доступа с правами `root`, или правами Администратора. Организациям требуются специальные правила поведения для этих людей, потому что, как мы все знаем, привилегиями могут злоупотреблять. Эти нормы поведения должны включать следующие пункты.

- Человек признает, что привилегированный доступ предполагает ответственность за его надлежащее использование.
- Человек обещает использовать высокие привилегии доступа исключительно по служебной необходимости. Руководство должно в явном виде описать, что является таким использованием.
- Компания признает, что люди могут совершать ошибки, и обеспечивает процедуры минимизации ущерба, к которому может привести ошибка. Например, системные администраторы должны делать резервные копии перед любыми изменениями.
- Должны быть определены процедуры, предписывающие, что делать, если благодаря привилегированному доступу кто-то получает информацию, которая иначе не стала бы известной. Например, предположим, что системный администратор устраняет проблему на почтовом сервере и случайно видит сообщение, показывающее, что кто-то играет на рабочем месте в сетевые азартные игры. Как должен поступить системный администратор? Политика должна описывать, каких действий организация ждет от системного администратора.

  Рассмотрим другой пример. Допустим, привилегированный пользователь узнает о чем-то не преступном, но также важном, например, об ожидаемом слиянии. Как должен поступить системный администратор. Опять же, нормы поведения должны быть явными и должны указывать, что необходимо делать сотруднику, узнавшему важную информацию компании.
- Последствия ошибки должны быть указаны. Мы полагаем, что в данном случае лучшая политика – отсутствие наказания за ненамеренную ошибку, если о ней было своевременно и честно сообщено. Чем раньше будет сообще-

но об ошибке, тем быстрее она может быть исправлена и тем меньший ущерб она вызовет из-за цепной реакции.

- Нужно предупредить о возможных санкциях за нарушение политики, вплоть до увольнения.

Сотрудники с привилегированным доступом должны дать расписку в том, что они прочитали нормы поведения для привилегированных пользователей. Оригинал этой расписки должен храниться у руководителя сотрудника или в отделе кадров, в зависимости от существующего в организации порядка. Как сотрудник, так и его руководитель должны получить копию расписки.

В качестве эффективной меры безопасности группа системных администраторов должна отслеживать, у кого есть привилегированный доступ к каким системам. Подобная практика особенно полезна, когда нужно сообщать системным администраторам о необходимости отключить привилегии доступа, в случае если привилегированный пользователь покидает организацию. В некоторых организациях есть политика, согласно которой срок действия привилегированного доступа заканчивается через 12 месяцев, если соответствующий документ не будет подписан повторно. Эта практика предполагает регулярный пересмотр политики. Еще одним хорошим средством являются автоматические напоминания.

Том дает младшим системным администраторам, которых он нанимает, следующие инструкции:

Три правила привилегированного доступа Тома

(1) Будьте внимательны. (2) Уважайте неприкосновенность личной информации. (3) Если вы что-то испортите, сразу говорите мне.

Правило 1: Будьте внимательны.

Вы можете нанести большой ущерб, являясь пользователем `root`/Администратор, администратором базы данных и т. д., поэтому будьте внимательны. Делайте резервные копии. Сделайте паузу, прежде чем нажать клавишу Enter. Делайте резервные копии. Проверяйте групповые символы, прежде чем их применять. Делайте резервные копии. Внимательно относитесь к тому, что вы выполняете. Делайте резервные копии. Не пейте во время работы с компьютерами. Делайте резервные копии.

Правило 2: Уважайте неприкосновенность личной информации.

Не смотрите на то, что не требуется для выполнения задачи. Не «просматривайте». Не смотрите чьи-то данные, если вы не хотите, чтобы кто-то просматривал ваши аналогичные данные.

Правило 3: Если вы что-то испортите, сразу говорите мне.

Вы будете делать ошибки. Это нормально. Вы никогда не будете наказаны за честную ошибку, если скажете мне о ней, как только поймете, что не можете ее исправить. Скорее всего, исправление ваших ошибок входит в мои обязанности, и вы должны будете смотреть, как я это делаю. Чем быстрее вы мне сообщите, тем лучше будет мне, потому что мне придется меньше исправлять. Однако, если вы скроете ошибку и мне придется исправлять ее, не зная, что она была сделана, я узнаю, какая была ошибка, кто ее сделал, и у вас будут неприятности.

Нужное напоминание в нужное время

Популярная программа sudo (Snyder et al. 1986) предоставляет ограниченный привилегированный доступ к UNIX-системам. Определенные версии sudo выводят сообщение:

«Мы надеемся, что вы получили стандартные указания от вашего системного администратора. Обычно они сводятся к следующему:
1. Уважайте неприкосновенность личной информации других людей.
2. Думайте, прежде чем печатать.»

Эта программа прекрасно и своевременно напоминает людям о политике.

Имейте свидетелей

Нестабильно работающий почтовый сервер компании повреждал почтовые ящики сотрудников. Пока патч для программы не вышел, системные администраторы обнаружили, что почтовые ящики можно было исправить при помощи текстового редактора. Однако во время исправления почтового ящика системные администраторы могли видеть сообщения сотрудников. Когда был поврежден почтовый ящик генерального директора, системные администраторы столкнулись с проблемой. В отрасли происходило много слияний, и системные администраторы не хотели брать на себя ответственность, связанную со случайным ознакомлением с важным сообщением из почтового ящика генерального директора. Они решили, что за работой по исправлению почтового ящика генерального директора будет наблюдать его помощник. Таким образом, помощник видел, что системный администратор не разглядывал конфиденциальную информацию, и знал, какая часть конфиденциальной электронной почты генерального директора была просмотрена. Это защищало как генерального директора, так и системного администратора.

Иногда эти политики регулируются федеральным законодательством. Например, Комиссия по ценным бумагам США (Securities and Exchange Comission – SEC) определила правила, запрещающие мониторинг сетей, используемых на фондовом рынке, что может сильно затруднить устранение сетевых неполадок на Уолл-стрит. Федеральная комиссия связи США (Federal Communications Commission – FCC) также имеет правила, регулирующие, как телефонные операторы и технический персонал могут использовать информацию, случайно полученную во время работы. Эти люди могут обсуждать данную информацию только с ее источником и не могут использовать ее для личной выгоды.

Наконец, сами пользователи сети должны понять, что мониторинг может быть элементом обслуживания сети. Должна быть политика мониторинга и неприкосновенности личной информации, рассмотренная в разделе 11.1.2.

12.1.5. Соблюдение авторских прав

В организациях должны быть политики, в которых указано, что сотрудники обязаны соблюдать законы об авторском праве. Например, компьютерное пиратство распространено повсеместно и многие люди не понимают, что «одолжить» программу, не предназначенную для свободного распространения, на самом деле значит *украсть* ее[1].

Компании очень заботятся о том, чтобы не быть уличенными в использовании пиратского программного обеспечения. Финансовые обязательства и негативное общественное мнение не очень приятны для руководителей и акционеров. Добавьте к этому рейды, открыто проводимые организациями по борьбе с компьютерным пиратством, и получите рецепт катастрофы. Вывод: не используйте пиратских программ на оборудовании компании и не позволяйте пользователям делать это тайком.

Советовать людям не пользоваться пиратскими программами не особенно эффективно, они всегда убеждены, что то, что они делают, не является компьютерным пиратством. Многие не понимают, что является пиратством, а если и понимают, то будут ссылаться на незнание, когда их поймают. «Я думал, у нас была корпоративная лицензия». «Я не знал, что она была установлена на еще одной машине». «Мне кто-то сказал, что все нормально».

Чтобы решить эту проблему, политика соблюдения авторских прав должна представить 3–4 примера наиболее распространенных нарушений. Например, в ней можно указать, что компьютерные программы с индивидуальной лицензией должны приобретаться для отдельных компьютеров и что установочный диск не должен использоваться на нескольких машинах. Также политика может требовать, чтобы руководства и материалы для программного обеспечения хранились в одной комнате с компьютером, на котором оно установлено.

Некоторые компании наказывают сотрудников за установку любых программ без явного одобрения руководства. В качестве альтернативы и ради простоты в политике могут быть указаны программы, которые сотрудники могут свободно загружать, например новые версии Adobe Acrobat Reader или веб-броузеров. Установка программ, которые не входят в список, должна быть одобрена руководством.

Наконец, полезным может быть пункт приблизительно следующего содержания: «Мы все стараемся снизить лишние расходы, и мы ценим ваши усилия в этой области. При этом пиратское программное обеспечение является средством снижения расходов, но мы не признаем его легитимной мерой. Никому в этой компании не разрешается заниматься пиратством, если кто-либо будет устанав-

---

[1] Пиратское программное обеспечение также представляет собой средство распространения компьютерных вирусов и поэтому является проблемой безопасности. В наши дни вирусы, распространяемые с пиратскими программами, редко замечают, потому что обычно они переносятся по Интернету с помощью электронной почты. Однако справедливости ради следует заметить, что была пара случаев, получивших широкую огласку, когда вирусы распространялись посредством коммерческих, упакованных в архив программ.

ливать пиратское ПО или попросит об этом вас, пожалуйста, выполните эту процедуру».

Самый простой способ обеспечить соблюдение политики – это пойти путем наименьшего сопротивления: покупайте популярные программы с лицензиями на все рабочие станции. Вы не сможете нарушить правила, если у вас есть корпоративная лицензия. Устанавливайте их в стандартном комплекте программного обеспечения на все рабочие станции. Люди вряд ли будут искать альтернативные программы, если они без проблем могут использовать программы, на которые у вас есть лицензия. Если это нереально, в качестве другого подхода можно требовать, чтобы все заявки на покупку новых рабочих станций или серверов включали также необходимые операционные системы и приложения или лицензии на них.

Одним из главных преимуществ бесплатного и открытого программного обеспечения является то, что лицензии разрешают копирование, если не активно призывают к нему. Лицензия, которую надо соблюдать, все же существует, но обычное использование редко вызывает проблемы. Если сотрудники изменяют исходный код или используют исходный код в качестве элемента другого продукта, нужно внимательно изучить лицензию. В некоторых крупных компаниях есть выделенная группа для глобального управления соблюдением лицензий по бесплатному/открытому программному обеспечению и поиска путей более эффективного использования их вовлеченности в сообщество программного обеспечения с открытым исходным кодом.

Важно довести до людей правду жизни: при предъявлении иска о нарушении авторских прав компании редко признают свою вину. Вместо этого они привлекают к ответственности человека, который допустил это нарушение, и обвиняют в нанесении ущерба его. Укажите это в своей политике и убедитесь, что эта политика до всех доведена.

Для системных администраторов особенно важно это понять. С гораздо большей вероятностью обвиняемым будет несчастный системный администратор, который использовал лицензию разработчика на операционную систему для ввода в строй новых рабочих станций, нежели менеджер, отказавшийся вовремя подписать заказ на покупку новых лицензий. Если ваше руководство требует от вас выполнения противозаконных действий, вежливо откажитесь, в письменной форме или по электронной почте.

Простое управление лицензиями на бумаге

Администрирование массовых лицензий необязательно должно быть сложным. Однажды Том заказал 50 лицензий на право использования программы и одну копию документации и самой программы. Затем он пронумеровал 50 строк на листе бумаги и, когда кому-то требовалась программа, вписывал в строку имя этого человека. Этот лист он вложил в руководство по установке. Это решение очень эффективно работало и требовало минимальных усилий – не нужно было поддерживать базу данных и не было дополнительных расходов.

Простое отслеживание лицензий при помощи групп

Есть очень простой способ отслеживать лицензии на программное обеспечение по сети. Допустим, у вас есть лицензия на 50 копий программы, которые можно выдавать людям, когда это потребуется. Создайте в Microsoft ActiveDirectory или LDAP группу, названную по названию программы (может быть, в формате `lic_Название_программы`). Когда вы установите программу на компьютере сотрудника, внесите его в группу. Теперь вы можете сосчитать количество людей в группе, чтобы определить, сколько было выдано лицензий. Особенно приятен тот факт, что при увольнении сотрудника и удалении его учетной записи он будет удален из группы и лицензия освободится.

12.1.6. Работа с правоохранительными органами

В организациях должна быть политика по работе с правоохранительными органами, чтобы системные администраторы знали, что делать, если с ними свяжутся их сотрудники. Сотрудники правоохранительных органов иногда обращаются к системным администраторам и привлекают их для помощи в расследованиях преступлений, связанных с компьютерами, а также в делах, связанных с сексуальными домогательствами, или других случаях, где необходимы доказательства. В таких ситуациях естественной реакцией может быть паника, поэтому, а также для того, чтобы избежать нарушения закона или политики компании, системным администраторам нужна соответствующая процедура. Вообще говоря, хорошая идея – работать с правоохранительными органами через руководителя. В одной компании была следующая процедура:

Если с вами связались правоохранительные органы

1. Расслабьтесь. Будьте спокойны.
2. Будьте вежливы (*у системных администраторов часто бывают проблемы с отношением к власти, и им нужно напоминать, что грубить следователю – плохо*).
3. Передайте дело своему руководителю. Можно сказать следующее: «В соответствии с нашей политикой мы охотно сотрудничаем с правоохранительными органами. Я должен сказать об этом своему начальнику. Не могли бы вы оставить свой телефон, чтобы он вам позвонил?» (*Сотрудники правоохранительных органов всегда дадут свой номер телефона. Шутники и аферисты – нет.*)
4. Если вы руководитель, свяжитесь с юридическим отделом для консультации.
5. Записывайте все требования, все телефонные звонки, связанные с обсуждением этих требований, и все введенные команды.

6. Системный администратор, собирающий доказательства, должен передавать их в юридический отдел, который, в свою очередь, предоставит их правоохранительным органам, если руководитель не даст других указаний. (*Такая политика защищает системного администратора.*)
7. Если с вами связалась внутренняя корпоративная служба безопасности, доказательства необходимо передать руководителю, который должен предоставить их сотрудникам службы безопасности. Будьте вежливы, разъясняя эту политику корпоративной службе безопасности: «Мы всегда выполняем требования вашего отдела. Однако политика нашего отдела предписывает мне собрать эти материалы и передать их моему начальнику, а затем он передаст их вам. Связаться с моим начальником можно...»

Организация *обязана* проверять личность человека, который говорит о себе как о сотруднике правоохранительных органов, прежде чем сообщать ему *что-либо вообще*, в том числе имя и контактную информацию вашего руководителя. Проводите эту проверку даже до того, как подтвердите, что вы системный администратор. Лучший способ – сказать человеку, что вам требуется проверить его личность. Спросите номер телефона человека и номер коммутатора службы, затем позвоните на номер коммутатора и попросите этого человека к телефону. Если вы сомневаетесь в том, что номер коммутатора соответствует действительному, проверьте его по телефонному справочнику.

Если вы не проверите личность человека, утверждающего, что он сотрудник правоохранительных органов, это может привести к катастрофе. К несчастью, некоторые злоумышленники выдают себя за сотрудников правоохранительных органов, когда воруют информацию компании, применяя тактику, называемую *социальной инженерией*. Она работает следующим образом.

1. Для начала собрать небольшое количество информации.
2. Позвонить, представившись сотрудником правоохранительных органов или новым работником компании.
3. Использовать небольшое количество информации для получения более полезной информации. Повторить то же самое с новой информацией.
4. Повторять предыдущие шаги, пока информации не будет достаточно для нанесения серьезного ущерба.

Неудавшаяся попытка социальной инженерии

Однажды молодому, наивному системному администратору позвонил некто и представился сотрудником местной полиции. Человек заявил, что он проверяет, как местные компании обеспечивают безопасность своих компьютерных сетей, в рамках программы помощи сообществу. Он задал несколько конкретных вопросов, на которые системный администратор охотно ответил.

В течение следующих нескольких дней некоторым сотрудникам компании звонил тот же человек, на этот раз представляясь новым сотрудником их группы компьютерной безопасности. Конечно, создавалось впечатление, что он разбирается в системе. К счастью, одна женщина попыталась проверить его личность, и, когда это ей не удалось, она связалась с руководи-

телем группы системных администраторов. В результате руководитель предупредил всех сотрудников компании, что действует мошенник и никто не должен раскрывать важную информацию по телефону, а о любых необычных запросах на важную информацию нужно сообщать руководителю. Эти действия остановили деятельность мошенника.

Если бы злоумышленник продолжил свои поиски, он мог бы воспользоваться своими методами для получения доступа к корпоративной сети. Например, когда он выдавал себя за сотрудника группы обеспечения безопасности, это казалось правдой, потому что он так много узнал о системе безопасности компании от доверчивого системного администратора. Если бы он продолжил, то мог бы собрать достаточное количество маленьких частиц информации, чтобы получить на их основе полный доступ к системе.

Настоящие сотрудники правоохранительных органов и персонал компании предоставят информацию для проверки их личности, и они не будут противиться, когда вы попросите их об этом.

Иногда потенциальные социальные инженеры разрабатывают свои планы, начиная с информации, найденной в мусорных баках и мешках, что называется «мусорологией». Они ищут все, что может помочь им нанести ущерб вашей компании: имена, номера телефонов или информацию о проектах.

Представьте, что злоумышленник находит в мусорном баке с бумагами компании бланк с упоминанием о таинственном «проекте Зет» в научно-исследовательском отделе. К нему прикреплен список людей, работающих над проектом, и их телефонных номеров. Злоумышленник воспользуется этим начальным материалом и описанной тактикой телефонных звонков, чтобы получить от ничего не подозревающих сотрудников все, что только можно. Такие люди способны добиться очень приятного впечатления во время телефонного разговора и могут достичь успеха, если сотрудники не будут бдительны. Злоумышленник может выдавать себя за нового сотрудника в проекте Зет, который работает с [вставьте имя кого-либо указанного в списке] и пытается узнать, как создать учетную запись, разобраться в подробностях удаленного доступа и т. д. Как только учетная запись будет создана, человек сможет войти прямо в ваши системы. Мораль этой истории заключается в том, что нужно сказать людям, чтобы они были осторожны, разговаривая по телефону, и уничтожали документы, которые могут содержать важную информацию, даже если они считают это глупым.

Если вы обслуживаете интернет-шлюз своей организации, то вероятность того, что с вами свяжутся сотрудники правоохранительных органов, гораздо выше. Если правоохранительные органы связываются с вами регулярно, пора подумать о рационализации процедур по работе с ними, чтобы избежать ошибок или положения обвиняемого. Вы можете пройти обучение в юридическом отделе и создать процедуру, которая позволит вам самостоятельно разбираться с охранниками правопорядка, и просто уведомлять юридический отдел о том, что было их обращение. Таким образом, юридическому отделу не потребуется все время направлять ваши действия. Конечно, исключительные случаи все равно нужно передавать в юридический отдел. В лучшем случае проблема быстро устраняется и в будущем жалобы не возникают. Однако у интернет-провайдеров и компаний по веб-хостингу могут быть продолжительные цепочки проблем.

Не будьте слишком услужливы

Как-то раз одна компания запустила демоверсию веб-службы, которая позволяла людям анонимно просматривать веб-страницы. Взломщики пользовались этой службой, чтобы наносить ущерб другим сайтам. К сожалению, правоохранительные органы сумели отследить сервер с программой сохранения анонимности. Это было плохо. Когда возникала проблема, правоохранительные органы связывались с системным администратором, который передавал сообщение всем, кто пользовался службой. После этого он забывал о проблеме, думая, что она решена. Его интернет-соединение совместно использовали много служб, поэтому, будучи типичным перегруженным работой системным администратором, он только через некоторое время заметил, что многократные обращения правоохранительных органов связаны с одной и той же службой.

Системный администратор беспокоился из-за недостатков службы, но также хотел угодить своим клиентам. Он посоветовал группе, как изменить службу, чтобы воспрепятствовать ее злонамеренному применению, но группа не послушалась его. Скоро обращения правоохранительных органов стали отнимать у него больше времени, так как его начали вызывать в суд. Неудивительно, что он стал очень раздражительным и сломался морально.

В конце концов он понял, что пытался решить эту проблему на неправильном уровне. Он обратился к своему руководителю, и тот согласился, что системный администратор не должен брать на себя ответственность за проблемы, вызванные одним из его пользователей, особенно учитывая, что он сделал эффективные предложения по исправлению службы. Он имел полномочия для того, чтобы потребовать от пользователя исправления программного обеспечения, или отключить его в течение 30 дней. Руководитель также решил, что лучше направлять обращения правоохранительных органов в юридический отдел, чтобы обеспечить их более грамотное рассмотрение.

Юридический отдел корпорации отключил службу в течение нескольких минут после того, как узнал о ситуации, не дожидаясь, пока пройдет целых 30 дней. Они были шокированы тем, что проблеме вообще позволили существовать.

Все это говорит о том, что системный администратор должен был с самого начала жестче вести себя с клиентами. Если он не имел решительности или полномочий отключить клиента, то должен был передать проблему в юридический отдел, который обошелся бы с клиентом гораздо суровее. Мораль этой истории – нужно быть строже с людьми, которые вредят вашей компании, даже если они клиенты. Если они становятся «хулиганами», лучше найти «хулигана» посильнее, который поможет вам с ними справиться.

Вне зависимости от того, что вы думаете о правилах, вы обязаны выполнять требования корпоративной службы безопасности. Если вы считаете эти требования неудобными, обратитесь к руководителю, не разбирайтесь в ситуации сами.

Паника с логами принтера

С молодым системным администратором, который обслуживал систему печати в крупной компании, связалась служба корпоративной безопасности. Для расследования дела о сексуальном домогательстве службе безопасности требовались логи, связанные с тем, что было напечатано на конкретном цветном принтере. Упомянутый принтер находился в здании, в котором работал системный администратор, а это означало, что он может знать подозреваемого. Системный администратор запаниковал. Он собрал все логи с этого принтера и переписал их на свой компьютер дома. Затем он удалил логи на работе. Наконец он обратился за советом к двум друзьям: «Кого-то могут уволить! Что мне делать?» Оба друга дали ему один совет: чтобы его самого не уволили, нужно восстановить логи и дать службе безопасности то, что она требовала. Скрывая доказательства, он поставил себя в опасное положение и стал выглядеть соучастником подозреваемого.

12.2. Тонкости

В данном разделе рассмотрено формирование ожиданий и несколько примеров ситуаций, с которыми вы можете столкнуться.

12.2.1. Формирование ожиданий по неприкосновенности личной информации и мониторингу

Установление политики неприкосновенности личной информации и мониторинга является принципиальным этическим вопросом. В данном разделе особое внимание уделяется необходимости все время напоминать пользователям об этой политике и ее последствиях.

Формирование ожиданий сотрудников в плане неприкосновенности личной информации важно, потому что ставить людей в ситуацию, когда они не знают законов, по которым живут, несправедливо. Наказывать людей за нарушение правила, о котором им никогда не говорили, жестоко.

Есть много способов сформировать ожидания. При найме нужно потребовать от сотрудников дать расписку в том, что они прочитали указания по неприкосновенности личной информации и мониторингу. Также компании могут требовать от сотрудников давать такие расписки ежегодно. Время от времени компании должны переиздавать положения о неприкосновенности личной информации в сводках новостей или бюллетенях[1]. Размещение краткого содержания политики на видном месте или даже фраза «Все сеансы открыты для мониторинга», отображаемая на каждом экране входа в систему, может быть более эффективным, чем наличие длинной политики, находящейся на веб-сервере, на который никто не заходит.

Оставлять сотрудников не информированными о правилах, касающихся неприкосновенности личной информации, может быть опасно для бизнеса. Пользо-

[1] Чтобы избежать путаницы в том, была ли политика изменена или просто переиздана, настаивайте на присвоении политикам номеров версий, а также указании дат.

ватели системы, которые не понимают, с какими рисками связаны их действия, не могут управлять этими рисками. Представьте, что пользователи будут обсуждать подробности патентованной деловой информации по электронной почте, которую считают безопасной. Если она не является таковой, возможна утечка информации. Из-за своей неосведомленности они подвергнут компанию ненужному риску.

В финансовом сообществе электронная почта регулярно просматривается на предмет нарушения норм Комиссии по ценным бумагам[1], например биржевых операций с использованием конфиденциальной (инсайдерской) информации. Угроза просмотра может быть достаточной для предотвращения нелегального обмена конфиденциальной информацией по электронной почте. Конечно, можно просто перевести операции с использованием инсайдерской информации обратно на каналы, которые труднее контролировать, например телефон. Однако это решение принимается Комиссией по ценным бумагам, а не вами.

Компании электронной коммерции и любые компании, ведущие международный бизнес, должны обращать внимание на законы о неприкосновенности личной информации, так как они различны в разных странах. Например, если вы работаете с гражданами ЕС, есть строгие нормы относительно того, как вы должны защищать личную информацию. Американские законы предполагают аналогичную ответственность (см. раздел 12.1).

Формирование ожиданий также защищает репутацию системных администраторов, поскольку недостаток информации приведет к тому, что пользователи будут предполагать худшее. Однажды у Тома был пользователь, который раньше работал в компании, где системного администратора уволили за чтение электронной почты других сотрудников. После этого пользователь считал, что все системные администраторы читают чужую электронную почту. Однако некоторые пользователи полагают, что электронная почта каким-то магическим образом является безопасной, и подвергаются неразумному риску, отправляя по электронной почте, например, данные о своих зарплатах. В компаниях, где смотрят реально на компьютерные сетевые системы, наиболее важные данные хранятся на сменных носителях – например, USB-«флэшках» или перезаписываемых CD/DVD, – а не размещают ее на сетевых файловых и почтовых серверах.

Так как сменные носители представляют собой простой способ для выноса данных с территории компании либо могут быть утеряны или украдены во время транспортировки, политика должна касаться и этих вопросов. Например, у продавцов очень распространено копирование своей адресной книги электронной почты и списка контактов на сменный носитель для дополнительного резервного копирования. Также часто случается, что эти резервные копии остаются у них после увольнения, хотя политики запрещают оставлять конфиденциальную информацию, просто потому, что «все так делают». Если ваша политика устанавливает другую планку, убедитесь, что руководство хочет ее поддерживать.

---

[1] В России это ФСФР, Федеральная служба по финансовым рынкам. – *Примеч. науч. ред.*

Пример: перенаправление электронной почты

В компании была либеральная политика, разрешающая перенаправление электронной почты бывших сотрудников на их новые адреса электронной почты в течение года. Политика создавала проблемы, потому что конфиденциальная деловая информация часто массово рассылалась по спискам, которые не обновлялись с целью удалить уволенных сотрудников. Все думали, что электронная почта внутри компании была безопасной, даже если сообщения рассылались по всему подразделению. Пока всем в компании не рассказали об этой проблеме, сотрудники не знали, что они рисковали безопасностью, рассылая массовые сообщения.

Лучшая политика – установить системы автоматического ответа с сообщением, включающим новый адрес электронной почты человека и явное указание, что сообщение отправителя не было перенаправлено. К сожалению, из-за угрозы сбора адресов электронной почты спамерами сейчас лучше просто указать, что учетная запись была удалена, и не писать никакого нового адреса электронной почты.

Сейчас у людей часто имеется личная электронная почта вне работы, поэтому такое уведомление уже не является необходимым.

12.2.2. Указание поступить незаконно/безнравственно

Ни одна глава об этике не была бы полной без обсуждения вопроса, что делать, если ваш руководитель просит вас совершить что-то незаконное, безнравственное или противоречащее правилам компании. Мы надеемся, что вам никогда не понадобится информация этого раздела, но лучше быть подготовленным и понимать потенциальные проблемы, чем быть застигнутым ими врасплох.

Самое важное, что нужно помнить в этой ситуации, – необходимо записывать события. Ведите записи, отражающие, когда делаются такие требования, когда происходят связанные с ними телефонные звонки, какие команды вы вводите для их выполнения и т. д. Записи – ваш друг.

Мы рекомендуем простой процесс: проверьте требование – может быть, вы неправильно его поняли; проверьте, является ли оно незаконным или противоречащим политике компании, – посмотрите в политике или спросите у кого-нибудь совета; если требование противоречит политике, вежливо отстаивайте свою точку зрения и открыто откажитесь выполнять требования.

Если руководитель настаивает, вы можете согласиться с ним, обратиться к вышестоящему руководству или сделать и то и другое одновременно. Во многих компаниях есть уполномоченный по рассмотрению жалоб, с которым вы конфиденциально сможете обсудить такие ситуации. В жестко регулируемых отраслях, например в финансовой сфере, есть четко определенные указания, что делать дальше. Даже в небольшой фирме у вас есть возможность обратиться в отдел кадров или юридический и сообщить, что вы в ситуации, в которой вам требуются указания.

Полезный прием – попросить оформить требование в письменной форме или в виде сообщения электронной почты. Это дает вам документ и заставляет человека письменно подтвердить свое требование. Если требование было правомерным, но неправильно понятым, его просмотр в сообщении электронной почты может прояснить ситуацию.

Человек, требующий чего-то безнравственного и знающий об этом, не оформит это в письменном виде. Это может положить конец сомнительному требованию. Однако трудно попросить оформить требование в письменной форме, чтобы это не звучало конфронтационно. Для большинства руководителей просьба повторить требование в письменном в виде или по электронной почте звучит как неподчинение. Вместо этого вы можете попросить: «Не могли бы вы мне отправить по почте напоминание, чтобы я смог посмотреть ваше требование после обеда?» Если человек не согласится, вы можете сказать, что сообщение требуется вам, чтобы удостовериться в том, что вы правильно понимаете требование. Если и это не получится, вам придется раскрыть свои карты: «Либо я не понимаю вашего требования, либо вы требуете от меня сделать что-то сомнительное». Затем предложите, чтобы к беседе присоединился кто-то еще, например ваш руководитель, руководитель вашего руководителя или любой другой, кого это напрямую касается.

Просьба прочитать чью-то электронную почту

Давайте рассмотрим эту ситуацию на вымышленном примере: начальник отдела Боб просит вас прочитать электронную почту начальника отдела Элис, чтобы узнать, не планирует ли ее отдел отменить проект, на который сильно рассчитывает отдел Боба. Хорошим ответом будет переспросить, чтобы убедиться, что вы поняли просьбу правильно: «Что вы просите меня сделать?»

Если требование подтверждается, проверьте, противоречит ли оно политике компании, найдите соответствующий пункт в указаниях вашей организации по неприкосновенности личной информации и мониторингу. Вежливо проверьте, понимает ли человек, что просит поступить безнравственно: «Может быть, я вас не расслышал?[1] Вы имеете в виду, что я должен...», и укажите, что это противоречит политике.

Воспользуйтесь политикой для вежливого напоминания Бобу. Боб может рационально обосновать свою просьбу, объясняя, что Элис отменила другие решения и что он пытается только помочь вам, потому что знает, что вы тоже рассчитываете на этот проект.

На этом этапе вам нужно принять решение. Вы можете временно уйти от ответа и поговорить с уполномоченным по рассмотрению жалоб, сотрудником службы корпоративной безопасности или руководителем Боба. Вы можете согласиться с требованием, но это делает вас соучастником. В дальнейшем Боб может потребовать чего-то еще, возможно, намекнув, что, если вы не согласитесь, он расскажет о предыдущем случае, утверждая, что вы сделали это по своей инициативе. Он также может утверждать, что, если вы не согласитесь, он просто найдет кого-то еще, кто это сделает. Эта тактика является очень опасной для того, кто пытается убедить человека что-то сделать.

Очевидно, что мы не можем принять решение за вас. Однако мы можем дать вам следующий совет: когда вы сомневаетесь, следует ли вам что-то делать, полу-

[1] Или, если требование было сделано по электронной почте, «Я думаю, что мог что-то перепутать или неправильно понять вашу просьбу...».

чите требование в письменной форме и записывайте, что конкретно вы делаете. Никогда не действуйте по устным указаниям, которые считаете сомнительными. Даже если вы думаете, что все может быть нормально, получите требование в письменном виде. Это важно не только для того, чтобы оградить себя, но и для того, чтобы помочь человеку, выдвигающему требование, удостовериться в том, что он действительно этого хочет. Если человек не хочет давать требование в письменном виде, то он не желает нести за него ответственность. В ваших записях должно быть указано время, требование, кто его сделал, почему это было сделано и что было сделано. Кроме того, отмечайте все необычное, что касается требования. Обычно люди жалеют о том, что не вели записи, когда уже слишком поздно. Логи с автоматическими временными метками обеспечивают лучшую отчетность и исключают утомительность ведения записей.

12.3. Заключение

Этика – это принципы поведения, которые регулируют действия людей. Для многих людей само слово *«этика»* является неопределенным и пугающим. Надеемся, что мы предоставили вам несколько руководящих принципов, которыми вы можете воспользоваться, и не ущемили вашу свободу сделать свой собственный выбор.

Этический кодекс системного администратора направлен на повышение профессионализма и улучшение имиджа системных администраторов, он устанавливает стандарт поведения. Политики, которые создает организация, должны включать нормы поведения пользователя сети/компьютера, нормы поведения пользователя с привилегированным доступом, политику соблюдения авторских прав и политику работы с правоохранительными органами. Принцип согласия, основанного на полученной информации, определяет, что у нас должна быть политика мониторинга и неприкосновенности личной информации, в явном виде доведенная до всех пользователей. В случае отсутствия санкций за нарушения и последовательной поддержки эти политики бесполезны.

Предварительное обдумывание возможных ситуаций помогает вам лучше подготовиться к ним. Постарайтесь подумать о потенциальных этических дилеммах, с которыми вы можете столкнуться, и о том, что вы будете делать в этих случаях. Это может быть хорошей темой для периодического обсуждения на собраниях персонала или во время обеда. Оно должно проходить в присутствии вашего руководителя, чтобы вы могли способствовать пониманию официальной политики.

Надеемся, главное, что вы усвоили из этой главы, – это следующее: если вы находитесь в непонятной ситуации, лучший способ защитить себя – вести записи. Просите оформить требование в письменной форме, чтобы создать запись о нем, записывайте, когда вы получаете телефонные звонки, записывайте, что вас просят делать и что вы делаете. Записывайте все!

Задания

1. Опишите ситуацию, в которой Этический кодекс системного администратора или принцип согласия, основанного на полученной информации, мог бы повлиять (или повлиял) на ваши действия.
2. Дайте примеры ситуаций, когда вы или ваша группа требовали соблюдения политик, о которых не знали ваши пользователи. Особенно подумайте

об области условий допустимого использования, совместного использования и доступности общих ресурсов и мониторинга системы. Как бы вы улучшили свою работу в этой области?

3. Вспомните случай, когда вы или другой системный администратор действовали не совсем профессионально. Как бы вы поступили, если бы знали об Этическом кодексе системного администратора?
4. Какие из рассмотренных в данной главе политик есть в вашей компании? Если вы работаете в крупной компании с корпоративными политиками, есть ли в вашем отделе собственные политики?
5. Охарактеризуйте политики, упомянутые в предыдущем вопросе, как легкие или строгие. Дайте примеры. Как бы вы изменили их и почему?
6. Спросите трех пользователей, знают ли они, где найти любой документ с политиками, упомянутыми в данной главе.
7. Представьте, что вы устраняли проблему и случайно услышали или прочитали, что ваш сослуживец продавал в офисе наркотики. Как бы вы поступили? А если бы человек планировал подрывную деятельность в компании? Воровал расходные материалы из офиса? Воровал оборудование для перепродажи на интернет-аукционе? Изменял супругу с начальником? А если бы этот человек был не вашим сослуживцем, а руководителем высокого уровня?
8. Какое время вы храните различные логи вашей системы (принтера, входа-выхода и т. д.)? Какое время вы хранили бы их, если бы попали в ситуацию с логами принтера из раздела 12.1.6? Почему?
9. Представьте, что вы работаете с веб-сайтом компании электронной коммерции. Инженер, не имеющий достаточных навыков или терпения для правильного тестирования своего кода в среде разработки, просит вас показать ему его логи на машине для сетевого обслуживания, а затем разрешить ему ненадолго изменить параметр ведения логов, чтобы получить больше информации. Вы можете этого сразу и не осознать, но у вас появится инженер, ведущий разработку на функционирующих узлах сетевого обслуживания. Как бы вы разобрались с этой ситуацией? Как бы вы могли ее предотвратить?
10. Руководитель просит вас выделить кому-то дополнительное дисковое пространство. Вы отвечаете, что у вас нет места, но он говорит: «Освободите пространство, этот человек важный». Через некоторое время он просит сделать то же самое для другого человека и говорит: «Вы сделали это для предыдущего человека, этот не менее важен». Как бы вы разобрались с этой ситуацией? Как бы вы могли ее предотвратить?
11. Сотрудница, не являющаяся системным администратором, имеет привилегированный доступ к своей рабочей станции, потому что это требуется для программ, которыми она пользуется. Друзья просят ее создать учетные записи в ее системе. Это противоречит политике, но она все равно выполняет просьбу. Один из ее друзей начинает заниматься незаконной деятельностью на рабочей станции. Как бы вы разобрались с этой ситуацией? А если бы сотрудник, нарушивший политику, стоял выше вас на служебной лестнице? Был бы равным вам по должности? Как бы вы могли предотвратить эту проблему?

Глава 13

Службы поддержки

Данная глава представляет собой общий обзор служб поддержки: что это такое, как их организовать, как ими управлять и т. д. Обработка обращений в службу поддержки рассмотрена в следующей главе.

Служба поддержки – это место, реальное или виртуальное, где люди могут получить ответы на свои вопросы о компьютерах, сообщить о проблемах и запросить новые услуги. Это может быть физическое помещение, куда люди могут прийти, или виртуальная служба поддержки, доступ к которой является электронным.

Нет ничего важнее, чем ваша служба поддержки, – это лицо вашей организации. Персонал службы поддержки производит первое впечатление на ваших пользователей и поддерживает ваши отношения с ними, хорошие или плохие. Персонал службы поддержки решает ежедневные проблемы, которые являются неотъемлемой частью мира современных компьютеров. Это те люди, которых зовут, когда у пользователей что-то случается. Хорошая служба поддержки достойно представляет вашу организацию. Типичный пользователь видит в вашей организации только службу поддержки и часто думает, что это и есть ваша организация. Пользователи не думают о том, какую работу делают сотрудники, которые не общаются с клиентами, и об инфраструктуре. Коротко говоря, служба поддержки нужна для помощи пользователям. Не забывайте о слове *«поддержка»* в названии «служба поддержки».

13.1. Основы

Главное, что вам нужно сделать, чтобы служба поддержки работала, – сначала организовать ее, а затем придать ей дружественный вид. Служба поддержки должна иметь достаточное количество персонала, чтобы справляться с нагрузкой; определенную область работы; рабочие процессы для персонала; процесс для передачи проблемы на более высокий уровень, когда дела идут плохо; а также программы отслеживания вызовов.

13.1.1. Организуйте службу поддержки

Служба поддержки есть в каждой организации. Она может быть физической, например располагаться в служебном помещении, или виртуальной, например по телефону или электронной почте. Иногда служба поддержки является неофициальной, когда каждый день часть времени системных администраторов тратится на непосредственную помощь пользователям.

Если в компании имеются всего один-два системных администратора, часто официальная служба поддержки отсутствует, но это бывает недолго. С ростом организации небольшие группы системных администраторов становятся большими, а из больших групп образуются корпоративные подразделения. Организации редко понимают, что им нужна формальная служба поддержки, пока не становится слишком поздно.

Мы считаем, что когда дело касается создания формальной службы поддержки, то чем раньше это будет сделано, тем лучше. Лучшее время – за 9 месяцев до того, как вы поймете, что должны были сделать это 6 месяцев назад. Организациям, не имеющим доступа к устройствам для путешествий во времени, требуются другие методы. Организации растут при помощи планирования, и создание формальной службы поддержки должно быть частью такого планирования. Если рост медленный, то вы можете просто ждать характерных признаков. Одним из таких признаков является следующий: системные администраторы начинают замечать, что их группа выросла до того предела, с которого начинаются проблемы в общении. Кроме того, системные администраторы могут заметить, что они не могут завершить работу по проекту, потому что их работу постоянно прерывают запросы пользователей. Обычно системные администраторы могут решить, что будет лучше, если один системный администратор будет отвлекаться утром, а днем сосредоточится на работе над проектом, а другой – наоборот. Если вы подумываете о такой структуре, то вы находитесь на пути к созданию формальной службы поддержки.

Переход от помощи по необходимости к формальной службе поддержки может быть неудобным для клиентов. Системные администраторы должны быть к этому готовы и приложить все усилия, чтобы упросить этот переход. Понятное доведение до людей процедур новой службы поддержки очень важно.

Рассказывайте людям об изменениях

При создании формальной службы поддержки, физической или виртуальной, нужно объяснять людям, что происходит. Когда в компании Lumeta было менее десяти сотрудников, большинство из них занимались компьютерной поддержкой сами, а Том вмешивался при более серьезных проблемах. В конце концов компания выросла и в ней появилось три системных администратора, в том числе специально выделенный для решения проблем, связанных с компьютерами и вопросами других сотрудников. Этот человек был службой поддержки во всех случаях. Пользователи не понимали, что у системных администраторов была разная специализация. Это раздражало как системных администраторов, которым надоедали не предназначенные для них вопросы, так и пользователей, которым не нравилось, что любой системный администратор не мог помочь во всех ситуациях. Проблема была решена, когда по электронной почте было разослано сообщение, разъясняющее, к каким системным администраторам нужно обращаться по разным видам проблем; это сообщение два раза подряд повторялось на еженедельных собраниях персонала. Вы можете предотвратить потенциальную неразбериху, разослав такое объявление одновременно с введением изменений.

Облегчайте переход

В подразделении из 75 человек была сеть, отделенная от централизованного, корпоративного IT-подразделения. Люди, много знавшие о системах, выполняли больше обязанностей системных администраторов, другие – меньше. Одна сотрудница с техническим образованием, по имени Карен (имя изменено), занималась резервными копиями и знала, как выполнять бóльшую часть установок и других частично автоматизированных задач. Практически по всей пользовательской документации было разбросано указание «Сначала отправьте Карен сообщение по электронной почте». В результате изменений в бизнесе подразделению в конце концов потребовалась централизованная поддержка, которую имели другие подразделения в этом здании. Пользователей раздражало, что вместо того, чтобы написать Карен, они теперь должны были писать в «поддержку». Пропал элемент непринужденности в общении. Вместо того чтобы прямо разобраться с эмоциональной проблемой, руководство просто продолжало заставлять людей поступать по новой схеме.

Карен была очень влиятельным лицом в подразделении, потому что все ее знали, и если бы она захотела, то смогла бы легко поднять волну недовольства. Она не стала частью новой схемы, ее просто «выпихнули», поэтому она почувствовала себя не у дел. В конце концов она уволилась, и, прежде чем новая система поддержки была полностью принята пользователями, прошло два года.

Проблем можно было бы избежать, если бы переход был организован лучше, с пониманием того, к чему привыкли пользователи, и интеграцией этой системы в новый процесс.

Службы поддержки необязательно должны быть настоящими физическими объектами, они могут быть виртуальными. О проблемах можно сообщать по электронной почте и так же получать ответы. Кроме того, можно использовать системы обмена текстовыми и голосовыми сообщениями, которые позволяют людям непосредственно общаться друг с другом без помощи телефона.

Системы самостоятельной помощи также популярны, но не должны рассматриваться как замена систем, которые предполагают общение с человеком. Учитывая распространенность Интернета, нужно обязательно иметь по крайней мере простое хранилище документации для пользователей по таким вопросам, как получение помощи, активация услуги и решение распространенных проблем. Можно воспользоваться простым одностраничным веб-сайтом со ссылками на важные документы, википедией, или даже блогом с возможностью поиска (одна запись на часто задаваемый вопрос). Веб-системы позволяют пользователям помогать себе самостоятельно, предоставляя документацию, списки часто задаваемых вопросов и ответов на них и оперативную помощь. Эти системы могут снизить загрузку персонала службы поддержки, но не способны обеспечить интерактивную отладку и решить рабочие вопросы, требующие взаимодействия в реальном времени. Должен быть номер телефона, по которому можно позвонить, чтобы сообщить о возможном сбое системы самостоятельной помощи.

13.1.2. Будьте дружелюбны

Служба поддержки должна иметь дружественный вид. В случае физической службы поддержки дизайн интерьера должен быть приятным и гостеприимным. Виртуальная служба поддержки должна быть в равной степени гостеприимной, что часто предполагает дизайн, использующий успокаивающие цвета, читаемые шрифты и список наиболее часто просматриваемых тем в левом верхнем углу первой страницы.

Лица сотрудников также должны быть дружелюбными и приветливыми, как и их характеры. Некоторые люди обладают личностными качествами, подходящими для работы с клиентами, другие их не имеют. Это должно учитываться при найме персонала. Атмосфера, создаваемая персоналом, будет отражать атмосферу, создаваемую администратором. Администратор, который кричит на подчиненных, обнаружит, что подчиненные кричат на клиентов. Добродушный администратор, который не прочь посмеяться и всегда дружелюбен, будет привлекать соответствующий персонал, что отразится на отношении к пользователям. Проще сразу создать атмосферу дружелюбия, чем потом поднимать плохую репутацию. Короче говоря, если вы администратор, будьте таким же дружелюбным, каким хотите видеть свой персонал. Будьте примером для подражания.

13.1.3. Отражайте корпоративную культуру

Вид и функции вашей службы поддержки должны отражать корпоративную культуру. Часто мы видим, что служба поддержки не имеет авторитета в компании, когда люди, которые там работают, не поддерживают корпоративную культуру. Например, культура очень строгой и формальной компании может отражаться в соответствующей манере одеваться и способах ведения бизнеса, а люди в службе поддержки носят футболки с надписями и джинсы и откуда-то сзади слышатся звуки видеоигры. Небольшой опрос выявит, что служба поддержки имеет репутацию кучки разгильдяев вне зависимости от того, насколько усердно они работают или качества обслуживания, которое они обеспечивают.

Случается и обратное. Когда Том работал в Bell Labs, его сослуживцы были очень креативными, свободомыслящими личностями. Требования к внешнему виду выражались фразой «вы должны быть одеты», а отношения были очень непринужденными. Группа системных администраторов Тома являлась связующим звеном между этими исследователями и корпоративным IT-подразделением. Каждый раз, когда эти две группы людей взаимодействовали напрямую, ситуация напоминала эпизод из плохой юмористической телепередачи.

Уделите время рассмотрению культуры и «посмотрите» на культуру своей службы поддержки в сравнении с культурой пользователей, которых они обслуживают. Постарайтесь развить культуру, которая подходит обслуживаемым пользователям.

13.1.4. Имейте достаточно персонала

Служба поддержки может быть полезной, только если в ней есть достаточное количество людей для своевременного обслуживания пользователей. Иначе люди будут искать помощи в других местах.

Определение численности персонала службы поддержки затруднительно, потому что оно изменяется от случая к случаю. В университетах, как правило, на одного сотрудника службы поддержки приходятся тысячи студентов. В корпоративных службах поддержки соотношение иногда выше, а иногда ниже. В среде компьютерных исследований соотношение часто равно 40:1 и системные администраторы первого уровня обычно имеют такой же опыт, как системные администраторы второго уровня в других службах поддержки, чтобы удовлетворять более высокому техническому уровню вопросов. В компаниях электронной коммерции обычно существуют отдельная службы поддержки для внутренних вопросов и служба поддержки «по работе с клиентами» для помощи в решении проблем оплачивающим клиентам. В зависимости от предоставляемых услуг соотношение может быть 10 000:1 или 1000 000:1.

Вопрос о правильном соотношении часто бывает тупиковым. Руководство всегда будет настаивать на более высоком соотношении, пользователи – на более низком. Вы всегда можете повысить соотношение, предоставляя пользователям меньше услуг, что обычно обходится организации дороже, поскольку пользователям приходится тратить время на выполнение обязанностей системных администраторов, а делают они это неэффективно.

Лучше уделить внимание не соотношению количества пользователей и сотрудников, а уровням интенсивности вызовов и времени обслуживания вызова. Например, вы можете отслеживать уровень занятости телефона службы поддержки, время, в течение которого пользователи ждут ответа на свое сообщение электронной почты, или время, которое требуется на решение проблемы, – естественно, за вычетом времени «ожидания пользователя», как упоминается в разделе 16.2.6.

При таком подходе основное внимание уделяется вопросам, более важным для пользователя. Соотношение числа пользователей и сотрудников является косвенной единицей измерения пользы для клиентов. В управлении, основанном на метрике, лучше использовать прямые единицы измерения.

Управление ресурсами на основе интенсивности вызовов также предполагает более разнообразный набор потенциальных решений. Вместо одного решения – управления численностью персонала – компании могут вкладывать средства в процессы, которые позволяют пользователям помогать себе самостоятельно, без вмешательства сотрудников. Например, можно создать новую систему автоматизации, позволяющую пользователям выполнять задачи, которые раньше требовали привилегированного доступа, предоставить сетевую документацию, автоматическое подключение новых услуг через веб-интерфейсы и т. д.

Для принятия решений о развитии процессов вам потребуются соответствующие метрики. Они могут показать хорошие варианты для автоматизации, документирования или обучения как системных администраторов, так и клиентов. Метрики могут выявить, какие процессы более эффективны, какие интенсивно используются или не используются вообще.

Пример: люди-броузеры

Неправильное обеспечение большей самостоятельности пользователей может иметь негативные последствия. Одна компания создала веб-сайт для предоставления простого доступа ко всей документации и часто за-

даваемым вопросам, ранее находившимся в компетенции службы поддержки. Изучая логи этого сайта, руководство обнаружило интересную закономерность. Сначала сайт был очень популярен. Его посещали пользователи. Интенсивность телефонных звонков снизилась, и все шло по плану. Однако к третьему месяцу логи показали новую тенденцию – выросло количество посещений сайта самой службой поддержки. Расследование показало, что люди снова стали звонить в службу поддержки, а ее сотрудники читали ответы с веб-сайта. Сотрудники службы поддержки работали как люди-броузеры! Ситуация была урегулирована, когда сотрудникам службы поддержки дали указание стараться отправлять людей на соответствующую веб-страницу, а не давать ответы напрямую. Пользователям порекомендовали заходить на сайт, прежде чем звонить в службу поддержки.

13.1.5. Определите полномочия поддержки

В службе поддержки должна быть политика, определяющая полномочия поддержки. Этот документ разъясняет, за что отвечает группа системных администраторов и за что она не отвечает. Элементами полномочий являются вопросы *что*, *кто*, *где*, *когда* и *как долго*.

- *Что* поддерживается: только компьютеры или сама локальная сеть? Все компьютеры вне зависимости от используемой ОС или только определенные ОС и определенные версии? Как решаются проблемы с неподдерживаемыми платформами?
- *Кто* будет поддерживаться: конкретное подразделение, здание, отдел, предприятие, университет? А если у человека есть офисы в разных зданиях, каждое из которых имеет свою службу поддержки? Только люди, которые платят? Только люди определенной должности и выше (или ниже)?
- *Где* находятся пользователи? Этот вопрос аналогичен вопросу *кто*, если вы поддерживаете, например, всех пользователей в конкретном здании или месте. Однако вопрос *где* также включает поддержку путешествующих пользователей, посетителей внешних филиалов, пользователей на демонстрационных выставках и сотрудников, работающих на дому.
- *Когда* предоставляется поддержка: часы работы с 8 до 18 ч? С понедельника по пятницу? Как решаются проблемы в остальное время? Должны ли люди ждать, пока служба поддержки откроется, или существует механизм, позволяющий обратиться к системным администраторам дома? Если в нерабочее время поддержки нет, что должно делать руководство хозяйственных отделов в случае пожара?
- *Какое время* должно тратиться на выполнение среднего требования? Некоторые категории требований должны выполняться немедленно, остальные должны занимать определенное время. Установление этих нормативов формирует ожидания персонала и пользователей. Пользователи предполагают, что все делается немедленно, если им не сказать, что определенные задачи выполняются дольше (см. раздел 31.1.3). В иерархической структуре должны быть перечислены определенные задачи, выполняемые быстро (5 мин), медленно (1 ч) и долго (требуют создания новой службы).

Наличие письменной политики полномочий поддержки – один из лучших подарков руководства группе системных администраторов. Без нее группа либо будет перегружена работой, стараясь сделать все для пользователей, либо будет выводить пользователей из себя, отказывая в решении насущных вопросов. Если вы руководитель, то ваша обязанность – четко объяснить, когда можно отказать и когда нельзя, в письменной форме и довести это до всех, кто с вами работает. Также эта политика должна быть общедоступна на внутреннем вебсайте для формирования ожиданий пользователей.

Когда мы консультируем перегруженных работой системных администраторов, мы часто узнаем, что у них нет письменной политики полномочий поддержки. Мы призываем системных администраторов создавать письменные отчеты о том, что они делают в течение недели, и записывать все незавершенные задачи. Демонстрация этого списка руководителям часто заставляет их понять, что подчиненные слишком сильно загружены работой над задачами, которые не являются приоритетными для подразделения. Часто руководители удивляются, когда узнают, что системные администраторы, в сущности, выполняют работу своих пользователей за них. Создание политики, определяющей полномочия поддержки, позволяет персоналу четко определять приоритеты группы.

Когда мы работаем с группами системных администраторов, которые приобрели репутацию черствых грубиянов, мы часто видим, что корень проблемы – отсутствие письменной политики полномочий. В этом случае наличие письменной политики устанавливает более высокую планку обязанностей группы.

Без письменной политика системные администраторы просто следуют набору устных указаний, а новые системные администраторы работают в соответствии с тем, что слышат от сотрудников своей группы. Новый системный администратор, стараясь помочь, может создать прецедент, не понимая, что тем самым он идет против неформальной политики. Еще хуже, если он испортит то, что не надо было трогать, или окажет медвежью услугу другому подразделению.

Пример: широкие полномочия, малые обязанности

Полномочия поддержки также предполагают определенные обязанности. Инженерный отдел компании по компьютерному проектированию в Нью-Джерси полностью располагался в одном здании. Политика службы поддержки предполагала помощь по любым вопросам, но системные администраторы имели четко определенную ответственность. Это работало, потому что они понимали, где их обязанности заканчиваются. Они полностью отвечали за определенные вопросы: если кто-то сообщал о проблеме с рабочей станцией, системный администратор устранял ее. По другим вопросам системные администраторы отстаивали интересы пользователей: если случалась проблема с WAN-соединением, которое они не контролировали, они брали на себя ответственность за связь с корпоративным сетевым центром и контроль за исправлением неполадки. С другими проблемами они действовали как служба перенаправления: при сообщении о перегоревшей лампочке в офисе они передавали его руководству хозяйственного отдела и не брали на себя ответственность по контролю за выполнением требования. Они стали информационным центром по запросам.

Для экономии средств региональный офис продаж располагался в том же здании. Служба поддержки финансировалась инженерным отделом, а не офисом продаж, поэтому ответственность по обслуживанию персонала офиса продаж была другой. Служба поддержки могла порекомендовать сотрудникам офиса продаж обратиться к необходимой документации или рассказать, где они могли пройти обучение, но они не могли оказывать помощь в настройке машин для демонстраций или презентаций. Персонал офиса продаж пользовался центральным сервером электронной почты, который поддерживался инженерной группой, поэтому поддержка электронной почты была полной, только если сотрудник пользовался почтовым клиентом, который поддерживался инженерной группой. Однако обычно были ограничения по поддержке персонала офиса продаж, потому что она была бесплатной.

Наличие четко определенных обязанностей защищало службу поддержки от выполнения большего объема работ, чем она могла выполнить, позволяя при этом обеспечивать очень дружественную систему перенаправления. Кроме того, политика полномочий не позволяла группе продаж злоупотреблять обслуживанием, предоставляя службе поддержки возможность сказать «нет», мотивированное требованиями руководства.

В службе поддержки должен быть продуманный процесс обработки требований, которые касаются технологий, не входящих в круг ее полномочий. Служба поддержки может просто сказать, что выполнение этого требования не входит в ее полномочия, и отказаться помогать, но это недружественный ответ. Гораздо лучше в явном виде указать, чем служба поддержки может, а чем не может помочь человеку, а затем предоставить небольшую помощь, заранее предупредив об ограничении по времени. Например, вы можете сказать: «Мы не поддерживаем системы с этой видеокартой, но я попытаюсь помочь вам в течение 30 мин. Если я не смогу решить вашу проблему, то вам придется решать ее самостоятельно». Вы можете потратить на решение проблемы 45 мин, а затем вежливо сказать пользователю, что исчерпали свой лимит времени. Пользователь оценит ваши усилия.

Формируйте ожидания, работая вне обычных полномочий

Одна из любимых историй Джея Стайлса (Jay Stiles) произошла до того, как DHCP сделал настройку сети автоматической. Какое-то время он работал в компании, где одна группа техников устанавливала в офисах сетевые розетки, а другая настраивала компьютеры для подключения к сети. Клиенты часто просили первую группу техников настроить им компьютеры. Техники не были обучены этому, но иногда соглашались под давлением настойчивых просьб. У них это редко получалось, и, пытаясь настроить компьютер, они часто нарушали другие конфигурации. Когда они совершали такие ошибки, вызывали их начальника и он оказывался в сложной ситуации: как отвечать на жалобу на сотрудника, который не должен был выполнять эту задачу и не сделал ее правильно?

Потом техники поняли, что, когда их просили настроить компьютер, они должны были прервать свою работу, отойти от машины и объяснить: «На самом деле это не входит в мои обязанности, но я немного знаю об этих компьютерах и могу попробовать. Но если я не справлюсь, то мне придется попросить вас подождать людей, которые должны это сделать. Хорошо?» Если они говорили эти волшебные слова, результат существенно отличался. Если у них получалось, пользователь был очень рад, зная, что техник выполнил работу, не входящую в его обязанности. Если не получалось, пользователь тоже был доволен, потому что техник хотя бы попытался.

Начальник начал получать благодарные звонки: «Техник пытался настроить мой компьютер и не смог, но я хочу поблагодарить его за то, что он так старался!»

Все дело в том, как себя позиционировать.

13.1.6. Указывайте, как получить помощь

Дополнением к полномочиям поддержки являются указания по получению помощи. Этот документ объясняет пользователям, как получить помощь: по телефону, электронной почте, при помощи системы заявок и т. д. Те или иные типы запросов могут направляться в определенные отделы, либо универсальная служба поддержки может быть единой точкой соприкосновения, которая перенаправляет требования в соответствующие отделы.

Такой документ должен содержать максимум несколько сотен слов. В идеальном случае на каждом новом компьютере должна быть более короткая версия, которая умещается на стикере. Можно добавить на фоновый рисунок Windows по умолчанию следующий текст: «IT-служба поддержки [Название компании]: [номер телефона], [адрес электронной почты], [веб-сайт]».

Это одна из наиболее важных вещей, которые может сделать руководство IT-отдела, чтобы помочь персоналу в распределении времени. Если пользователи не получили явного указания правильного способа получения помощи, они будут связываться с системными администраторами напрямую, отрывая их в неудобное время и тем самым делая невозможным завершение крупных проектов. Или, что еще хуже, с системными администраторами будут связываться дома!

13.1.7. Определите процессы для персонала

У персонала службы поддержки должны быть четко определенные процессы, которые он будет соблюдать. В небольшой системе это не так важно, потому что процессы в основном являются несистематизированными и недокументированными, поскольку используются людьми, которые их создали. Однако в крупной организации процессы должны быть документированы.

В очень больших службах поддержки в качестве элемента обучения используются *сценарии*. Каждая поддерживаемая услуга имеет соответствующую цепь диалога, которая должна соблюдаться при поддержке этой услуге. Например, сценарий по обработке запроса на услугу удаленного доступа собирает соответ-

ствующую информацию и указывает оператору, что делать, будь то прямое подключение удаленного доступа или перенаправление запроса в соответствующую обслуживающую организацию. Сценарий для запроса о сбросе пароля должен из соображений безопасности требовать от пользователей подтверждения своей личности, возможно, знанием уникальной личной информации, прежде чем устанавливать новый пароль.

В главе 14 рассмотрены формальные процессы, которыми сотрудники службы поддержки могут пользоваться для обработки отдельных жалоб на неполадки.

13.1.8. Создайте процесс передачи проблемы на более высокий уровень

Передача проблемы на более высокий уровень – это процесс, при котором проблема передается от текущего персонала кому-то с более высоким уровнем знаний и опыта. Первая линия операторов должна уметь справляться с 80–90% всех обращений и передавать остальные сообщения на второй уровень поддержки. На этом уровне люди могут иметь больше опыта, больше знаний и, возможно, другие обязанности. В крупных организациях может быть до четырех и более уровней, на более высоких уровнях могут привлекаться люди, которые создали или поддерживают рассматриваемую службу.

Распространено правило, по которому первый уровень поддержки должен передавать на более высокий уровень все обращения, время выполнения которых составляет не менее 15 мин. Однако тогда проблема ложится на плечи сотрудников второго уровня поддержки, которые могут работать над проектами, и в результате у них будет на это меньше времени. Эту ситуацию можно разрешить, если назначить одного сотрудника поддержки второго уровня, который каждую неделю будет работать с сотрудниками первого уровня, то есть на неделю сделать его рабочим проектом службу поддержки. Хотя сотрудники более высоких уровней обычно не любят такую политику, в достаточно крупной организации им потребуется заниматься этим только приблизительно раз в 6 недель. Положительным побочным эффектом этой стратегии является то, что персонал первого уровня будет учиться у сотрудника второго уровня. Кроме того, сотрудник второго уровня лучше поймет типы вопросов, поступающих в службу поддержки, что поможет определить, какие новые проекты больше всего помогут сотрудникам первого уровня и пользователям.

Также процесс передачи на более высокий уровень применяется пользователями, когда они не удовлетворены получаемой поддержкой. Все надеются, что это будет происходить как можно реже, но всегда найдется кто-то, кто захочет поговорить с руководителем. Служба поддержки должна быть к этому готова. Большое количество обращений, передаваемых на второй уровень, – признак более крупной, системной проблемы. Обычно это показывает, что персоналу первого уровня требуется дополнительное обучение или у них нет средств для нормального выполнения своей работы. Если руководству передается большое количество обращений, в работе службы поддержки могут быть системные проблемы.

Передача запроса как самоцель

Передача запроса на более высокий уровень должна существовать не просто для успокоения рассерженных пользователей. Служба поддержки

одного небольшого интернет-провайдера часто получает звонки от рассерженных людей, которые хотят поговорить с менеджером. В таком случае человек, поднявший трубку, передает ее своему соседу слева, который говорит, что он менеджер. Хотя это работает в краткосрочной перспективе или при бурном росте бизнеса, мы не думаем, что это надежный способ работы службы поддержки.

13.1.9. Письменно определите «экстренный случай»

Это может показаться простым, но письменное определение того, что является экстренным случаем, может стать политическим конфликтом. Оно может быть частью более крупного документа об уровне обслуживания или отдельной политикой, созданной, чтобы помочь персоналу службы поддержки принять правильное решение. Это определение часто включено в политику передачи проблемы на более высокий уровень.

Часто мы видим, что системные администраторы перегружены работой, поскольку каждый пользователь заявляет об экстренном случае, который требует немедленного внимания. У системных администраторов, которые считают, что пользователи говорят такие слова, чтобы манипулировать ими, ухудшается моральное состояние и повышается уровень стресса. Наличие письменной политики позволяет системным администраторам знать, когда выражать несогласие, и предоставляет им документ, на который при необходимости можно сослаться. Если пользователь все еще будет не согласен с этой оценкой, системный администратор может передать вопрос кому-то в вышестоящем руководстве, кто может принять решение. Это позволяет системному администратору сосредоточиться на технических обязанностях, а руководству – на установке приоритетов и предоставлении ресурсов.

Каждая компания должна уметь определить, что такое экстренный случай. На заводе экстренный случай – это все, что останавливает сборочную линию. В веб-службе или у интернет-провайдера экстренным случаем может быть все, что не позволяет обслуживанию соответствовать SLA. Торговая организация может определить экстренный случай как все, что не позволяет запустить демонстрацию, внести в базу данных квартальные прибыли или рассчитать комиссионные сборы. В учебном заведении с жестко установленным графиком занятий, которые нельзя просто перенести или задержать из-за сбоя системы, экстренным случаем может быть все, что способно повредить запланированным занятиям, зависящим от технических средств, а также нарушить другие мероприятия в течение учебного года: прибытие новых студентов, сроки экзаменов, публикацию оценок, сроки окончания набора новых студентов и т. д.

Планируйте хорошо

В канцелярии колледжа, где учился Том, висел плакат с надписью: «Ваше плохое планирование не является экстренным случаем». Студентам это не нравилось, но плакат не убирали. Фактически это утверждение было одним из наиболее важных уроков, которые университет мог преподать своим студентам, прежде чем они попадут в реальный мир.

13.1.10. Предоставьте программу отслеживания заявок

Каждой службе поддержки нужна какая-то программа для помощи в обработке заявок. Альтернативой ей является ведение записей на бумаге. И хотя для начала это удобно и вполне достаточно для компаний с одним или двумя системными администраторами, это решение не масштабируется. Заявки теряются, а у руководства нет возможности контролировать процесс для лучшего распределения ресурсов. Это первое, что необходимо для программы службы поддержки. С ростом службы поддержки программа может помочь в других областях. Сценарии, рассмотренные в главе 13.1.7, могут отображаться автоматически и быть «интеллектуальными», являясь элементом процесса сбора информации, а не просто статичным экраном.

Программа службы поддержки должна поддерживать назначение заявкам какой-либо формы приоритета. Это не только помогает оправдать ожидания пользователей, но и позволяет системным администраторам лучше планировать свое время. Системный администратор должен уметь легко перечислить важнейшие заявки, которые были ему переданы.

Другой важный аспект программы состоит в том, что она ведет логи, где записывается, кем были сделаны те или иные заявки. Статистический анализ таких логов может быть полезен в управлении службой поддержки. Однако, если программа не собирает такую информацию, вы не сможете воспользоваться преимуществами такой статистики. Это часто происходит при большом количестве личных и телефонных обращений. В таких случаях может быть удобна функция программы, которая позволяет записывать часто повторяющиеся вопросы или заявки в специальной форме, открывающейся одним щелчком мыши. Для заполнения полей с информацией о пользователе можно использовать определитель номера.

Программа службы поддержки также может автоматизировать сбор данных по удовлетворенности пользователей. Каждый день программа может делать случайную выборку вчерашних пользователей и опрашивать их о качестве обслуживания.

Пример: от хорошего к плохому

В компании-разработчике программного обеспечения около 1500 человек пользовались улучшенной версией бесплатной системы отслеживания заявок. Она была очень простой в использовании и поддерживала несколько различных интерфейсов, самым популярным из которых был интерфейс электронной почты. Система отслеживала пользователя, отдел, категорию, состояние, адресата заявки, время, потраченное на ее выполнение, исполнителя, приоритет, дату выполнения и т. д. Собственные скрипты обеспечивали метрику, которой руководство могло воспользоваться, чтобы оценить, как идет работа. Пользователи могли посредством веб-интерфейса просмотреть историю своих заявок и другие связанные с ними записи. Кроме того, пользователи могли посмотреть очередь заявок сотрудника и место их заявки в списке приоритетов. И хотя система не была идеальной, всем было удобно пользоваться ею и все могли получать с ее помощью необходимую информацию.

Группа управления информационными системами (Management Information System – MIS), которая обеспечивала поддержку баз данных и приложений, работавших на самом высоком уровне, и не была частью группы системных администраторов, получила задание на создание новой системы отслеживания заявок для центра поддержки пользователей. Руководство этой группы расширило сферу действия проекта, чтобы сделать его единой унифицированной системой отслеживания заявок, которая использовалась бы также производственной группой, MIS и группой системных администраторов. Ни в MIS, ни в производственной группе не было системы отслеживания заявок, поэтому они разрабатывали систему, не зная, что такое хорошая система. Никому в группе системных администраторов о проекте не сказали, поэтому ее потребности и потребности пользователей, обслуживаемых ею, не были учтены при проектировании.

Была создана система с графическим пользовательским интерфейсом (Graphical User Interface – GUI), которая, однако, не имела интерфейсов электронной почты и командной строки. Создание новой заявки проходило через десяток различных всплывающих окон, которые появлялись медленно и которые нужно было перетаскивать мышью, чтобы навести на экране хоть какой-то порядок. Обновление заявки вызывало появление пяти или шести различных всплывающих окон. Для многих системных администраторов с модемным доступом из дома система была очень медленной. Она не работала с Mac или UNIX, так как клиент был сделан только под Microsoft Windows. Часто на то, чтобы открыть заявку, требовалось больше времени, чем на решение проблемы, поэтому многочисленные мелкие заявки больше не отслеживались. То, что когда-то было быстрым процессом, основанным на электронной почте, стало десятиминутным усилием. Несколько системных администраторов вернулись к отслеживанию проектов на бумаге или в голове.

Пользователи жаловались на то, что больше не могут видеть состояние своих заявок или их положение в очередях приоритетов. Также они были недовольны тем, что больше не могли открыть заявку через электронную почту и что новая система отправляла им слишком много сообщений, когда в заявке изменялось небольшое поле. Обо всех этих недостатках группа системных администраторов заявила сразу, как только им внезапно представили новую систему, которой они должны были начать пользоваться, но было слишком поздно что-то менять.

Предполагалось, что система предоставит лучшие средства для создания более точной метрики. Однако, поскольку многие данные больше не вводились в систему, это было не так, даже несмотря на то, что предоставляемые ею средства для метрики были неплохими.

Очень важно, чтобы программа службы поддержки была подходящей для рабочего процесса людей, которые ею пользуются. Если в неделю делается одна заявка, то долгое время создания заявки допустимо. Однако, если вы ожидаете сотни заявок в день, создание новой заявки должно быть почти мгновенным, как отправка электронной почты. Не используйте программу службы поддержки для представления кардинально новых принципов работы.

Выбор программы для службы поддержки – непростое дело. Большинству программ потребуется серьезная адаптация к вашей системе. Когда вы примете решение вложить средства в программу службы поддержки, будьте готовы вкладывать их также и в адаптацию, чтобы системные администраторы могли эффективно ее использовать. Если пользоваться программой будет трудно, они не будут ее использовать или станут прибегать к ней только для крупных проектов.

13.2. Тонкости

Теперь, когда у нас есть надежная служба поддержки, последние штрихи помогут нам расширить ее по многим различным направлениям: качество, сфера действия, прозрачность политики и масштабирование.

13.2.1. Статистические усовершенствования

О службе поддержки можно собирать более сложные статистические данные. Вы можете отслеживать количество передач заявок на более высокий уровень, чтобы определить, где требуется дополнительное обучение персонала. Однако при обсуждении с высшим руководством вопросов бюджета и планирования лучше использовать ретроспективную статистику. Вы можете добиться выделения бóльших средств, если сможете показать многолетние тенденции роста количества пользователей, интенсивности звонков, типов звонков, предоставляемых услуг и удовлетворенности клиентов. Когда вас попросят о поддержке новой технологии или службы, вы можете использовать прошлогодние данные, чтобы оценить возможные затраты на поддержку.

Ценность статистики растет с ростом организации, потому что руководство становится все менее вовлеченным в работу непосредственно. В небольших организациях обычно сложнее собрать статистику, потому что методы работы часто являются менее автоматизированными и не могут быть приспособлены для сбора данных. С ростом организации становится проще собирать статистику, а ее сбор становится более важным.

Определите самых активных подателей 10% заявок

Системные администраторы обычно любят подробности. Статистика обходит подробности, чтобы найти общие тенденции. Поэтому системные администраторы часто являются не самыми лучшими людьми для сбора статистических данных о заявках в службу поддержки.

Том был в замешательстве, когда его попросили собрать статистические данные о системе заявок службы поддержки. Чтобы составить полезную статистику, сначала нужно было бы изменить программу, чтобы она записывала, сколько времени ушло на обслуживание заявки, классифицировала типы работ и указывала отдел, для которого работа выполнялась. В дальнейшем, собирая эти данные в течение года, он мог бы создать отличные схемы и графики для полного анализа.

Проблема была в том, что начальнику нужен был ответ в течение 24 ч. Его начальник предложил совершенно другой подход: процесс можно

упростить, если предположить, что выполнение всех заявок занимает одинаковое время. Том был в ужасе, но в конце концов убедился в том, что в среднем выполнение всех заявок требовало среднего времени.

Затем его начальник предложил создать запрос в базе данных, который определял бы, кто подал больше всего заявок. Оказалось, что в прошлом году три пользователя создали 10% всех заявок.

Вместо того чтобы тщательно классифицировать все заявки, Том и его начальник ознакомились с небольшим количеством заявок каждого из трех наиболее активных пользователей и поговорили с системными администраторами, которые больше всего им помогали. Они узнали, что один человек постоянно требовал помощи для продукта, не входившего в число требуемых для работы, и системные администраторы все равно ему помогали. Руководитель проявил твердость и сказал системным администраторам, что данный продукт не поддерживался намеренно, потому что это было слишком хлопотно. Дальнейшие запросы должны были отклоняться. Руководитель обратился к пользователю и сказал ему, что тот должен либо решать свои проблемы самостоятельно, либо позволить службе поддержки помочь ему перейти на стандартный для корпорации продукт. Обычно служба поддержки не обеспечивала такую услугу перехода, но в данном случае она бы ее поддержала.

Второй из наиболее активных пользователей задавал много элементарных вопросов. Руководитель Тома поговорил с руководителем пользователя о том, что этот человек должен пройти дополнительное обучение. Руководитель пользователя был поражен уровнем помощи, который требовался сотруднику, и позаботился об этой проблеме.

Третий пользователь, мягко говоря, заставлял системных администраторов делать свою работу. Вопрос был передан его руководителю, и тот позаботился о его решении.

При отсутствии какой-либо статистики некоторые основные грубые оценки все-таки оказались очень полезны. Один лишь этот прием позволил избавиться приблизительно от 10% всех заявок, поступавших в систему. Это серьезное улучшение!

13.2.2. Поддержка в нерабочее время и в режиме 24/7

Так как компьютеры становятся критически важными для все большего числа бизнес-процессов, пользователи чаще просят поддержки в режиме 24/7. И хотя в некоторых организациях может потребоваться полная поддержка в три смены, некоторые способы обеспечения поддержки в режиме 24/7 не так дороги.

Можно создать голосовой почтовый ящик, который при поступлении новой корреспонденции отправляет сообщение на пейджер. Этот пейджер различные сотрудники могут по очереди передавать друг другу. Обязанностью сотрудника может быть не исправить проблему, а просто сообщить о ней компетентному человеку либо звонить разным людям, пока не найдет кого-нибудь, способного помочь. Это требует, чтобы у всех сотрудников были номера домашних телефонов остальных.

Другой вариант этого подхода – все руководители групп пользователей должны знать телефонный номер администратора службы поддержки, который будет по очереди вызывать системных администраторов, пока кого-нибудь не найдет. Такой подход имеет преимущество за счет распространения личной информации среди меньшего количества людей, но может утомить администратора службы поддержки и не учитывает его отпуска. Однако можно решить и этот вопрос, например, разделив эту обязанность между двумя администраторами.

Вы также можете относиться к этому вопросу так, как в других отраслях относятся к пожарной и другим системам сигнализаций, потому что современный эквивалент ночного пожара в исследовательской лаборатории – это сбой главного сервера. Персонал обеспечения безопасности на заводах всегда имеет список телефонов на случай аварии, пожара и т. д. и звонит, начиная с верха списка, пока кого-нибудь не найдет. В зависимости от ситуации этот человек может сказать охраннику, к кому обратиться.

Поддержка в нерабочее время в T. J. Watson

В конце 1990-х годов предприятие IBM T. J. Watson расширило процедуру действий при пожаре и других авариях на основные компьютерные системы. Если в основном компьютере происходил сбой, пользователи могли позвонить на пост охраны и сообщить о проблеме. У охранников был специальный список сотрудников, которым нужно звонить в случае проблем, связанных с компьютерами.

Вне зависимости от того, как с системным администратором связываются в нерабочее время, этому человеку нужно компенсировать затраченное время, иначе стимула устранять проблему не будет. Некоторые организации доплачивают за время на вызове сумму, рассчитанную в полуторакратном размере от зарплаты сотрудника. В других организациях могут применяться другие способы компенсации времени, официальные или неофициальные[1].

13.2.3. Лучшая реклама службы поддержки

Хорошо, если ваши политики определены, а объявления общедоступны на вебсайте. Однако вряд ли кто-то будет искать их, чтобы прочитать. В данном разделе мы рассмотрим, как обеспечить, чтобы ваши политики и объявления были прочитаны и поняты.

С появлением Сети стало легко обеспечить доступность всех политик всем пользователям. Это обязательно. Однако вы должны привлечь пользователей на свой сайт. Некоторые организации системных администраторов обзавелись веб-порталами, где представлены все службы, политики и документация. Сообщите своим пользователям о таком способе получения важной для них информации – и они будут знать, где искать информацию, важную для вас.

Составьте правильный текст сообщения. Общайтесь с пользователями, чтобы выяснить, что для них важно. Трудно заставить людей читать что-то, что не

[1] Например, сотруднику предоставляется отгул на такое же время – или в некоторых случаях в полтора раза большее – без вычета времени из отпуска.

важно для них. Какая им разница, будет ли сервер `server3` работать в выходные? Но сообщение о том, что база данных на сервере `server3` в выходные не будет доступна, привлечет их внимание.

Новые политики можно рассылать пользователям по электронной почте или в бумажном виде, если они особенно важны. Порталы могут выделять «политику месяца». Если сообщение выиграет от повторения, разместите в подходящих местах плакаты. Часы работы физической службы поддержки должны быть указаны на всех входных дверях. Люди проводят много времени, разглядывая стены в ожидании своей очереди; заполните эти пустые стены сообщениями, которые вы хотите донести до посетителей. Плакаты, на которых написано «Меняйте свой пароль раз в 30 дней!» или «Сервер `server3` будет выведен из эксплуатации 1 мая» дают хорошие советы и предупреждают о грядущих изменениях.

Сообщения наиболее эффективны, когда их получают в нужное время. Если `server3` через месяц выводится из эксплуатации, говорите это людям каждый раз, когда они пользуются им.

13.2.4. Различные службы поддержки для предоставления обслуживания и решения проблем

С ростом организации может иметь смысл создать две отдельные группы службы поддержки: одну для заявок на новые услуги, а другую – для сообщения о проблемах, которые появляются после того, как служба будет успешно активирована. Часто обеспечением новых услуг занимается третья группа, особенно если это требует физического труда. Третья группа может быть внутренней службой поддержки, в которую могут обращаться монтажники всей организации, чтобы передать на более высокий уровень проблемы с установкой. Хотя часто бывает, что эта третья группа является вторым уровнем одной из других служб поддержки.

Выгода от такого разделения службы поддержки в том, что три или четыре группы могут работать под управлением различных администраторов. Администратор может эффективно управлять только ограниченным количеством людей. Такое разделение рабочей силы явно показывает, чем управляют разные администраторы. Они все должны отчитываться перед одним руководителем, чтобы обеспечивались наличие связи и отсутствие перекладывания вины.

Другое преимущество создания нескольких групп в том, что их сотрудников можно отдельно обучать различным навыкам, необходимым для выполнения их задач. Это дешевле, чем нанимать людей, имеющих достаточно опыта для выполнения всех задач.

Предоставление услуги – процесс, который должен быть одинаковым для всех клиентов. Первоначальный сбор данных может осуществлять кто-то, обученный задавать правильные вопросы. Этот человек может иметь больший опыт продаж, чем другие сотрудники. Решение проблем установки – это узкотехнический вопрос, и обучение может быть адаптировано к этой ситуации. Отдельная служба поддержки для сообщения о проблемах требует персонала с более серьезным техническим опытом. Такое разделение рабочей силы очень важно для роста организации до очень крупных размеров.

Наличие веб-системы заявок на предоставление новых услуг может исключить ввод большого объема данных и предотвратить ошибки. Если данные вводит

пользователь, это снижает количество опечаток, которые могут быть вызваны вводом данных третьим лицом. Система может обеспечивать проверку распространенных ошибок и отклонять непоследовательные или конфликтующие запросы. При поступлении заявок по телефону можно посоветовать подателю заявки заполнить соответствующую веб-форму.

Для поддержки этих функций не нужно создавать полностью новую программную систему. Данные формы могут просто отправляться в обычную систему отслеживания заявок, которая затем будет их обрабатывать.

13.3. Заключение

Для ваших пользователей служба поддержки – это то, как они вас видят, как получают обслуживание и как решаются их проблемы. Это самый важный элемент вашей репутации. Для вас служба поддержки – это средство, которое необходимо создать, как только ваша организация вырастет до определенного размера, и которое впоследствии послужит для разделения рабочей силы по мере увеличения числа сотрудников. Служба поддержки не нужна небольшим организациям, но есть определенная точка роста, на которой она становится полезной, а затем – критически важной.

Служба поддержки – это «лицо» вашей организации, поэтому сделайте его счастливым и дружелюбным, вне зависимости от того, является служба поддержки физической или виртуальной. Правильное определение размера службы поддержки очень важно и влияет не только на ваш бюджет, но и на удовлетворенность пользователей. При планировании службы поддержки вы должны определить, что поддерживается, кто поддерживается, где они находятся, когда вы предоставляете поддержку и в течение какого времени пользователи могут ожидать выполнения средней заявки. Создание точных планов по финансированию и набору персонала упрощается за счет сбора статистики, рассмотренного в разделе 13.1.10.

Для персонала должны быть определены процессы, определяющие, как будет обеспечиваться поддержка различных услуг и как проблемы станут передаваться на более высокий уровень. Для сбора статистики по всем заявкам и отслеживания проблем, на которые поступило более одной заявки, должны использоваться программные средства.

После обеспечения всего вышеперечисленного служба поддержки может развиваться в других областях. Можно организовать поддержку в нерабочее время, лучше рекламировать политики, а при серьезном росте службу поддержки можно разделить на отдельные группы для предоставления новых услуг и сообщения о проблемах.

Мы многое обсудили в данной главе, и каждый вопрос в той или иной степени касался общения. Служба поддержки – это то, как пользователи общаются с вашей организацией, и часто задача вашей службы поддержки – доводить до пользователей как, когда и почему что-то сделано. Такое общение влияет на то, какой будут считать вашу компанию – дружественной или недружественной. Собранная статистика помогает во время планирования довести до руководства потребности организации. Процедуры передачи вопросов на более высокий уровень позволяют направить общение в новое русло, когда возникает тупиковая ситуация. Наличие письменной политики поддержки в нерабочее время

формирует ожидания пользователей и предотвращает раздражение от неожиданных звонков поздно ночью.

Задания

1. Опишите структуру персонала вашей службы поддержки.
2. Сколько сотрудников имеется в вашей службе поддержки в настоящее время? Почему было выбрано это количество?
3. Какого сотрудника службы поддержки вашей организации считают наименее дружелюбным к пользователям? Как вы это узнали? Как бы вы помогли этому человеку стать лучше?
4. Насколько тесны ваши отношения со службой поддержки? Какую статистику вы используете для управления ею или предоставляете своему руководству? Какие дополнительные статистики были бы вам полезны?
5. Выясните, какие пользователи создают 10% – или 1% для более крупных компаний – всех ваших заявок. Какие закономерности вы видите в этих заявках и как можно использовать эту информацию, чтобы улучшить вашу службу поддержки?
6. Сообщите о проблеме сегодня в 10 ч вечера. Опишите, как все прошло.

Глава 14

Работа с пользователями

В конце Второй мировой войны США оказались в ситуации сильного избытка производственных мощностей. В результате компании начали производить сотни новых продуктов, предоставляя людям и организациям беспрецедентный выбор. Тысячи людей, вернувшихся с войны, нашли работу в сфере продажи этих новых продуктов. Все вместе эти факторы обеспечили начало новой эры в американской экономике.

Вместе с выбором пришла конкуренция. Компании поняли, что просто большой системы продаж было уже недостаточно, требовалась хорошая система продаж. Они начали интересоваться тем, что отличает продавцов с хорошими результатами от всех остальных.

Эти тенденции вызвали расширение изучения процесса продаж в бизнес-школах. Исследования показали, что лучшие продавцы, понимали они это или нет, пользовались особым, структурированным методом, который включал конкретные фразы или шаги. Средние продавцы различным образом отклонялись от этих фраз или произносили некоторые фразы плохо. У продавцов с плохими результатами последовательность методов практически отсутствовала.

Методам, которые теперь были определены, можно было научить. Таким образом, навыки продаж выросли из интуитивного процесса в формальный с четко определенными элементами. Ранее обучение продажам делало акцент в основном на разъяснение характеристик и достоинств продукта. Впоследствии обучение стало включать разъяснение самого процесса продаж.

Разложение этого процесса на отдельные этапы открыло путь для его дальнейшего исследования, а значит, и улучшения. Каждый этап можно было изучить, измерить, преподать, отработать и т. д. Повысилось внимание к деталям, потому что каждый этап можно было исследовать отдельно. Кроме того, можно было изучить полную последовательность: целостный подход.

Мы думаем, что, если бы кто-то объяснял структурированный процесс продавцам с высокими результатами, это звучало бы странно. Для них это естественно. Однако для начинающих эта схема предоставляет структуру процесса, который они изучают. После того как они ее освоят, они смогут изменять или приспосабливать ее к своей ситуации. Без предварительного изучения одной структурированной системы трудно разобраться, как создать свою собственную.

В 1990-е годы системное администрирование пошло по такому же пути. Раньше оно было умением или искусством немногих людей. С бурным развитием корпоративной компьютеризации, приложений внутренних сетей и Интернета спрос на системных администраторов рос так же активно. В ответ на эти требо-

вания появилось огромное количество новых системных администраторов. Качество их работы было различным. Обучение часто проходило в форме изучения функций конкретного продукта. Другие методы обучения включали изучение инструкций и документации, обучение в процессе работы и учебные курсы при общественных и профессиональных учреждениях.

Системному администрированию требовалось развиваться в направлении, аналогичном процессу продаж. В конце 1990-х годов мы наблюдали рост академического изучения системного администрирований (Burgess 2000). На самом деле написать эту книгу нас побудила такая же необходимость обеспечить обучение, основанное на темах, принципах и теоретических моделях, подходящих для всех платформ, а не на конкретных подробностях определенных технологий, разработчиков и продуктов (Limoncelli and Hogan 2001).

14.1. Основы

Системные администраторы тратят много времени, отвечая на запросы пользователей. В данной главе мы представим структурированный процесс, определяющий, как собираются, оцениваются, выполняются и проверяются запросы пользователей[1]. Реагирование на запросы пользователей – более конкретная задача, чем общие вопросы, связанные с работой службы поддержки.

Запросы пользователей – это заявки на устранение неполадок, звонки, сообщения о проблемах, хотя в вашей компании это все может называться иначе. Эти запросы могут иметь вид «Я не могу печатать», «Сеть работает медленно» или «Программа, которая компилировалась вчера, больше не компилируется».

Системные администраторы выполняют много задач, но часто пользователи видят только ту их часть, которая включает ответ на их запросы, а не работу по выполнению служебных задач, которую они и не должны видеть. Следовательно, то, как вы отвечаете на запросы пользователей, очень важно для репутации.

Метод обработки этих запросов пользователей состоит из девяти этапов, которые можно разделить на четыре фазы:

- Фаза A: Приветствие («Здравствуйте»)
  - Этап 1: Приветствие
- Фаза B: Определение проблемы («Что случилось?»)
  - Этап 2: Классификация проблемы
  - Этап 3: Описание проблемы
  - Этап 4: Проверка проблемы
- Фаза C: Планирование и выполнение («Исправить это»)
  - Этап 5: Предложение решений
  - Этап 6: Выбор решения
  - Этап 7: Выполнение решения
- Фаза D: Проверка («Проверить это»)
  - Этап 8: Проверка исполнителем
  - Этап 9: Проверка пользователем

[1] Этот процесс основан на статье Тома (Limoncelli 1999).

Данный метод предоставляет структуру процесса, который для новых системных администраторов чаще является стихийным. Он помогает вам более эффективно решать проблемы, позволяя сосредоточиться, и избегать ошибок. Он вводит общую терминологию, которая, при условии использования ее всей группой системных администраторов, повышает взаимопонимание в группе.

Это средство не даст использующим его людям дополнительного технического опыта, но оно может помочь более молодым сотрудникам понять, как старшие системные администраторы подходят к решению проблем. Творчество, опыт, нужные ресурсы, средства, а также личное и внешнее управление все так же важны.

Если пользователи понимают эту модель, им становится проще получить необходимую помощь. Они будут подготовлены за счет знания нужной информации и при необходимости смогут даже помочь системному администратору в ходе процесса.

Как изображено на рис. 14.1, фазы обеспечивают следующее:

- Сообщение о проблеме
- Определение проблемы
- Планирование и исполнение решения
- Проверку того, что проблема решена

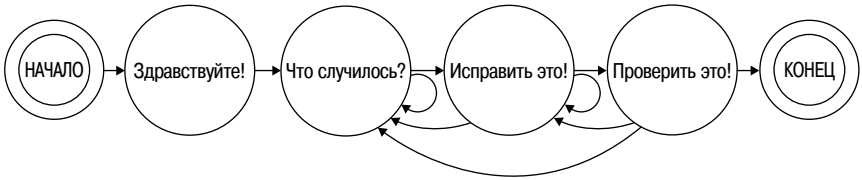

***Рис. 14.1.** Общая схема решения проблемы*

Иногда определенные этапы при необходимости повторяются. Например, в ходе этапа 4 (проверка проблемы) системный администратор может обнаружить, что проблема была классифицирована неправильно, и должен будет вернуться к этапу 2 (классификация проблемы). Это может произойти на любом этапе и требовать возврата к любому из предыдущих этапов.

Программы для отслеживания неполадок

Невозможно переоценить важность использования программных пакетов для отслеживания сообщений о проблемах. В 1980-е и в начале 1990-х годов системные администраторы редко пользовались программами для отслеживания таких сообщений. Однако сегодня установка таких программ приводит к серьезным изменениям, влияющим на вашу возможность планировать свое время и предоставлять последовательные результаты пользователям. Если вы обнаружите, что в компании нет программы отслеживания неполадок, просто установите что-то, чем вам было удобно пользоваться на предыдущем месте работы, или программу, у которой есть список интернет-адресов электронной почты активных сторонников.

14.1.1. Фаза A/этап 1: приветствие

Первая фаза состоит из одного обманчиво простого этапа (рис. 14.2). У пользователя узнают сведения о проблеме. Этот этап включает все, связанное с получением запроса пользователя. Он может изменяться от фразы «Чем я могу вам помочь?» по телефону до веб-сайта, который собирает сообщения о проблемах. На этапе 1 нужно пригласить пользователя в систему и начать процесс на позитивной, дружелюбной и располагающей ноте.

***Рис. 14.2.** Фраза приветствия*

Человек или система, отвечающие на запрос, называются **встречающим**. Встречающим может быть человек, находящийся в помещении физической службы поддержки, отвечающий по телефону, доступный по электронной почте или при помощи какой-либо технологии мгновенного обмена сообщениями; автоответчик; даже веб-форма, собирающая данные. Для простого и надежного доступа, обеспечивающего пользователю возможность сообщить о проблеме, требуются различные способы сбора данных.

Иногда о проблемах сообщают автоматизированные средства, а не люди. Например, средства сетевого мониторинга, такие как Big Brother (Peacock and Giuffrida 1988) HP OpenView и Tivoli, могут уведомлять системного администратора о возникшей проблеме. Процесс будет тем же самым, хотя некоторые этапы могут ускоряться этими средствами.

Каждая компания и каждый пользователь различны. Каждая часть каждой организации имеет свой наиболее подходящий способ сообщения о проблемах. Является ли пользователь локальным или удаленным? Опытным или новым? Является ли поддерживаемая технология сложной или простой? Эти вопросы могут помочь вам в выборе способа приветствия.

Как пользователи узнают о способах получения помощи? Представьте доступных встречающих при помощи табличек в коридорах, сводок новостей, наклеек на компьютерах и телефонах и даже при помощи баннеров на внутренних веб-страницах. Лучшие места – это те, куда пользователи уже смотрят: наклейки на их компьютерах, сообщения об ошибках и т. д.

Впрочем, этот список, конечно, не является полным, мы видели встречающих, использующих электронную почту, телефон, помещение службы поддержки, офис системных администраторов, презентацию на веб-сайтах и в собственных приложениях, а также в сообщениях систем автоматизированного мониторинга.

14.1.2. Фаза B: определение проблемы

Во второй фазе основное внимание уделяется классификации проблемы и ее записи и проверке (рис. 14.3).

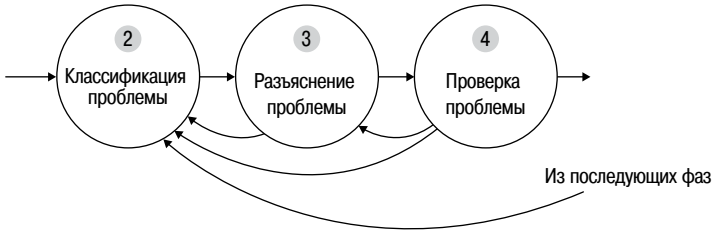

Рис. 14.3. *Что случилось?*

14.1.2.1. Этап 2: классификация проблемы

На этапе 2 запрос классифицируется, чтобы определить, кто должен с ним разбираться. Роль **классификатора** может выполнять человек, или классификация может быть автоматизированной. Например, в помещении службы поддержки для классификации проблемы персонал может выслушать ее описание. Автоответчик может попросить пользователя нажать кнопку 1 для проблем с компьютером, 2 – для проблем с сетью и т. д. Если те или иные системные администраторы помогают только определенным группам пользователей, запросы могут быть автоматически перенаправлены на основе адреса электронной почты пользователя, введенного вручную идентификационного номера сотрудника или информации телефонного определителя номера.

Если процесс не является автоматическим, обязанность человека – классифицировать проблему по описанию или задавая пользователю дополнительные вопросы. Для правильной классификации может использоваться формальное дерево решений.

Вам может потребоваться задать дополнительные вопросы, если вы мало знакомы с системой пользователя. Это часто происходит в службах поддержки компаний электронной коммерции или очень крупных корпораций.

Вне зависимости от того, как осуществляется классификация, пользователю нужно сообщить о том, к какой категории было отнесено его обращение, – благодаря обратной связи можно избежать потенциальной ошибки. Например, если классифицирующий сотрудник говорит пользователю: «Это похоже на проблему с печатью. Я передам этот вопрос кому-нибудь из нашей группы поддержки принтеров», пользователь остается вовлеченным в процесс. Пользователь может заметить, что проблема является более широкой, чем просто печать, что приведет к ее классификации как сетевой проблемы.

Если используется автоответчик, пользователь уже классифицировал запрос. Однако пользователь может быть не самым компетентным человеком для принятия такого решения. Следующий человек, который будет говорить с пользователем, должен быть готов оценить его выбор так, чтобы это не выглядело обидным. Если пользователь классифицировал запрос неправильно, это нужно вежливо исправить. Мы считаем, что лучший способ – сообщить пользователю правильный номер телефона, по которому ему следовало позвонить, или назвать кнопку, которую ему нужно нажать, а затем системный администратор должен перевести вызов на нужный номер. В некоторых компаниях выбирают один из этих подходов, но лучше сделать и то и другое.

Если классифицировать проблему просят пользователя, возможные варианты необходимо подбирать внимательно и время от времени пересматривать. Чтобы выявлять несоответствие понимания категорий классификации между пользователями и вами, вам нужно собирать статистические данные или, по крайней мере, изучать жалобы пользователей.

Поддержка пользователей в маркетинговом ключе

В меню автоответчика должна использоваться терминология, которую ожидают услышать пользователи. У одного крупного производителя сетевого оборудования меню было основано на маркетинговой терминологии подразделения линий продукции, а не на технической терминологии, которую применяло большинство ее пользователей. Это вызывало бесконечную путаницу, потому что с чисто технической точки зрения маркетинговая терминология имела мало общего с действительностью. Это было особенно актуально для пользователей любой компании, поглощаемой этой компанией, потому что продукты поглощаемой компании классифицировались по маркетинговым терминам, незнакомым ее пользователям.

На этом этапе многие заявки могут быть перенаправлены или отклонены. Пользователь, запрашивающий новую услугу, должен быть перенаправлен в соответствующую группу, которая занимается запросами на услуги. Если выполнение запроса не входит в обязанности группы поддержки, пользователь может быть отправлен в другой отдел. Если запрос противоречит политике и поэтому должен быть отклонен, то вопрос может быть передан руководству, если пользователь будет не согласен с решением. Поэтому важно иметь четко определенные полномочия обслуживания и процесс запроса новых услуг.

В очень крупных компаниях вы, скорее всего, обнаружите, что действуете от лица пользователя, обращаясь в различные отделы или даже службы поддержки тех или иных отделов. Сложные случаи, которые включают проблемы с сетями, приложениями и серверами, могут потребовать, чтобы сотрудник службы поддержки работал с тремя или более организациями. Сориентироваться вместо пользователя в этом хитросплетении связей – ценная услуга, которую вы можете ему предоставить.

14.1.2.2. Этап 3: описание проблемы

На этапе 3 пользователь разъясняет проблему во всех подробностях, и эту информацию записывает **регистратор**. Часто это делает тот же сотрудник (или система), который осуществляет классификацию. Навык, который требуется на этом этапе, – умение слушать и задавать правильные вопросы, чтобы получить от пользователя необходимую информацию. При записи нужно выявить и зафиксировать важные подробности.

В описании проблемы разъясняются ее подробности и записывается достаточное количество признаков, чтобы неполадку можно было воспроизвести и исправить. Неопределенное или неполное описание проблемы является плохим. Описание

проблемы считается хорошим, если оно полное и указаны все связанные с неполадкой аппаратные и программные средства, а также их местоположение, последнее время, когда они работали, и т. д. Иногда доступна не вся нужная информация или она является неточной.

В качестве примера хорошего описания проблемы можно привести следующее: «Компьютер talpc,example.com (с ОС Windows Vista), находящийся в комнате 301, не может печатать документы MS-Word 2006 на цветном принтере «rainbow», расположенном в комнате 314. Вчера все работало нормально. На других принтерах печатать можно. Пользователь не знает, есть ли эта проблема на других компьютерах».

Некоторые классы проблем можно полностью описать простыми методами. О проблемах маршрутизации в Интернете лучше всего сообщать, указывая два IP-адреса, которые не могут связаться друг с другом, но способны связываться с другими узлами. Указание полного маршрута между узлами, если это возможно, может серьезно помочь.

Избыток информация обычно лучше, чем ее недостаток. Однако пользователей может раздражать, когда их просят предоставить информацию, которая, очевидно, является лишней, например версию ОС, если проблема – дым из монитора. Но при этом мы постоянно видим, что веб-системы сообщения о неполадках требуют заполнения всех полей.

Бесполезно ожидать, что описание проблемы пользователями будет полным. Пользователям нужна помощь. Описание проблемы, показанное ранее, взято из реального примера, когда пользователь отправил системному администратору по электронной почте сообщение, в котором было написано просто «Помогите! Я не могу печатать». Трудно придумать более непонятную и неполную просьбу. В ответ были отправлены вопросы: «На каком принтере? С какого компьютера? Из какого приложения?».

Пользователь ответил раздраженной фразой: «Мне нужно распечатать эти слайды до 15 часов! Я улетаю на конференцию!» После этого системный администратор отказался от электронной почты и воспользовался телефоном. Это позволило пользователю и классифицирующему сотруднику общаться быстрее. Вне зависимости от средства связи важно, чтобы этот диалог прошел и чтобы об окончательном результате было доложено пользователю.

Иногда сотрудник, записывающий описание, может устроить быстрый экскурс по следующим этапам, чтобы ускорить процесс. Он может спросить, включено ли устройство в розетку, читал ли человек инструкцию и т. д. Однако такие вопросы, как «Он включен в розетку?» и «Вы читали инструкцию?», заставляют пользователей защищать себя. У них есть только два возможных варианта ответа, и лишь один из них правильный. Старайтесь избегать ситуаций, когда пользователи чувствуют, что их толкают ко лжи. Вместо этого спросите, в какую розетку включено устройство; во время телефонного разговора попросите подтвердить, что кабель хорошо укреплен на обоих концах. Скажите пользователю, что вы посмотрели инструкцию и на случай дальнейших неполадок ответ находится на странице 9.

Вы должны разговаривать с пользователем так, чтобы он никогда не чувствовал себя идиотом. Нам было противно, когда мы слышали, как сотрудник службы поддержки говорил пользователю, что «даже восьмилетний ребенок понял бы» то, что он объясняет. Вместо этого успокаивайте пользователей, говорите, что с опытом они станут лучше разбираться в компьютерах.

Помогайте пользователям не уронить своего достоинства

Находить способы общения, позволяющие пользователям сохранить свое достоинство, может быть очень полезно. Один системный администратор в Лондоне принимал звонок от человека, который был в панике, потому что не мог распечатать свои месячные отчеты на принтере, используемом практически исключительно для этой цели. После ряда проверок системный администратор обнаружил, что принтер не был включен в розетку. Он сказал пользователю, что, скорее всего, уборщики отключили принтер, когда им потребовалась розетка для пылесоса.

Спустя месяц тот же человек позвонил системному администратору с той же проблемой и сказал, что теперь он проверил и убедился, что принтер включен в розетку. Разбор показал, что на этот раз принтер был выключен. Пользователь был очень смущен, что оба раза упустил такие очевидные факты, и купил системному администратору пива. После этого проблема больше не возникала.

Из-за того что системный администратор не критиковал пользователя и держал его в курсе проблемы, пользователь научился решать проблемы сам, люди остались в дружеских отношениях, а системный администратор получил пиво.

Гибкость важна. В предыдущем примере пользователь сказал, что необходимо срочно распечатать месячный отчет. В данном случае может быть уместно предложить воспользоваться другим принтером, который точно работает, а не исправлять неполадку прямо сейчас. Это ускоряет процесс, что важно для срочной проблемы.

В крупных компаниях запросы записываются и выполняются разными людьми. Такая дополнительная передача вносит проблему, поскольку записывающий сотрудник может не иметь непосредственного опыта, который нужен, чтобы точно знать, что нужно записать. В данном случае целесообразно иметь заранее спланированные схемы сбора данных для различных ситуаций. Например, если пользователь сообщает о проблеме с сетью, описание проблемы должно включать IP-адрес, номер комнаты, в которой не работает машина, и что конкретно у человека не получается сделать по сети. Если проблема связана с печатью, вы должны записать имя принтера, используемый компьютер и приложение, отправившее документ на печать.

Будет лучше, если ваша программа отслеживания заявок станет записывать различную информацию в зависимости от категории проблемы.

14.1.2.3. Этап 4: проверка проблемы

На этапе 4 системный администратор пытается воспроизвести проблему, то есть выполняет роль **воспроизводителя**. Если проблему невозможно воспроизвести, то она, вероятно, была неправильно описана и нужно вернуться к этапу 3. Если проблема появляется периодически, процесс ее воспроизведения становится более сложным, но не является невозможным.

Ничто не дает вам лучшего понимания проблемы, чем наблюдение ее в действии. Это важнейшая причина необходимости проверки проблемы. Но мы все равно видим, как наивные системные администраторы все время пропускают этот этап. Если вы не проверите проблему, то рискуете работать над ней часами, прежде чем поймете, что занимаетесь совсем не тем, чем нужно. Часто описание пользователя уводит в неверном направлении. Пользователь, не имеющий технических знаний для точного описания проблемы, может направить вас по ложному следу. Просто вспомните обо всех случаях, когда вы пытались помочь кому-то по телефону, у вас это не получалось и тогда вы шли на рабочее место этого человека. Стоило вам взглянуть на его экран – и вы говорили: «О! Это совершенно другая проблема!» И после нажатия нескольких клавиш неполадка исправлялась. Вы не были способны воспроизвести проблему локально, поэтому не смогли увидеть ее суть, а следовательно, определить, что на самом деле произошло.

Очень важно, чтобы метод, используемый для воспроизведения проблемы, был записан для последующего повторения на этапе 8. Включение тестирования в скрипт или пакетный файл упростит проверку. Одним из преимуществ систем, управляемых из командной строки, таких как UNIX, является простота, с которой можно автоматизировать последовательность действий. Графические интерфейсы затрудняют эту фазу, когда нет способа автоматизировать тест или включить его в исполняемый объект.

Охват процедуры проверки не должен быть слишком узким, или слишком широким, или неправильно направленным. Если тесты слишком узкие, проблема в целом может быть не решена. Если тесты слишком широкие, системные администраторы могут потратить время на отслеживание того, что проблем не вызывает.

Возможно, что направление поисков окажется неверным. В ходе попытки воспроизвести проблему пользователя может быть обнаружена другая, не связанная с ней проблема в системе. Некоторые проблемы в системе могут существовать, не влияя на пользователей, и о них не будут сообщать. Если на пути к устранению проблемы будет обнаружено и исправлено множество других, не связанных с ней неполадок, это может раздражать как системного администратора, так и пользователя. Не связанная с искомой неполадка, которая не является критической, должна быть записана, чтобы ее можно было исправить в будущем. С другой стороны, трудно определить, является ли она критической, поэтому ее исправление может быть полезным. Кроме того, она может внести неразбериху или так изменить систему, что отладка будет затруднена.

Иногда прямая проверка невозможна и даже не требуется. Если пользователь сообщает, что сломан принтер, проверяющему может не потребоваться воспроизводить проблему, пытаясь что-то напечатать. Может быть, достаточно проверить, что новые задачи печати становятся в очередь и не печатаются. В этой ситуации достаточно такой поверхностной проверки.

Однако в других случаях действительно требуется точное воспроизведение. У проверяющего может не получиться воспроизвести проблему на своем компьютере, и ему может понадобиться выполнить это на компьютере пользователя. Как только проблема будет воспроизведена в системе пользователя, может быть полезно продублировать ее где-нибудь еще, чтобы определить, является ли она локальной или глобальной. При поддержке сложного продукта у вас должна быть лаборатория с оборудованием, на котором можно воспроизводить сообщаемые проблемы.

Проверка в компаниях электронной коммерции

В компаниях электронной коммерции особенно трудно воспроизвести систему пользователя. Хотя Java и другие системы обещают, что вы можете «написать один раз и запускать везде», в реальности у вас должна быть возможность воспроизвести систему пользователя для различных моделей и версий веб-броузеров и даже межсетевых экранов. Одной компании потребовался тестовый доступ к своему сайту с межсетевым экраном и без него. Благодаря усилиям службы обеспечения качества компании у нее появился компьютер, подключенный к Интернету для такого тестирования. Так как компьютер был незащищен, он был физически изолирован от других машин, а ОС регулярно переустанавливалась.

14.1.3. Фаза C: планирование и выполнение

В этой фазе неполадка исправляется. Это включает планирование возможных решений, выбор одного из них и его выполнение (рис.14.4).

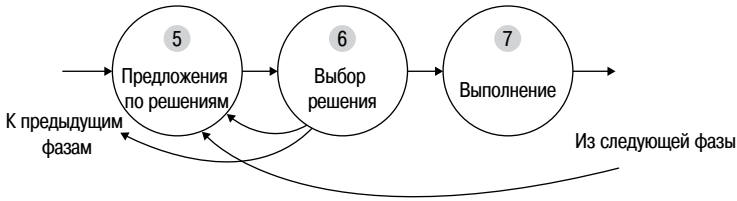

Рис. 14.4. *Последовательность исправления*

14.1.3.1. Этап 5: предложение решений

Это этап, на котором специалист в конкретной области (Subject Matter Expert – SME) предлагает возможные решения. В зависимости от проблемы их может быть много или мало. Для некоторых проблем решение может быть очевидным и предлагаться будет только оно. В других случаях возможно много решений. Часто проверка проблемы на предыдущем этапе помогает определить возможные решения.

«Лучшее» решение может быть различным в зависимости от ситуации. В одном финансовом учреждении служба поддержки решила проблему клиента с сетевой файловой системой NFS (Network File System) при помощи перезагрузки. Это было быстрее, чем пытаться непосредственно исправить неполадку, и позволило клиенту снова приступить к работе. Однако в исследовательской системе может иметь смысл попытаться найти источник проблемы, возможно, отключив и заново подключив NFS-раздел, вызывавший проблему.

Пример: радикальные решения для печати

В одном из наших предыдущих примеров с печатью из-за того, что пользователю требовалось в ближайшее время ехать в аэропорт, лучше было

предложить альтернативное решение, например рекомендовать другой принтер, который работал нормально. Если пользователь – это руководитель, который летит из Нью-Джерси в Японию с посадкой в Сан-Хосе, то может быть целесообразным передать файл в офис в Сан-Хосе, где его можно напечатать, пока пользователь в полете. Пока руководитель ждет пересадки в аэропорту Сан-Хосе, клерк может передать ему распечатку. Том видел, как реализуется такое решение. В данном случае печатающим устройством был очень дорогой плоттер. В каждом филиале компании был только один такой плоттер.

Некоторые решения дороже остальных. Любое решение, требующее личного посещения, обычно дороже того, которое может быть выполнено удаленно. Такой тип обратной связи может быть полезным для принятия решений о покупке. Недостаток возможностей по удаленной поддержке влияет на общие расходы на обслуживание продукта. Для удаленной поддержки таких продуктов существуют как коммерческие, так и некоммерческие средства.

Системный администратор, который не знает никаких вариантов решения, должен передать проблему другим, более опытным системным администраторам.

14.1.3.2. Этап 6: выбор решения

После перечисления возможных решений одно из них выбирается для первой попытки или для очередной, если мы повторяем эти этапы. Эта задача также выполняется специалистом в конкретной области.

Выбрать лучшее решение обычно либо очень просто, либо очень сложно. Однако часто решения не могут и не должны выполняться одновременно, поэтому нужно определить приоритет возможных решений.

Пользователь должен быть привлечен к этому определению приоритета. Пользователи лучше понимают свои временные ограничения. Если пользователь – продавец потребительских товаров, то отсутствие доступа к компьютеру в течение рабочего дня для него будет гораздо более неприятным, чем, например, для редактора технической документации или даже разработчика при условии, что у них не подходят предельные сроки. Если решение А решает проблему окончательно, но требует отключения, а решение В исправляет неполадку лишь временно, то нужно узнать у пользователя, что «правильно» в конкретной ситуации – А или В. Все возможности обязан объяснить специалист в области проблемы, но системный администратор может знать некоторые из них, будучи знакомым с системой. Возможно наличие предопределенных нормативов обслуживания по времени отключения в течение дня. Системные администраторы на Уолл-стрит знают, что простой в течение дня может стоить миллионы, поэтому могут быть выбраны краткосрочные «заплатки», а долгосрочное решение назначено на следующее выделенное для обслуживания время. В исследовательской среде правила относительно времени отключения более свободные и долгосрочное решение может быть выбрано сразу[1].

[1] Некоторые компании излишне централизуют свои службы поддержки, в результате чего системные администраторы не знают, в какую категорию входят их пользователи. Обычно это мешает в работе.

При работе с более опытными пользователями может быть полезным позволить им участвовать в данной фазе. Они могут предоставить полезную обратную связь. Если пользователи неопытные, изложение всех подробностей может пугать и запутывать их без необходимости. Например, перечисление всех возможных вариантов от простой ошибки конфигурации до невосстановимого сбоя жесткого диска может вызвать у пользователя панику и обычно является плохой идеей, особенно когда оказывается, что проблема – это всего лишь опечатка в CONFIG.SYS.

Даже если пользователи неопытные, их нужно привлекать к участию в определении и выборе решения. Это может помочь обучить их, чтобы в случае дальнейших сообщений о проблемах работа шла более гладко, и даже позволить им решать свои проблемы. Это также может дать пользователям чувство собственной нужности – теплое чувство причастности к команде/компании, а не просто ощущение «юзера». Этот подход может помочь сломать стереотип «они против нас», распространенный в сфере индустрии в настоящее время.

14.1.3.3. Этап 7: выполнение решения

На этапе 7 решение выполняется. Точность и скорость, с которыми выполняется этот этап, зависят от навыков и опыта человека, реализующего решение.

Термин **исполнитель** относится к системному администратору, оператору или рабочему, выполняющему необходимые технические задачи. Этот термин пришел из других отраслей, таких как телекоммуникации, в которых приемщик может получить заказ и запланировать предоставление услуги, а исполнители протягивают кабели, подключают линии и т. д. для предоставления услуги. В компьютерной сети за планирование продуктов и процедур, используемых для предоставления услуг пользователям, может отвечать проектировщик сети, но, когда в маршрутизаторе нужно добавить дополнительный Ethernet-интерфейс, карту устанавливает и настраивает монтажник.

Иногда исполнителем становится пользователь. Эта ситуация является особенно распространенной, когда пользователь является удаленным и его система обладает малыми возможностями по удаленному управлению или вообще их не имеет. В этом случае успех или неудача данного этапа зависит и от пользователя. Требуется диалог между системным администратором и пользователем, чтобы решение заработало. Пользователь выполнил решение правильно? Если нет, то не причинил ли он больше вреда, чем пользы?

Ведите диалог, учитывая навыки пользователя. Если вы будете произносить по буквам каждую команду, пробел и специальный символ, то это может обидеть продвинутого пользователя. А неопытного пользователя может пугать, если системный администратор быстро говорит сложную последовательность команд. В таких ситуациях лучше спросить «Какое сообщение появилось, когда вы это ввели?», чем «Это сработало?». Однако будьте внимательны и не переоценивайте пользователей – некоторые из них сильно преувеличивают свою опытность по сравнению с реальной.

Такое общение – это не врожденный навык, и ему можно научиться. Можно пройти обучение. Курсы в этой области обычно имеют названия, содержащие такие фразы, как «активное слушание», «межличностная коммуникация», «межличностная эффективность» или просто «продвинутая коммуникация».

В этот момент, казалось бы, работа может считаться законченной. Однако это не так, пока результат не проверили и пользователь не удовлетворен. Это приводит нас к последней фазе.

14.1.4. Фаза D: проверка

На данном этапе проблема уже *должна* быть устранена, но нам нужно это проверить. Эта фаза не будет закончена, пока пользователь не согласится с тем, что неполадка была исправлена (рис. 14.5).

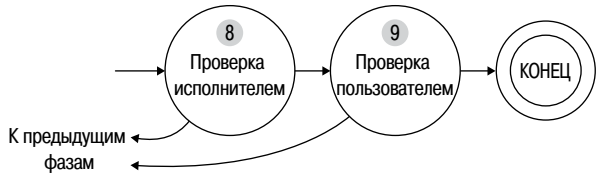

Рис. 14.5. *Последовательность проверки*

14.1.4.1. Этап 8: проверка исполнителем

На этапе 8 исполнитель, который работал на этапе 7, проверяет, были ли успешными меры, принятые для устранения проблемы. Если процесс, который использовался для воспроизведения проблемы на этапе 4, не был подробно записан или не будет точно повторен, проверка не пройдет правильно. Если проблема все еще присутствует, вернитесь к этапу 5 или, возможно, к более раннему этапу.

UNIX-программа diff

В этой ситуации может быть полезна UNIX-команда `diff` – она отображает различия между двумя текстовыми файлами. Сохраните выходные данные при воспроизведении проблемы. После принятия мер по исправлению неполадки запустите программу еще раз и сохраните выходные данные в новом файле. Запустите `diff` для этих файлов, чтобы посмотреть, есть ли какие-либо отличия. Кроме того, вы можете скопировать выходные данные, показывающие проблему, в новый файл и отредактировать их, чтобы они выглядели как результат на работающей системе (у вас может быть работающая система для создания образца «хорошего» результата). Затем программой `diff` можно воспользоваться для сравнения текущих результатов и исправленных выходных данных. Вы узнаете, что внесли правильные изменения, когда `diff` сообщит, что файлы одинаковы. Некоторые системы не предоставляют выходных данных, пригодных для использования `diff`, но для их приспособления под `diff` можно воспользоваться Perl и другими средствами.

Пример: проблема с разными установками TEX

Однажды пользователь смог дать Тому пример файла TEX, который успешно обрабатывался приложением TEX, установленным в его предыдущем подразделении, но не обрабатывался нынешним. У Тома была учетная запись на компьютерах предыдущего отдела пользователя, поэтому он имел образец для сравнения. Это было очень полезно. В конце концов он смог исправить установку TEX за счет успешного уточнения проблемы и сравнения обеих систем.

14.1.4.2. Этап 9: проверка пользователем/закрытие

На последнем этапе пользователь должен убедиться, что проблема решена. Если пользователь не удовлетворен, работа не считается сделанной. На этом этапе главную роль играет пользователь.

Предположительно, если исполнитель убедился, что решение сработало (этап 8), этот этап не нужен. Однако часто на этом этапе пользователи сообщают, что проблема еще существует. Это настолько важный вопрос, что мы выделили его в отдельный этап.

Проверка пользователем обнаруживает ошибки, сделанные в предыдущих фазах. Возможно, пользователь плохо объяснил проблему, системный администратор не понял пользователя или неправильно записал проблему, – это сложности, связанные с общением. Возможно, ошибки появились в фазе планирования. Проблема, проверенная на этапе 4, могла быть другой проблемой, которая также существует, или метод проверки проблемы мог быть неполным. Решение могло не устранить проблему в целом или превратить ее в непостоянную.

В любом случае, если пользователь не считает, что неполадка была исправлена, есть несколько способов действий. Очевидно, нужно повторить этап 4, чтобы найти более точный метод воспроизведения проблемы. Однако можно вернуться и к другим этапам. Например, проблему можно заново классифицировать (этап 2), или описать (этап 3), или передать более опытным системным администраторам (этап 5). Если ничего не получится, вам может потребоваться передать проблему руководству.

Важно заметить, что «проверка» предполагает выяснение не того, рад ли пользователь, а того, выполнен ли его запрос. Удовлетворенность пользователя – это параметр, который оценивается в другой области.

После завершения проверки пользователем вопрос считается закрытым.

14.1.5. Риск пропуска этапов

Каждый этап важен. Если какой-либо этап этого процесса будет проделан плохо, процесс может завершиться неудачей. Многие системные администраторы пропускают этапы из-за недостатка опыта или из-за ненамеренной ошибки. Многие стереотипы о плохих системных администраторах формируются из-за того, что системные администраторы пропускают определенный этап. Мы дали каждому из этих стереотипов условное название и составили список возможных способов улучшить работу системных администраторов.

- *Людоед*: Сердитые, саркастичные системные администраторы стараются отпугнуть пользователей на первом же этапе и даже не приветствуют их. *Предложение*: Руководство должно установить планку дружелюбия. Обязанности должны быть зафиксированы в письменной политике, доведенной как до системных администраторов, так и до пользователей.
- *Гонитель*: Если вам когда-нибудь приходилось звонить по телефону в отдел технической поддержки крупной компании и человек, ответивший на звонок, отказался передать ваш запрос в нужный отдел, то вы понимаете, что мы имеем в виду. *Предложение*: Создайте формальное дерево решений, чтобы было известно, какие проблемы куда передавать.
- *Самонадеянный*: Обычно этап 3 не пропускается, но такие системные администраторы склонны быстро решать, что они поняли проблему, хотя на са-

мом деле это не так. *Предложение*: Обучите человека активному слушанию; если это не принесет успеха, отправьте его на соответствующие учебные курсы.

- *Безответственный*: Системный администратор, который пропускает проверку проблемы (этап 4), обычно занят устранением не той проблемы. Однажды Том был в панике, узнав, что «сеть не работает». На самом деле один неопытный пользователь не смог прочитать свою электронную почту и сообщил, что «сеть не работает». Сообщение не было проверено недавно нанятым системным администратором, который еще не понял, что некоторые неопытные пользователи сообщают так обо всех проблемах. Оказалось, что почтовый клиент пользователя был неправильно настроен. *Предложение*: Научите системных администраторов воспроизводить проблемы, особенно прежде чем передавать их на более высокий уровень. Напомните, что нехорошо вызывать панику у Тома.
- *Мастер-ломастер*: Неопытные системные администраторы обычно недостаточно творчески или излишне творчески подходят к предложению и выбору решений (этапы 5 и 6). Но пропуск этих этапов целиком приводит к другой проблеме. После обучения использованию Ethernet-анализатора (сетевого сниффера), неопытный, но полный энтузиазма системный администратор применял это средство для решения всех проблем, о которых сообщалось. Он исправлял неполадки неправильно. *Предложение*: Обеспечьте обучение или наставничество. Расширьте множество решений, с которыми знаком системный администратор.
- *Халтурщик*: Иногда некомпетентные системные администраторы при неправильном выполнении решений приносят больше вреда, чем пользы. Довольно глупо пытаться исправить неполадку не на той машине, тем не менее такое бывает. *Предложение*: Научите системного администратора смотреть, что было напечатано, прежде чем нажимать на клавишу Enter или щелкать по кнопке OK. Включение имени узла в консольную команду может быть очень важно.
- *Залетная птица*: Такой системный администратор приходит в офис пользователя, нажимает на несколько клавиш, прощается и говорит: «Это должно исправить неполадку». Пользователи раздраженно узнают, что проблема не была решена. По правде говоря, введенные команды действительно должны были исправить неполадку, но этого не произошло. *Предложение*: Руководство должно установить планку по проверке.
- *Торопыга*: Некоторые системные администраторы одержимы «закрытием заявки». Часто системных администраторов оценивают по тому, насколько быстро они закрывают заявки. В этом случае системные администраторы вынуждены пропускать последний этап. Такие действия аналогичны работе сильно загруженных продавцов, сосредоточенных на «закрытии дела». *Предложение*: Руководство должно оценивать работу не на основании скорости решения проблем, а на основании комбинации параметров, обеспечивающих предпочтительное поведение. Параметры не должны включать время ожидания пользователя при подсчете времени выполнения запроса. Системы отслеживания должны поддерживать установку запроса в состояние «ожидание пользователя», пока от пользователя ожидаются действия, и это время должно вычитаться из параметра времени выполнения.

14.1.6. Работа в одиночку

Если вы единственный системный администратор в компании, то также можете выиграть от использования этой модели для того, чтобы обеспечить пользователям четко определенный способ сообщения о проблемах, запись и проверку этих проблем, предложение решений, их выбор и выполнение, а также необходимые проверки того, была ли решена проблема. Когда системный администратор в организации один, проблемы с конкретными приложениями могут передаваться в службы поддержки их разработчиков.

14.2. Тонкости

После того как вы освоили базовый процесс, можно улучшить его при помощи ряда методов. На уровне деталей вы можете подумать об улучшении каждого этапа, на общем уровне – проверить согласованность всех этапов.

14.2.1. Обучение, основанное на модели

Внутреннее обучение должно быть основано на этой модели, чтобы системные администраторы последовательно пользовались ею. После первоначального обучения более опытный персонал должен наставлять менее подготовленных системных администраторов, чтобы помочь им усвоить то, чему они учились. На определенных этапах могут помочь конкретные типы обучения.

Можно вносить улучшения, уделяя внимание каждому этапу. По каждому этапу можно написать целые книги. Это уже произошло в других профессиях с похожими моделями, например по уходу за больными, продажам и т. д.

Недостаток обучения вредит процессу. Например, неправильное распределение обязанностей затрудняет направление вопроса нужному человеку после классификации. Неопытные сотрудники при записи данных на этапе 3 не соберут нужной информации, что затруднит дальнейшие этапы и может потребовать дополнительного обращения к пользователю. Письменная схема, отражающая, кто за что отвечает, а также стандартный список данных, которые необходимо собрать для каждой классификации, облегчат эти проблемы.

14.2.2. Целостное усовершенствование

Помимо внимания к улучшению каждого этапа, вы также можете сосредоточиться на улучшении процесса в целом. Переход к каждому следующему этапу должен быть плавным. Если пользователь видит внезапный, резкий переход между этапами, процесс может выглядеть непрофессиональным или бессвязным.

Каждая передача создает возможности для ошибок и неправильного понимания. Чем меньше передач, тем меньше возможностей для ошибок.

Если компания достаточно маленькая и в ней всего один системный администратор, то такую ошибку совершить невозможно. Однако с ростом и усложнением систем и сетей одному человеку становится невозможно знать и поддерживать всю сеть. По мере развития систем передачи становятся неизбежным бедствием. Это объясняет распространенное представление о том, что более крупные груп-

пы системных администраторов не так эффективны, как небольшие. Следовательно, с ростом группы системных администраторов вы должны уделять внимание обеспечению высококачественной передачи. Кроме того, вы можете выбрать принцип одной точки контакта, или представителя пользователя для решения проблемы. Это приводит к тому, что пользователь в процессе решения проблемы видит одно лицо.

14.2.3. Более близкое знакомство с пользователями

Если каждый раз, обращаясь за помощью, пользователь разговаривает с одним и тем же человеком, системный администратор, скорее всего, лучше узнает потребности конкретного пользователя и сможет предоставить более качественное обслуживание. Всегда существуют способы повысить вероятность такого развития событий. Например, подгруппы отдела системных администраторов могут быть прикреплены к конкретным группам пользователей, а не к технологии, которую они поддерживают. Кроме того, если отвечающий на звонки персонал очень многочисленный, группа может воспользоваться центром обработки вызовов телефонной системы, где пользователи звонят по одному номеру и центр обработки вызовов передает их вызов свободному оператору. Современные системы центров обработки вызовов могут направлять вызовы на основе информации от определителя номера, используя эту функцию, например, для передачи вызова тому же оператору, с которым пользователь говорил в прошлый раз, если тот свободен. Это означает, что будет существовать тенденция к тому, чтобы пользователи каждый раз говорили с одним и тем же человеком. Достаточно приятно говорить с кем-то, кто узнает ваш голос.

14.2.4. Специальные объявления о серьезных отключениях

Во время серьезных отключений сети многие пользователи могут пытаться сообщать о проблемах. Если пользователи сообщают о проблемах через автоответчик («Нажмите 1 для..., нажмите 2 для...»), такая система обычно может быть запрограммирована для объявления об отключении сети перед перечислением вариантов. «Пожалуйста, имейте в виду, что сетевое соединение с Денвером в данный момент неисправно. Наш провайдер ожидает, что оно будет исправлено к 15 часам. Нажмите 1 для... нажмите 2 для...».

14.2.5. Анализ тенденций

Каждый месяц уделяйте немного времени поиску тенденций и принимайте меры на их основе. Это необязательно должен быть сложный анализ, как показывает следующий пример.

Пример: кто делает больше всего запросов?

В одной компании мы просто смотрели, какие пользователи в прошлом году открыли больше всего заявок. Мы обнаружили, что 3 из 600 сотрудников открыли 10% всех заявок. Это много! Можно было легко сходить к руководителю каждого сотрудника, чтобы обсудить, как мы могли бы

предоставить лучшее обслуживание. Если человек делал так много запросов, мы, очевидно, не удовлетворяли его потребностей.

Один сотрудник открывал так много заявок, потому что докучал системным администраторам требованиями устранить ошибки в старой версии программы набора текста LATEX, которой он пользовался, отказываясь перейти на последнюю версию, где было устранено большинство имевшихся проблем. Его руководитель согласился, что лучшим решением было потребовать от своего сотрудника перейти на последнюю версию LATEX, и взял на себя ответственность проконтролировать это.

Следующий руководитель посчитал, что его сотрудник задавал элементарные вопросы, и решил отправить его на обучение, чтобы тот стал более самостоятельным.

Последний руководитель пришел к выводу, что его сотрудник делал так много запросов оправданно. Однако руководитель согласился, что его сотрудник слишком часто перекладывал на нас выполнение своей работы. В течение нескольких ближайших месяцев сотрудник стал более самостоятельным.

Вот еще несколько тенденций, которые нужно выявлять:

- *Обращается ли пользователь с одной и той же проблемой постоянно?* Почему она повторяется? Требуется ли пользователю обучение или эта система действительно настолько неисправна?
- *Задается ли много вопросов той или иной категории?* Трудно ли пользоваться этой системой? Можно ли ее переделать или заменить либо улучшить документацию?
- Много ли клиентов сообщают об одной и той же проблеме? Можно ли извещать их всех сразу? Должны ли такие проблемы иметь более высокий приоритет?
- *Можно ли перевести некоторые категории запросов на самообслуживание?* Часто клиент обращается к системному администратору, потому что выполнение запроса требует привилегированного доступа, например доступа привилегированного пользователя или администратора. Найдите способы, чтобы позволить пользователям помогать себе самостоятельно. Многие из этих запросов можно перевести на самообслуживание при помощи веб-программирования. В UNIX-системах есть программы установления идентификатора пользователя (Set User ID – SUID), которые при правильном администрировании позволяют пользователям запускать программы, выполняющие привилегированные задачи, а затем отменяют привилегированный доступ, как только выполнение программы завершится. Отдельные программы SUID могут предоставлять пользователям возможность выполнять определенную задачу; можно создать пакетные программы SUID, предоставляющие расширенный уровень привилегий, запускающие программу третьей стороны, а затем снижающие привилегии до нормального уровня. Написание программ SUID очень сложно, и ошибки могут привести к уязвимостям в безопасности. Такие системы, как sudo (Snyder et al. 1986), позволяют вам управлять привилегиями SUID по отдельным пользователям и по командам и были проанализированы достаточным количеством

экспертов по безопасности, чтобы считаться относительно безопасным способом предоставления SUID-доступа обычным пользователям.

- *Какие пользователи чаще всего к вам обращаются?* Подсчитайте, из какого отдела поступает больше всего запросов или у кого самое высокое среднее количество запросов на сотрудника. Подсчитайте, какие пользователи делают 20% запросов. Соответствуют ли эти соотношения вашей модели финансирования или определенные группы пользователей «обходятся» дороже других?
- *Является ли конкретный запрос, требующий больших затрат времени, одним из наиболее распространенных?* Если пользователи часто случайно удаляют файлы и вы каждую неделю тратите много времени на то, чтобы восстанавливать файлы с магнитной ленты, вам лучше потратить время на то, чтобы помочь пользователям узнать о `rm -i` или других программах безопасного удаления. Кроме того, может быть целесообразно обратиться с просьбой закупить систему, поддерживающую сохранение состояния и позволяющую пользователям делать восстановление собственноручно. Если вы предоставите отчет по количеству и частоте запросов на восстановление, руководство сможет принять более обоснованное решение или поговорить с некоторыми пользователями, чтобы они были более внимательны.

В этой главе не рассматриваются метрики, но системы параметров, заложенные в этой модели, могут быть лучшим способом обнаружения областей, которые нужно улучшить. Процесс из девяти этапов можно легко приспособить для подсчета параметров. Разработка параметров, определяющих нужное поведение, является сложной. Например, если системные администраторы оцениваются по тому, как быстро они закрывают заявки, это может случайно вызвать тенденцию «стремления к закрытию», рассмотренную ранее. Если системные администраторы предотвращают неполадки заранее, то сообщаемые проблемы станут более серьезными и будут требовать больше времени. Если среднее время выполнения растет, означает ли это, что мелкие проблемы были устранены, или это значит, что системные администраторы стали медленнее решать все проблемы[1]?

14.2.6. Пользователи, знающие процесс

Более образованный пользователь – лучший пользователь. Пользователи, которые понимают девять выполняемых этапов, могут быть более подготовленными при сообщении о проблеме. Эти пользователи при обращении могут предоставить более полную информацию, потому что они понимают важность полноты информации в решении проблемы. При сборе этой информации они более узко определят сообщение о проблеме. У них могут быть особые предложения по воспроизведению проблемы. Они могут сузить проблему до конкретной машины или ситуации. Дополнительная подготовка может даже привести к тому, что они сами решат проблему! Обучение пользователей должно включать объяснение процесса из девяти этапов для упрощения взаимодействия между пользователями и системными администраторами.

---

[1] Страта выступает за использование заявок от системных администраторов для заблаговременных исправлений и запланированных проектов, чтобы вклад системных администраторов был виднее.

Подготовка пользователей в отделе регистрации транспортных средств

Том заметил, что отдел регистрации транспортных средств Нью-Джерси недавно изменил свое сообщение при удержании вызова, чтобы оно включало список из четырех документов, которые должны быть на руках, если человек звонил для продления регистрации транспортного средства. Теперь, вместо того чтобы говорить с человеком только с целью узнать, что у вас нет, например, номера страхового полиса, повысилась вероятность того, что, когда вы будете соединены, у вас окажется все необходимое для выполнения операции.

14.2.7. Архитектурные решения, соответствующие процессу

Архитектурные решения могут препятствовать или способствовать процессу классификации. Чем сложнее система, тем труднее может быть идентифицировать и воспроизвести проблему. К сожалению, некоторые широко распространенные принципы проектирования, например разделение системы на уровни, не согласуются с процессом из девяти этапов. Например, неполадка с печатью в большой UNIX-сети может быть проблемой с DNS, программным обеспечением сервера, программным обеспечением клиента, неправильной настройкой системы пользователя, сетью, DHCP, конфигурацией принтера и даже самим принтером. Обычно многие из этих уровней обслуживаются различными группами людей. Точная диагностика проблемы требует, чтобы системные администраторы были экспертами во всех этих технологиях либо чтобы уровни осуществляли перекрестный контроль.

При проектировании системы вы должны иметь в виду, как продукт будет поддерживаться. В электронной промышленности есть принцип «проектирования для производства», мы должны думать в категориях «проектирования для обслуживания».

14.3. Заключение

Эта глава об общении. Процесс помогает нам лучше осознавать, как мы общаемся с клиентами, и предоставляет нам базовую терминологию для использования при обсуждении нашей работы. У всех профессионалов есть базовая терминология, применяемая для эффективного общения друг с другом.

В данной главе представлена формальная, структурированная модель обработки запросов от пользователей. Этот процесс делится на четыре фазы: приветствие, идентификацию, планирование и выполнение, исправление и проверку. В каждой фазе есть отдельные этапы, представленные в табл. 14.1.

Соблюдение этой модели делает процесс более структурированным и формализованным. Когда он будет организован, появятся области для развития в вашей организации.

Таблица 14.1. Обзор фаз решения проблемы

Фаза	Этап	Роль
Фаза A: «Здравствуйте!»	1. Приветствие	Встречающий
Фаза B: «Что случилось?»	2. Классификация проблемы	Классификатор
	3. Описание проблемы	Регистратор
	4. Проверка проблемы	Воспроизводитель
Фаза C: «Исправить это»	5. Предложение решений	Специалист в конкретной области
	6. Выбор решения	
	7. Выполнение решения	Исполнитель
Фаза D: «Проверить это»	8. Проверка исполнителем	
	9. Проверка пользователем	Пользователь

Вы можете интегрировать эту модель в планы обучения системных администраторов, а также объяснить ее пользователям, чтобы они могли лучше излагать свои требования. Данная модель может применяться для оценки параметров. Она предоставляет возможность анализа тенденций, хотя и простейшего, но это лучше, чем ничего.

Невозможно переоценить преимущества применения программ отслеживания запросов в службу поддержки по сравнению с попытками запоминать запросы, записывать их на бумаге или полагаться на ящики электронной почты. Автоматизация снижает трудоемкость работы с входящими запросами и сбора статистических данных. Программы, отслеживающие заявки, реально экономят ваше время. Однажды Том подсчитал, что группа системных администраторов тратила на отслеживание запросов час в день на человека. Это потеря двух человеко-дней в неделю!

Процесс, рассмотренный в данной главе, разъясняет вопросы поддержки пользователей, определяя, какие этапы нужно выполнить для успешной обработки одного запроса. Мы показали, почему надо выполнять эти этапы и как каждый этап готовит вас к следующим.

Несмотря на то что знание модели может повысить эффективность работы системного администратора за счет разделения труда, это не панацея, она не заменит творческий подход, опыт и наличие нужных ресурсов. Модель не заменяет обучения, средств и поддержки руководства, но она должна быть элементом хорошо организованной службы поддержки.

Многие системные администраторы от природы хорошо работают с пользователями и негативно реагируют на подобные структурированные методы. Мы рады за тех, кто нашел свою собственную структуру и пользуется ею, получая стабильные хорошие результаты. Мы уверены, что она имеет много элементов, рассмотренных здесь. Делайте то, что работает у вас. Чтобы обучить необходимое количество системных администраторов на месте, потребуются более прямые инструкции. Для миллионов системных администраторов, которые не нашли оптимальной структуры для себя, принятие этой модели будет хорошим началом.

Задания

1. Бывают ли случаи, когда вам не нужно пользоваться моделью из девяти этапов?
2. Какие средства используются у вас для обработки запросов пользователей и как они согласуются с моделью из девяти этапов? Существуют ли способы, которые могут подойти лучше?
3. Как вы приветствуете пользователей в своей среде? Какими способами вы могли бы пользоваться, но не пользуетесь? Почему?
4. В своей среде вы приветствуете пользователей различными способами. Как можно сравнить эти способы по стоимости, скорости (быстрому выполнению) и предпочтению пользователей? Является ли наиболее дорогой метод самым предпочтительным для пользователей?
5. Некоторые описания проблем могут быть краткими, как в примере с проблемой маршрутизации на этапе 3. Обратитесь к вашей системе отслеживания сообщений о неисправностях и найдите пять наиболее часто сообщаемых проблем. Каково самое короткое описание, полностью описывающее проблему?
6. Обратитесь к вашей системе отслеживания заявок и определите десять пользователей, создавших больше всего заявок за последние 12 месяцев, а затем отсортируйте их по группам пользователей или отделам. Далее определите, в каких группах пользователей число заявок на человека максимально. Какие пользователи создают 20% заявок? Что вы будете делать теперь, когда у вас есть эти сведения? Изучите другие тенденции из раздела 14.2.5.
7. Какие из девяти этапов самые важные? Обоснуйте свой ответ.

Часть III

Процессы изменений

Глава 15

Отладка

В данной главе мы проведем глубокий обзор всего, что касается процесса отладки. В главе 14 мы рассматривали отладку в более широком контексте работы с пользователями. Данная глава, напротив, касается вас и того, что вы делаете, столкнувшись с конкретной технической проблемой.

Отладка – это не просто внесение изменения, которое исправляет неполадку. Отладка начинается с понимания проблемы, выяснения ее причины, а затем вносится изменение, устраняющее проблему. Временные или поверхностные исправления, например перезагрузка, которые не устраняют причину проблемы, гарантируют только больший объем работы для *вас* в будущем. Мы продолжим эту тему в главе 16.

Так как у любого, кто читает эту книгу, есть определенный уровень интеллекта и опыта[1], нам не потребуется подробно разбирать эту тему. Вам приходилось заниматься отладкой, вы знаете, что это такое. Мы постараемся раскрыть вам тонкости процесса и рассмотрим несколько способов, как сделать его еще более плавным. Мы призываем вас к системному подходу. Это лучше, чем поступать по наитию.

15.1. Основы

В данном разделе представлены советы по правильному определению проблемы, введены две модели поиска проблемы, а в заключении приведены некоторые размышления о качествах лучших средств.

15.1.1. Ознакомьтесь с проблемой пользователя

Первый шаг в исправлении неполадки – понять, подробно разобраться в том, что пытается сделать пользователь и какой элемент не работает. Другими словами, пользователь что-то делает и ожидает конкретного результата, но вместо этого происходит что-то другое.

Например, пользователи могут пытаться прочитать свою электронную почту, но у них это может не получиться. Они могут сообщать об этом по-разному: «Моя почтовая программа не работает», или «Я не могу соединиться с почтовым сервером», или «Мой почтовый ящик исчез!». Любое из этих утверждений может быть правдой, но проблема также может связана с неполадкой в сети, сбоем

[1] А ведь мы с вами просто великолепны!

электропитания в серверной или ошибкой DNS. Эти вопросы могут находиться за пределами понимания пользователя или требовать разбора. Следовательно, для вас важно подробно разобраться, что пытается сделать пользователь.

Иногда пользователи не могут правильно выразить свои мысли, поэтому забота и понимание должны быть превыше всего. «Не могли бы вы помочь мне разобраться, как должен выглядеть документ?»

Часто пользователи применяют жаргон, но делают это неправильно. Они полагают, что именно это хочет слышать системный администратор. Они стараются помочь. Будет вполне оправданно, если системный администратор ответит на это: «Постойте, пожалуйста. Что конкретно вы пытаетесь сделать? Просто расскажите об этом без технических понятий».

Обычно жалоба не является проблемой. Пользователь может пожаловаться, что принтер сломан. Это звучит как просьба отремонтировать принтер. Однако системный администратор, который уделит достаточно времени, чтобы разобраться в ситуации в целом, может узнать, что пользователю нужно напечатать документ раньше, чем будут доставлены запчасти. В этом случае становится ясно, что жалоба клиента касается не оборудования, а необходимости напечатать документ. Распечатка на другом принтере становится лучшим решением.

Некоторые пользователи оказывают вам ценную услугу, разобравшись в проблеме, прежде чем о ней сообщить. Для старшего системного администратора такие пользователи являются помощниками, но помните, что всему есть предел. Может быть, приятно получить такое сообщение: «Я не могу печатать, я думаю, это проблема DNS». Однако мы не считаем, что таким сообщениям нужно безусловно верить. Вы понимаете архитектуру системы лучше пользователей, поэтому вам все-таки нужно проверить как часть сообщения о DNS, так и проблему с печатью. Возможно, лучше всего интерпретировать этот текст как два различных сообщения, которые могут быть и связанными: у определенного пользователя не работает печать и определенная проверка DNS не удалась. Например, имя принтера может не входить в DNS в зависимости от архитектуры системы печати. Часто пользователи будут пинговать узел, чтобы показать проблему маршрутизации, но не обратят внимания на сообщение об ошибке и тот факт, что не удалось найти имя узла в DNS.

Найдите реальную проблему

Один из пользователей Тома сообщил, что конкретный сервер, расположенный в другом подразделении на удалении приблизительно в тысячу миль, не пингуется. Он дал маршруты, информацию о прохождении эхозапроса и множество подробных доказательств. Вместо того чтобы разбираться с возможными проблемами DNS, маршрутизации и функционирования сети, Том спросил: «Зачем вам нужно пинговать этот узел?» Оказалось, что пингование узла не входило в обязанности сотрудника, он пытался использовать этот узел как сервер аутентификации. Проблема, с которой нужно было разобраться, должна была звучать так: «Почему я не могу воспользоваться службой A, которая зависит от сервера аутентификации на узле B?»

Связавшись с владельцем сервера, Том нашел очень простой ответ: узел B был выведен из эксплуатации и правильно настроенные клиенты должны

были автоматически начать аутентификацию на новом сервере. Это не было вопросом работы сети, а касалось конфигурации клиента. Пользователь прописал в своей конфигурации статический IP-адрес, хотя не должен был так поступать. Если бы Том начал решать проблему, изложенную в первоначальном виде, было бы зря потрачено много времени.

Коротко говоря, сообщение о проблеме должно содержать информацию об отсутствии ожидаемого результата. Теперь давайте разберемся с причиной.

15.1.2. Устраняйте причину, а не симптом

Чтобы обеспечить долговременную надежность, вы должны находить и устранять причину проблемы, а не просто искать ее обход или способ быстрого восстановления после нее. Несмотря на то что обход и быстрое восстановление полезны, устранение причины проблемы в корне лучше.

Часто мы оказываемся в следующей ситуации: сослуживец сообщает о том, что возникла проблема и что он ее исправил. Мы спрашиваем: «Какая была проблема?»

«Нужно было перезагрузить узел».

«Какая была проблема?»

«Я же тебе сказал! Нужно было перезагрузить узел».

На следующий день узел снова нужно перезагружать.

Узел, требующий перезагрузки, – это не проблема, а, скорее, ее решение. Проблема могла быть в том, что система зависла, драйверы устройств, содержащие ошибки, работали неправильно, процесс ядра не освобождал память и единственным выходом была перезагрузка и т. д. Если бы системный администратор определил, какова была истинная проблема, можно было бы решить ее раз и навсегда.

То же самое касается фразы «Мне пришлось закрыть и перезапустить приложение или службу» и других таинственных слов. Часто мы видели, как кто-то решает проблему нехватки места на диске, удаляя старые файлы логов. Однако проблема возвращается, когда файлы логов снова вырастают. Удаление файлов логов устраняет симптомы, а запуск скрипта, который будет обновлять и автоматически удалять логи, устранил бы проблему.

Даже крупные компании склонны устранять симптомы вместо первопричин проблем. Например, Майкрософт получила множество негативных отзывов в прессе, когда сообщила, что основной чертой Windows 2000 будет более быстрая перезагрузка. На самом деле пользователи скорее предпочли бы, чтобы ее не приходилось так часто перезагружать.

15.1.3. Подходите системно

Важно подходить к поиску и исправлению причины методически, или системно. Для системного подхода вы должны формировать гипотезы, проверять их, записывать результаты и вносить изменения на основании этих результатов. Все остальное – это просто внесение случайных изменений, пока проблема не исчезнет.

При отладке обычно используются процесс исключения и последовательное уточнение. **Процесс исключения** предполагает выведение различных элементов системы до исчезновения проблемы. Проблема будет содержаться в части, выведенной последней. **Последовательное уточнение** предполагает внесение в систему компонентов с проверкой на желаемое изменение на каждом этапе.

Процесс исключения часто используется при отладке оборудования, например заменяются платы памяти, пока не исчезнет ошибка памяти, или вынимаются карты, пока машина не сможет загрузиться. Исключение используется и с программными приложениями – в качестве примера можно привести удаление потенциально конфликтующих драйверов или приложений, пока ошибка не исчезнет. В некоторых ОС для сужения области поиска есть средства поиска возможных конфликтов и тестовые режимы.

Последовательное уточнение – аддитивный процесс. Для выявления проблемы IP-маршрутизации команда `traceroute` сообщает о наличии связи через один сетевой переход, затем – через два, три, четыре и т. д. Когда результат перестает возвращаться, мы знаем, что маршрутизатор на этом переходе не может возвращать пакеты. Проблема в этом последнем маршрутизаторе. Когда связь есть, но теряются пакеты, можно воспользоваться похожей методикой. Вы можете отправить на следующий маршрутизатор несколько пакетов и проверить, не теряются ли они. Можно последовательно уточнять тест, включая более удаленные маршрутизаторы, пока не будет обнаружена потеря пакетов. Тогда вы можете утверждать, что потеря произошла на последнем добавленном сегменте.

Иногда последовательное уточнение можно рассматривать как отладку **следования маршруту**. Для этого вы должны следовать маршруту данных или проблемы, изучая выходные данные каждого процесса, чтобы убедиться, что они являются подходящими исходными данными для следующего этапа. В UNIX-системах распространен конвейерный подход к обработке. Одна задача создает данные, другие последовательно изменяют или обрабатывают эти данные, а последняя задача записывает их. Некоторые процессы могут проходить на различных машинах, но на каждом этапе данные можно проверить. Например, если каждый этап генерирует файл лога, то вы можете изучать логи каждого этапа. При отладке проблемы с электронной почтой, когда предполагается прохождение сообщения с одного сервера на шлюз и затем на сервер получателя, вы можете просмотреть логи на всех трех машинах, чтобы убедиться, что на каждой из них сообщение было обработано правильно. При отслеживании сетевой проблемы вы можете воспользоваться средствами, позволяющими вам просматривать пакеты, проходящие через линию связи, чтобы наблюдать за каждым этапом. Маршрутизаторы Cisco поддерживают сбор проходящих по линии пакетов, соответствующих определенному набору признаков, в UNIX-системах есть команда `tcpdump`, в Windows-системах – Ethereal. Если вы имеете дело с UNIX-программой, использующей оболочку – средство для отправки данных через ряд программ, – команда `tee` может сохранять копию каждого этапа.

В этих методах можно применять сокращение и оптимизацию. Основываясь на предыдущем опыте, вы можете пропустить этап или два. Однако часто это является ошибкой, потому что вы «прыгаете» к завершению.

Мы хотели бы отметить, что, если вы *собираетесь* «прыгнуть» к завершению, проблема часто бывает связана с последним изменением в узле, сети или другом проблемном объекте. Обычно это свидетельствует о недостатке тестирования. Поэтому, прежде чем начать устранять проблему, подумайте, какие изменения

были внесены недавно: было ли подключено к сети новое устройство, какое было последнее изменение в конфигурации узла, изменилось ли что-нибудь на маршрутизаторе или в брандмауэре. Часто ответы на эти вопросы дают верное направление поиска причины.

15.1.4. Пользуйтесь правильными средствами

Отладка требует наличия соответствующих средств диагностики. Некоторые из них являются физическими устройствами, другие – программами, которые покупают, загружают, а также разрабатывают самостоятельно. Однако самым важным средством являются знания.

Средства диагностики позволяют вам увидеть внутренние процессы работы устройства или системы. Однако, если вы не знаете, как понимать то, что вы видите, вся информация в мире не поможет вам решить проблему.

Обучение обычно включает изучение того, как работает система, как увидеть ее внутренние процессы и как интерпретировать то, что вы видите. Например, при обучении использованию Ethernet-анализатора (сниффера), легко научить человека перехватывать пакеты. Бóльшая часть времени обучения тратится на объяснение того, как работают различные протоколы, чтобы вы понимали, что видите. Научиться обращаться со средством легко. Глубокое понимание того, что средство позволяет вам видеть, приобретается значительно дольше.

UNIX-системы имеют репутацию простых в отладке, скорее всего, потому, что много опытных системных администраторов, работающих с UNIX, имеют глубокое знание внутренних процессов системы. Такое знание легко приобрести. UNIX-системы снабжаются документацией об их внутренних процессах, первые пользователи даже имели доступ к исходному коду. Во многих книгах (Lions 1996; McKusic, Bostic and Karels 1996; Mauro and McDougall 2000) исходный код ядер UNIX анализируется в образовательных целях. Большая часть этих систем управляется скриптами, которые можно легко прочитать, чтобы понять, что происходит за кулисами.

Microsoft Windows сразу приобрела репутацию системы, работу которой трудно отлаживать. Сторонники UNIX утверждали, что это черный ящик, в котором нет возможности получить необходимую информацию для устранения проблем в Windows-системах. На самом деле такие механизмы существовали, но единственным способом узнать о них было обучение, предоставляемое разработчиком. С точки зрения культуры, придерживающейся свободных взглядов на информацию, под это очень трудно подстроиться. Распространение информации о доступе к внутренним процессам Windows и интерпретации полученной информации заняло много лет.

Поинтересуйтесь, откуда берется результат, выдаваемый тестировщиком

Важно понимать не только отлаживаемую систему, но и средства, используемые для отладки. Однажды Том помогал сетевому технику со следующей проблемой: компьютер не мог обмениваться информацией ни с одним сервером, хотя индикатор наличия связи светился. Техник отключил компьютер от сети и подключил новое портативное устройство,

которое могло тестировать и выявлять большое количество сетевых проблем. Однако устройство отображало список результатов без информации о том, как оно их получило. Техник, не задумываясь, обосновывал свои решения на данных этого устройства. Том спросил: «Устройство пишет, что оно подключено к сети B, но как оно это определило?» Техник не знал этого или ему было все равно. Том сказал: «Я не думаю, что оно действительно подключено к сети B! Сейчас сети B и C соединены, поэтому, если разъем работает, оно должно писать, что одновременно подключено к сетям B и C». Техник не согласился, потому что такое дорогое устройство не могло ошибаться и проблема должна быть с компьютером.

Оказалось, что устройство угадывало IP-сеть после нахождения единственного узла в сегменте локальной сети. Этот разъем был подключен к концентратору, к которому была подсоединена другая рабочая станция в другом офисе. Соединение концентратора с магистральным каналом отключилось от остальной сети. Без знания того, как устройство осуществляло свои проверки, не было возможности определить, почему оно выводило такое сообщение, и дальнейшая отладка оказалась бы напрасной. К счастью, был подозрительный признак – устройство не указывало сети C. Процесс разбора результата привел к истинной причине проблемы.

Что делает инструмент хорошим? Мы предпочитаем малые инструменты крупным и сложным. Лучшее средство – это то, которое обеспечивает простейшее решение проблемы. Чем сложнее средство, тем больше вероятность того, что оно будет действовать по-своему или просто будет слишком большим, чтобы добраться до источника проблемы.

Проблемы с подключением разделов NFS могут решаться тремя простыми средствами: `ping`, `traceroute` и `rpcinfo`. Каждое из них выполняет одну функцию, и выполняет ее хорошо. Если клиент не может подключиться к конкретному серверу, убедитесь, что между ними проходят эхо-запросы и ответы. Если не проходят, то это проблема сети и `traceroute` может ее локализовать. Если `ping` проходит, то связь работает и проблема, должно быть, в протоколе. Со стороны клиента элементы протокола NFS можно проверить при помощи `rpcinfo`[1]. Вы можете проверить `traceroute` с `portmap`, а затем с `mountd`, `nfs`, `nlockmgr` и `status`. Если ничего не получится, то можно сделать вывод, что соответствующая служба не работает. Если все будет работать, вы можете сделать вывод, что это проблема разрешения экспорта. Обычно это означает, что имя узла, указанное в таблице экспорта, не соответствует тому, что видит сервер при обратном DNS-запросе. Это чрезвычайно мощная диагностика, осуществляемая очень простыми средствами. Вы можете использовать `rpcinfo` для всех протоколов Sun, основанных на RPC (Stern 1991).

Протоколы, основанные на TCP, часто можно отлаживать при помощи других трех средств: `ping`, `traceroute/tracert` и `telnet`. Эти средства доступны на всех платформах, поддерживающих TCP/IP (Windows, UNIX и др.). Опять же, для диагностики проблем соединения используются средства `ping` и `traceroute`, затем можно воспользоваться `telnet` для ручной симуляции многих протоколов, основанных на TCP. Например, администраторы электронной почты знают достаточно об SMTP (Crocker 1982), чтобы при помощи TELNET подключиться

[1] Например, `rpcinfo -T udp servername portmap` в Solaris или `rpcinfo -u servername portmap` в Linux.

к порту 25 и ввести команды SMTP, как если бы они были клиентом; изучая результаты, можно выявить многие проблемы. Аналогичные методы работают для NNTP (Kantor and Lapsley 1986), FTP (Postel and Reynolds 1985) и других основанных на TCP протоколах. В книге *«TCP/IP Illustrated, Volume 1»* У. Ричарда Стивенса (Stevens 1994) предоставлен прекрасный обзор работы протоколов.

Иногда лучшие средства – это простые средства собственной разработки или комбинация других небольших инструментов и приложений, как показано в следующем примере.

Обнаружение проблемы задержки

Однажды Тому сообщили о большой задержке в сетевом соединении. Проблема появлялась только периодически. Он запустил постоянный (один раз в секунду) эхо-запрос между машинами, который должен был показать проблему, и записывал его результаты несколько часов. Он наблюдал постоянное хорошее (низкое) значение задержки, за исключением периодических проблем. Для анализа логов, выявления запросов с высокой (более чем в три раза выше среднего значения первых 20 запросов) задержкой и выделения запросов без ответа была написана небольшая программа на Perl. Он заметил, что запросов без ответа не было, но время от времени ответы на несколько запросов приходили гораздо позже. Он воспользовался электронной таблицей для построения графика по временной оси. Визуализация результатов помогла ему заметить, что проблема появлялась каждые 5 мин с отклонением 1–2 с. Она появлялась и в другое время, но каждые пять минут она возникала всегда. Могло ли обновление таблицы маршрутизации перегружать процессор маршрутизатора? Перегружал ли протокол соединение?

В процессе исключения он локализовал проблему на конкретном маршрутизаторе. Его процессор был перегружен расчетами таблицы маршрутизации, которые проходили каждый раз при реальном изменении сети плюс каждые пять минут при обычном обновлении таблицы маршрутизации. Это согласовывалось с ранее собранными данными. То, что это был перегруженный процессор, а не перегруженное сетевое соединение, объясняло, почему задержка росла, а пакеты не терялись. В маршрутизаторе был достаточный буфер для обеспечения сохранности всех пакетов. После устранения проблемы с маршрутизатором снова были применены тест эхо-запросов и анализ логов, чтобы убедиться в устранении проблемы.

Пользователь, который сообщил о проблеме, был ученым с очень высокомерным отношением к системным администраторам. После того как подтвердилось устранение проблемы, ему показали методику, в том числе временные графики. Его отношение значительно улучшилось, когда он увидел, насколько совершенными были их методы.

Относитесь к настройке как к отладке

Быстродействие сети ограничивается шестью типами ошибок:

1. Потери, повреждение пакетов, перегрузка каналов связи, плохое оборудование

2. IP-маршрутизация, большое время двойного оборота
3. Нарушение порядка пакетов
4. Недостаточный размер буферов
5. Недопустимые размеры пакетов
6. Неэффективные приложения

Любая из этих проблем может скрывать все остальные проблемы. Вот почему решение проблем с быстродействием требует высокого уровня подготовки. Так как средства отладки редко являются очень хорошими, тестирование становится «чем-то вроде поиска самого слабого звена невидимой цепи» (Mathis 2003). Следовательно, если вы решаете любую из перечисленных проблем и у вас ничего не получается, остановитесь и подумайте, может быть, это какая-то другая проблема.

15.2. Тонкости

Тонкости предполагают реальное развитие основ: лучшие средства, лучшие знания о применение средств и лучшее понимание отладки системы.

15.2.1. Лучшие средства отладки

Лучшие средства лучше! Всегда найдется место для новых средств, которые лучше старых. Может быть, трудно постоянно быть в курсе последних разработок и легко упустить возможность первым принять на вооружение новую технологию. Ряд форумов, например конференции USENIX и SAGE, а также вебсайты и почтовые рассылки могут помочь вам узнавать об этих новых средствах, как только они появляются.

Мы сторонники простых средств. Улучшение инструментов не должны быть их усложнением. На самом деле иногда новизна средства заключается в его простоте.

При выборе новых средств оценивайте их по проблемам, которые они могут решать. Постарайтесь не обращать внимания на аспекты, которые являются показными, данью веяниям моды. Наличие «**модных слов**» означает, что продукт поддерживает модные в данный момент тенденции в отрасли и постоянно появляется на обложках журналов вне зависимости от того, приносит ли эта помпезность какую-то пользу.

Спросите: «Какую реальную проблему он будет решать?» Продавцу легко направить ваше внимание на показные, яркие аспекты, но делает ли это продукт полезнее? Используется ли цвет разумно, для выделения важных деталей, или просто для красоты? Актуальны ли «модные слова» о нем? Конечно, он поддерживает SNMP, но можно ли будет интегрировать его в вашу систему SNMP-мониторинга? Или SNMP используется просто для настройки устройства?

Попросите пробную версию продукта и найдите время поработать с ним в течение пробного периода. Не бойтесь отослать его обратно, если не посчитаете полезным. Продавцы не слишком обидчивы, и обратная связь, которую вы предоставляете, поможет разработчикам в дальнейших версиях сделать продукт лучше.

15.2.2. Формальное обучение работе со средствами отладки

Несмотря на то что инструкции – это здорово, формальное обучение может стать преимуществом, которое отличает вас от других. Формальное обучение имеет ряд преимуществ.

- Обычно предоставляется обучение вне места работы, что исключает постоянное прерывание работы и позволяет сосредоточиться на овладении новыми навыками.
- Формальное обучение обычно охватывает все функции, а не только те, которые у вас было время попробовать.
- Преподаватели часто обнаруживают ошибки или особенности, о которых разработчик мог не захотеть рассказать в руководстве.
- Часто у вас есть доступ к лаборатории машин, где вы можете испытывать то, что не смогли бы испытать в других условиях из-за рабочих требований.
- Вы можете указать в своем резюме, что прошли обучение, больше заинтересовав потенциальных работодателей этим, чем своим фактическим опытом, особенно если вы получили сертификат.

15.2.3. Понимание системы от начала до конца

Наконец, высшая точка организации работы по отладке – наличие по крайней мере одного человека, который понимает, как работает система, от начала и до конца. В небольшой системе это просто. Однако по мере того, как системы растут и становятся более сложными, люди специализируются и получается так, что они знают только свою часть системы. Наличие человека, знающего всю систему в целом, бесценно в случае крупной аварии. В серьезной экстренной ситуации лучше всего собрать команду экспертов, каждый из которых представляет один уровень иерархии.

Пример: архитекторы

Как найти сотрудников, имеющих такие глубокие знания? Один из способов – развивать своих сотрудников.

В Synopsys имелись должности «архитекторов» в каждой технологии – они были как раз такими людьми со всеобъемлющими знаниями. Эти архитекторы имели глубокие знания в более широкой области, чем их технология, и они были хорошими разноплановыми специалистами. Их официальной функцией было отслеживание направления развития отрасли: они предсказывали потребности и технологии на следующие 2–5 лет и готовились к ним (создавали прототипы, тестировали альфа/бета-версии и помогали разработчикам придерживаться определенного направления), проектировали новые службы, наблюдали, что происходит в группе, направляли людей к более разумным и масштабируемым решениям и т. д. Выполняя эти функции, они всегда были рядом, когда для поиска серьезных проблем требовались глубокие знания.

Таинственное удаление файлов

Вот пример ситуации, где для устранения проблемы требовались глубокие знания. Пользователь обнаружил, что некоторые его файлы исчезали. Если быть более точным, у него было около 100 Мб данных в личной папке, и все, кроме 2 Мб, исчезло. Он восстановил свои файлы. В среде была система, которая позволяла пользователям восстанавливать файлы из резервных копий без вмешательства системных администраторов. Однако два дня спустя случилось то же самое, на этот раз остались другие файлы, и снова их общий объем был равен 2 Мб. Это продолжалось пару недель, но он не чувствовал большого неудобства от необходимости восстанавливать свои файлы и стеснялся беспокоить системных администраторов такой нелепой проблемой.

Первым предположением системных администраторов было наличие вируса, но сканирование на вирусы ничего не выявило. Следующим предположением было, что кто-то решил таким образом подшутить над ним или задание для планировщика cron было написано неправильно. Пользователю дали номер пейджера, на который он должен был позвонить при следующем исчезновении файлов. Одновременно, для того чтобы отследить, кто удалял на том сервере файлы, были запущены сетевые анализаторы трафика. На следующий день пользователь сообщил системным администраторам, что его файлы исчезли. Его спросили: «Какое ваше действие было последним?». Он просто вошел в систему на машине в лаборатории, чтобы попутешествовать по Интернету. Системные администраторы были озадачены. Средства сетевого мониторинга показывали, что удаления не осуществлялись ни с компьютера пользователя, ни с машины злоумышленника, ни с неправильно запрограммированного сервера. Системные администраторы сделали все, чтобы устранить проблему, пользуясь своими знаниями об элементах системы, но проблема оставалась нерешенной.

Вдруг один из старших системных администраторов, идеально знающий системы, в том числе Windows, UNIX и все соответствующие протоколы, понял, что веб-броузеры хранят кэш, который очищается, чтобы его размер оставался ниже определенного предела, часто равного 2 Мб. Мог ли броузер на этой машине удалять файлы? Разбор показал, что на машине в лаборатории был веб-броузер, в котором было настроено странное размещение кэша. Это размещение было вполне нормальным для некоторых пользователей, но, когда в систему заходил этот пользователь, размещение было эквивалентным его личной папке из-за ошибки (или особенности?), связанной с тем, как Windows распознавала пути к папкам, которые включали несуществующие подпапки. Броузер находил кэш со 100 Мб данных и удалял файлы, пока используемое пространство не становилось менее 2 Мб. Это объясняло, почему при каждом появлении проблемы оставались разные файлы. После исправления конфигурации броузера проблема была устранена.

Первоначальные попытки решения проблемы – сканирование на вирусы, проверка заданий планировщика cron, отслеживание протоколов – оказались бесполезными, потому что они проверяли отдельные части. Проблема была решена только тем, кто обладал целостным пониманием системы.

Знание физики иногда помогает

Иногда недостаточно даже всеобъемлющего знания системы. В двух известных случаях для отслеживания первопричины проблемы потребовалось знание физики.

В книге «*The Cuckoo's Egg*» (Stoll 1989) описана реальная история о том, как Клифф Столл (Cliff Stoll) отслеживал злоумышленника, который пользовался его компьютерной системой. За счет отслеживания сетевой задержки и применения некоторых физических расчетов Столл смог точно определить, в какой точке мира находится злоумышленник. Книга читается как шпионский роман, но все было на самом деле!

Знаменитая история «Случай с отправкой электронной почты на 500 миль» и связанные с ней FAQ (Harris 2002) описывает попытку Трея Харриса (Trey Harris) устранить удивительную проблему. История началась со звонка начальника отдела статистики его университета, который утверждал: «Мы не можем отправить электронную почту дальше чем на 500 миль». Объяснив, что «электронная почта на самом деле работает не так», Харрис начал расследование, которое показало, что эта проблема, к его удивлению, действительно существовала. Время ожидания было установлено слишком низким, что вызывало проблемы, если система подключалась к серверам, которые находились достаточно далеко, чтобы время двойного оборота было больше, чем очень маленькое число. Расстояние, которое свет проходил за это время, было равно 3 световым миллисекундам, или приблизительно 558 милям.

15.3. Заключение

Каждый системный администратор занимается отладкой и обычно создает мысленный список стандартных решений распространенных проблем. Однако отладка должна быть системным, или методическим, процессом, основанным на знании того, что пытается сделать пользователь, и направленным на устранение первопричины проблемы, а не ее симптомов. Некоторые методы отладки являются субстрактивными – процесс исключения, – а другие аддитивны – последовательное уточнение. Устранение первопричины важно, поскольку, если она не будет устранена, проблема появится снова, создавая, таким образом, больше работы системному администратору.

Несмотря на то что в данной главе основное внимание уделяется максимально быстрому решению возникшей проблемы, иногда вы должны обеспечивать быстрый обход проблемы, чтобы устранить причину позже (см. главу 14). Например, вы можете выбрать быстрое исправление в рабочее время и использовать интервалы техобслуживания (глава 20) для внесения постоянных и глобальных исправлений.

Лучшие средства помогают решать проблемы более эффективно, не внося чрезмерной сложности. Формальное обучение использованию этих средств предоставляет знания и опыт, которые вы не сможете получить из инструкции. Наконец, в случае серьезного сбоя или когда проблема кажется специфической, ничто не заменит одного или нескольких человек, знающих систему от начала до конца.

Простые средства помогают решать серьезные проблемы. Сложные средства иногда скрывают, как они принимают решения.

Отладка часто предполагает общение между вами и вашими пользователями. Вы должны понять проблему в плане того, что пользователь пытается выполнить и как проблема проявляется.

Задания

1. Выберите технологию, с которой вы работаете. Назовите средства отладки, которыми вы пользуетесь для этой технологии. Для каждого средства укажите, является ли оно собственной разработкой, коммерческим или бесплатным? Можно ли использовать его совместно с другими средствами? Какое формальное или неформальное обучение работе с этим средством вы прошли?
2. Опишите недавнюю техническую проблему, с которой вы столкнулись, и способ, которым вам удалось ее решить.
3. В истории в разделе 15.1.4 пользователь был впечатлен методикой, использованной для решения его проблемы. Как бы ситуация отличалась, если бы пользователь был нетехническим менеджером, а не ученым?
4. Какие средства, которых у вас нет, вы хотели бы иметь? Почему?
5. Выберите одно средство, которым вы часто пользуетесь. Опишите в технических терминах, как оно работает.

Глава 16

Однократное устранение проблем

Исправить что-то один раз лучше, чем исправлять это постоянно. Несмотря на то что это кажется очевидным, иногда такой подход невозможен из-за тех или иных ограничений, либо оказывается, что вы постоянно исправляете одну и ту же неполадку, не понимая этого, либо решение на скорую руку просто кажется более удобным. Учитывая это, вы можете поставить перед собой несколько целей. Во-первых, вы можете лучше планировать свое время. Во-вторых, вы можете стать лучшим системным администратором. В-третьих, если это необходимо, вы лучше можете объяснить пользователю, почему для исправления какой-то проблемы вам потребовалось больше времени.

В главе 15 рассматривался системный процесс устранения проблемы. Данная глава посвящена общей концепции текущей ситуации.

16.1. Основы

Один из наших любимых принципов – «исправляйте один раз». Если что-то нарушено, то это должно быть исправлено однократно, чтобы больше к этому не возвращаться. Если проблема может появиться на других машинах, то на них нужно проверить ее наличие и исправить неполадку.

16.1.1. Не тратьте время зря

Иногда, особенно в случае с проблемами, которые кажутся тривиальными или затрагивают вас, только когда проявляются, может показаться легче исправить что-то на скорую руку, не устраняя проблемы окончательно. У вас может даже не возникнуть мысли о том, что вы постоянно решаете одну и ту же проблему, которая могла быть устранена однократно ценой чуть бóльших усилий.

Устраняйте проблемы однократно

Однажды Том помогал системному администратору перенастраивать два больших сервера Sun Solaris. Конфигурация требовала большого количества перезагрузок для проверки каждого этапа процесса. После каждой перезагрузки системный администратор входил в систему снова. Учетная запись `root` на этом узле не имела правильно установленных `tty` `TERM`, `PATH` и других системных переменных. Обычно это не беспокоило его. Например, было неважно, что переменная `TERM` не установлена, потому что он

не пользовался никакими средствами, основанными на curses[1]. Однако это означало, что его консоль не поддерживала редактирование в командной строке. Без него ему приходилось набирать заново гораздо больше, чем обычно требовалось. Он работал в консоли, поэтому у него даже не было мыши, при помощи которой можно вырезать и вставлять текст. В конце концов ему понадобилось отредактировать файл при помощи экранного редактора (vi или emacs) и он установил свою переменную TERM, чтобы можно было пользоваться программой.

Тому было тяжело смотреть, как этот человек вновь и вновь вручную устанавливал эти переменные. Однако, по мнению системного администратора, его подход был очень рациональным, потому что он тратил время на установку той или иной переменной только непосредственно перед тем, как она требовалась в первый раз. Иногда он загружался, вводил одну команду и перезагружался, это было очень крупным выигрышем, учитывая, что в этот раз не надо было устанавливать никаких переменных. Однако в случае более длинных сеансов Тому казалось, что системный администратор отвлекался от проблемы из-за необходимости отслеживать, какие переменные еще не были установлены. Часто у системного администратора что-то не получалось из-за отсутствия нужных переменных, после чего он устанавливал их и заново вводил команду.

Наконец Том вежливо предположил, что, если бы у системного администратора был файл /.profile с установленными переменными, он мог бы уделять больше внимания проблеме, чем рабочей среде. *Исправляйте неполадку однократно, вывод A: устраняйте проблему раз и навсегда*.

Системный администратор согласился и начал с нуля создавать файл /.profile узла. Том остановил его и напомнил, что, вместо того чтобы создавать файл /.profile с нуля, ему следовало скопировать его с другого узла. *Исправляйте неполадку однократно, вывод B: используйте то, что уже сделали другие, не изобретайте велосипед*. Копируя стандартный файл /.profile, который имелся на большинстве других узлов в той лаборатории, системный администратор использовал уже имеющиеся возможности. Кроме того, он снижал неупорядоченность системы, выбирая машину, отличающуюся от других, и делая ее такой же, как все.

После того как системный администратор скопировал файл /.profile с другой машины, Том спросил, зачем они вообще все это делали. Разве в Solaris JumpStart уже не было хорошего файла /.profile, который имелся на всех остальных машинах? В главе 3 мы видели преимущества автоматизации трех серьезных этапов установки: загрузки ОС, обновления ОС и конфигурации сети. В этой среде был сервер JumpStart, почему им не воспользовались?

Оказалось, что эта машина пришла из другого места и владелец просто настроил ее IP-адрес, он не пользовался JumpStart (риск таких действий в плане безопасности – совершенно другой вопрос). Это было сделано для экономии времени, потому что вряд ли узел остался бы там больше чем на пару дней. Год спустя он все еще был там. Том и системный администратор расплачивались за пользователей, которые хотели сэкономить

[1] Библиотека в UNIX, позволяющая обеспечить подобие графического интерфейса в текстовом режиме. – *Примеч. науч. ред.*

время. Пользователь сэкономил время, но за счет времени Тома и системного администратора.

Затем Том понял еще кое-что. Если на машине не использовался JumpStart, то вряд ли она была внесена в список узлов, которые автоматически обновляли систему. Этот узел не обновлялся с момента своего создания. Он был небезопасно настроен, не имел ни одного из недавних обновлений по безопасности и не проверялся на проблему Y2K – 1 января 2000 года у него точно возникли бы проблемы.

Исправляйте неполадку однократно, вывод С: устраняйте проблему на всех узлах одновременно. Изначально проблема была в том, что в Solaris включен очень малый файл /.profile. Решением в данной компании была установка лучшего файла /.profile в момент установки системы через JumpStart. Проблема была устранена на всех узлах одновременно за счет того, что ее устранение было частью процедуры установки. Если файл требовалось изменить, можно было воспользоваться системой обновления для распространения новой версии по всем машинам.

В итоге процедура, которую нужно было проделать Тому и его сотруднику, потребовала вдвое большего времени, потому что на узле не использовался JumpStart. Часть задержек была вызвана тем, что этой системе не хватало стандартной, продуманной и дружественной к системному администратору конфигурации. Другие задержки были связаны с тем, что в ОС имелось много неправильно или не полностью настроенных функций.

Этот случай лишний раз напоминает о том, что правильное построение основ настолько хорошо, что вы забываете, как было плохо, когда вы не выстроили основы правильно. Том привык к системам, в которых узлы были правильно настроены. Он принимал это как должное.

16.1.2. Избегайте временных решений

Предыдущий раздел был довольно оптимистичным в плане возможности в каждой ситуации исправить неполадку наилучшим образом. Однако это не всегда возможно. Иногда ограничения по времени или ресурсам требуют быстрого решения, пока нельзя запланировать полное устранение проблемы. Иногда полное исправление может требовать неприемлемого в определенных ситуациях прерывания обслуживания и приходится довольствоваться временными мерами, пока не будет назначен технологический перерыв. Иногда временные меры требуются из-за причин, связанных с ресурсами. Может быть, для устранения проблемы нужно написать программу или установить оборудование. Это займет определенное время. Если диск заполнен логами, то постоянной мерой может стать установка программы, обновляющей логи. Установка такой программы может занять определенное время, но в это время можно удалить старые логи вручную.

Важно, чтобы за временными решениями следовали постоянные. Для этого требуется определенный механизм, чтобы проблемы не оставались незамеченными. Возвращаясь к нашему примеру с диском, заполненным логами, при большой рабочей нагрузке может быть очень соблазнительно удалить старые логи и перейти к следующей задаче, не отметив, что к вопросу нужно вернуться

для его окончательного решения. Записывать такие действия может быть трудно. Написанные на бумаге заметки теряются. Не у каждого всегда есть под рукой ежедневник. Гораздо проще отправить себе напоминание по электронной почте. Наличие приложения, позволяющего отправлять новые заявки по электронной почте, даже лучше. Если вы можете создать новую заявку при помощи электронной почты, то будете способны создать ее где угодно, чтобы вам не нужно было помнить о ней. Обычно электронную почту можно отправлять с сотового телефона, двустороннего пейджера, коммуникатора или КПК.

UNIX-системы обычно можно настроить для отправки электронной почты из командной строки. Не нужно ждать, пока запустится почтовый клиент. Просто введите одно-два предложения для напоминания и создайте заявку позже, когда будет время[1]. Однако нужно отметить следующее: во многих местах UNIX-системы настраиваются так, что могут правильно отправлять электронную почту, только если являются частью цепи доставки электронной почты. Поэтому электронная почта, отправленная из командной строки на других машинах, не доставляется. Очень легко создать простую конфигурацию «нуль-клиента» или «перенаправления всей электронной почты на сервер», которая устанавливается как опция настройки по умолчанию. Другие способы являются непрофессиональными и ведут к путанице, связанной с потерей электронной почты.

Временные меры чисто психологически кажутся проще постоянных. Мы чувствуем, что сделали что-то значительное за небольшое время. Для нашего самомнения это гораздо приятнее, чем начинать крупный проект для однократного устранения проблемы или добавления нового пункта в наш бесконечный список дел.

Исправление одних и тех же мелких недостатков раз за разом входит в привычку. С точностью собаки Павлова мы выполняем одни и те же действия каждый раз, когда наши системы мониторинга уведомляют нас о проблеме. После этого мы убеждаем себя покончить с проблемой раз и навсегда: «В следующий раз у меня будет время для окончательного исправления!» Со временем мы начинаем так хорошо делать временные «заплатки», что забываем о существовании постоянных мер. Мы ощущаем себя постоянно занятыми, но не чувствуем, что что-то выполняем. Мы просим начальников или коллег взглянуть на наш рабочий день свежим взглядом. Сделав это, они видят, что наше время тратится на вытирание пола, вместо того чтобы просто выключить воду.

Мы так привыкаем к временным мерам, что становимся в них экспертами. Стыдно, но, обнаруживая, насколько мы преуспели в них, мы гордимся своими успехами, демонстрируя написанные нами макросы и другие методы экономии времени, которые мы нашли.

Такая ситуация является распространенной. Чтобы ее предотвратить, нужно разорвать замкнутый круг.

Пример: недоставленная электронная почта

Том осуществлял много рассылок при помощи Majordomo, очень простого менеджера рассылок, который управляется сообщениями электронной почты для командного процессора, запрашивающими начало и окончание подписки. Сначала он старательно изучал каждое сообщение о недостав-

[1] В Bell Labs у Тома была репутация сотрудника с практически равным количеством собственных заявок и заявок от пользователей.

ке и узнавал, что адрес электронной почты в определенном списке был уже недействительным. Если адрес оставался недействительным в течение недели, он удалял человека из списка рассылки. Он повысил эффективность своей работы при помощи программы фильтрации электронной почты, которая отправляла сообщения о недоставке в определенную папку, где он каждые несколько дней просматривал все сообщения. Затем он установил скрипты, которые помогали ему выявить проблему – отслеживать, кому не доставлялись сообщения и продолжалось ли это в течение недели, – и макрос, удалявший людей из списков рассылки.

В конце концов оказалось, что он каждый день проводил за этой работой более часа. Это влияло на сроки выполнения других его проектов. Он знал, что другие программы (Viega, Warsaw and Memheimer 1998) обрабатывали бы сообщения о недоставке лучше или передали бы работу владельцам отдельных списков рассылки, но у него никогда не было времени установить эти программы. Он вытирал пол, вместо того чтобы выключить воду.

Единственным для Тома способом разорвать этот замкнутый круг было игнорировать сообщения о недоставке в течение недели и пару раз задержаться после работы, чтобы установить новую программу, не отвлекаясь от работы и не затрагивая сроки выполнения других проектов. Даже после этого проект пришлось отложить, по крайней мере ненадолго. Когда Том наконец принял решение, установка и тестирование программы заняли примерно 5 ч. Новая программа снизила время его вмешательства до 1 ч в неделю, экономя 4 ч в неделю, то есть половину рабочего дня каждую неделю. Каждый год Том терял бы около месяца рабочих дней, если бы не отказался от временных мер в пользу постоянного решения.

Давайте более подробно рассмотрим вывод А: устраняйте проблему раз и навсегда. Конечно, он кажется простым, однако мы часто видим, что неполадку исправляют только для того, чтобы увидеть, что при перезагрузке она появляется снова. Иногда знание того, какие меры являются постоянными, а какие при перезагрузке нужно повторять, как раз и отличает неопытного системного администратора от мастера.

Многие ОС запускают скрипты, или программы, при загрузке машины. Скрипты, включенные в процесс загрузки машины, нужно время от времени редактировать. Иногда нужно запустить новый демон, например HTTP-сервер Apache. Порой нужно внести изменение в конфигурацию, например установить флаг на новом сетевом интерфейсе. Вместо введения этих команд вручную при каждой перезагрузке машины их нужно внести в скрипты автозагрузки. Будьте внимательны при написании таких скриптов. Если в них вкрадется ошибка, система может больше не загрузиться. Мы всегда перезагружаем машину вскоре после изменения любых скриптов автозагрузки, таким способом мы выявляем проблему сразу, а не через несколько месяцев, когда перезагрузка машины действительно потребуется.

Пример: постоянные настройки конфигурации

Реестр Microsoft Windows решает многие из этих проблем. Содержимое реестра постоянно и сохраняется при перезагрузке. У каждой хорошо написанной программы есть записанные в реестре параметры и конфигурация. Программам не нужно изобретать велосипед. Каждая служба, или демон, как они называются в UNIX, может не запуститься, не прерывая при этом весь процесс загрузки.

В какой-то мере Майкрософт попыталась исправить это однократно, предоставив разработчикам программ реестр, панель управления службами и панель управления устройствами, вместо того чтобы требовать от каждого разрабатывать что-то подобное для всех продуктов.

16.1.3. Учитесь у плотников

Системные администраторы могут многому научиться у плотников. Они строили и ремонтировали гораздо дольше, чем мы.

Плотники говорят: «Семь раз отмерь, один отрежь». Повторное измерение предотвращает множество ошибок. Дерево стоит дорого. Небольшое дополнительное внимание стоит недорого по сравнению с потраченным зря деревом.

Кроме того, плотники понимают, как копировать предметы. Плотник, которому нужно отрезать несколько деревянных брусков одного размера, отрезает первый брусок нужной длины и использует его для измерения других. Это гораздо точнее, чем пользоваться вторым бруском для измерения третьего, третьим – для измерения четвертого и т. д. Последний метод легко приводит к накоплению ошибок.

Системные администраторы могут многое почерпнуть из этих методов. Копирование чего-либо – это возможность один раз сделать что-то правильно, а затем повторить это много раз. Измерять несколько раз – хорошая привычка. Проверяйте свою работу дважды, прежде чем окончательно внести какие-либо изменения. Перечитайте файл конфигурации, попросите кого-нибудь еще посмотреть на команду перед выполнением, проверьте емкость системы, прежде чем рекомендовать расширение. Проверяйте, проверяйте и еще раз проверяйте.

Будьте осторожны при удалении файлов

В оболочках UNIX легко случайно удалить файлы. Это иллюстрируется классическим для UNIX примером, когда пытаются удалить все файлы, которые заканчиваются на .o, но случайно вводят команду `rm * .o` – обратите внимание на пробел, ошибочно вставленный после символа `*`, – и удаляют все файлы в директории. К счастью, в UNIX-оболочках также легко «семь раз отмерить». Вы можете заменить `rm` на `echo`, чтобы просто перечислить файлы, которые будут удалены. Если будут перечислены правильные файлы, вы можете воспользоваться редактированием командной строки, чтобы заменить `echo` на `rm`.

Такой подход – отличный метод «семь раз отмерить» за счет осуществления быстрой проверки для предотвращения ошибок. Применение редактирования командной строки аналогично применению первого деревянного бруска для измерения следующего. Мы видели системных администраторов, которые пользовались этим методом, но вводили команду заново после того, как убеждались, что команда `echo` вывела все правильно, а это делает бессмысленным весь подход. Повторный ввод команды подвергает процесс риску накопления ошибок. Уделите время изучению редактированию командной строки в оболочке, которой вы пользуетесь.

Пример: Copy Exact

В Intel есть философия Copy Exact (точное копирование). Как только что-то сделано правильно, это точно копируется в других местах. Например, если построен завод, дополнительные мощности создаются его точным копированием в других местах. Не нужно изобретать велосипед. Системные администраторы также используют эту политику. Полезные скрипты распространяются по другим местам и используются без изменений, устраняя беспорядок с системами, немного различающимися в каждом месте. Это вынуждает всех системных администраторов поддерживать одинаковые системы, разрабатывать код, который без адаптации работает во всех местах, и сообщать об усовершенствованиях автору первоначальной версии, чтобы распространить их повсюду, не пропуская таким образом ни одно место.

Пример: атомная энергия во Франции

После экспериментов с различными проектами атомных электростанций во Франции остановились на одном варианте, который используется на 56 атомных электростанциях. Из-за того что все станции должны быть одинаковыми, их было построить проще, чем эквивалентные американские. Что более важно, это упростило управление безопасностью. «Урок от происшествия на одной станции может быть быстро усвоен руководителями других 55 станций[1]». Это невозможно в США с их большим количеством различных энергетических компаний, у каждой из которых свои проекты.

Системные администраторы могут использовать этот принцип при проектирование сетей удаленных офисов, инфраструктур серверов и т. д. Повторение упрощает управление.

Вы никогда не услышите, чтобы плотник сказал: «Я подпилил эту доску три раза, а она еще слишком короткая!» Подпиливание одной и той же доски не сделает ее длиннее. Системные администраторы часто делают одно и тоже раз за разом, и их раздражает, что они постоянно получают одинаковые неудачные

[1] *http://www.pbs.org/wgbh/pages/frontline/shows/reaction/readings/french.html*

результаты. Вместо этого нужно попробовать что-то другое. Системные администраторы жалуются на проблемы безопасности и ошибки, но доверяют программному обеспечению от компаний без адекватных систем контроля качества. Системные администраторы запускают критически важные системы без брандмауэров для Интернета. Системные администраторы исправляют неполадки путем перезагрузки вместо устранения первопричины.

> **Отличный совет**
>
> В известной комнате UNIX в Bell Labs на стене висит небольшая табличка: «Перестаньте делать то, что не работает».

16.2. Тонкости

Данный раздел этой главы повествует о том, как устранять проблемы не самостоятельно, а за счет автоматизации. Один из типов автоматизации устраняет симптомы и сообщает системному администратору, чтобы он обеспечил постоянные меры. Другой тип автоматизации принимает постоянные меры самостоятельно.

Автоматизация, устраняющая проблемы, может быть опасной. Мы видели слишком много плохой фантастики, в которой робот «устраняет» проблему, убивая невинных людей или уничтожая Землю. Следовательно, автоматизация должна быть особенно осторожной в своих действиях и должна вести логи, чтобы ее работу можно было проверить.

Автоматизация часто исправляет симптомы, не устраняя первопричину. В данной ситуации очень важно, чтобы автоматизация обеспечивала сообщение о том, что что-то было сделано, – тогда человек сможет обеспечить принятие постоянных мер. Мы видели автоматизацию, которая решает проблему заполнения диска путем удаления старых файлов логов. Это работает хорошо, пока потребители дискового пространства не потеснят чрезмерно файлы логов и удаляемые файлы логов вдруг не станут слишком маленькими. Тогда автоматизация требует немедленного вмешательства человека, а человек обнаруживает очень сложную проблему. Если бы автоматизация сообщила человеку, что она приняла временные меры, то она предоставила бы человеку время для принятия постоянных мер.

Однако в этом случае мы рискуем попасть в ситуацию «мальчика, который кричал про волка»[1]. Очень легко привыкнуть игнорировать предупреждения о том, что автоматика приняла временные меры и требуется более глобальное решение. Если в этот раз временные меры сработали, то они сработают и в следующий раз. В первый раз игнорировать такое сообщение обычно безопасно. Постоянные меры нужно принимать в следующий раз. Так как у системного

[1] Имеется в виду детская сказка. Один пастушок просто для забавы часто звал людей на помощь для защиты от волка, которого на самом деле не было. Когда волк и вправду напал на стадо, на помощь никто не пришел, поскольку все подумали, что мальчик лжет и на этот раз. – *Примеч. науч. ред.*

администратора работы обычно всегда больше, чем времени на нее, нетрудно предсказать, что «следующий раз» может быть очень нескоро. В больших системах велика вероятность того, что предупреждения каждый раз будут видеть разные системные администраторы. Если каждый из них посчитает, что он проигнорировал сообщение первым, ситуация превратится в серьезную проблему.

Устранение самой проблемы редко можно автоматизировать. Автоматизация может помочь вам при небольшом сбое, но не способна исправить программное обеспечение с ошибками. Например, она может отключить неуправляемый процесс, но не может исправить ошибку в программе, которая делает его неуправляемым.

Иногда автоматизация может устранить саму проблему. Крупные системы с виртуальными машинами могут выделить дополнительные процессоры для ресурсоемких вычислений, увеличить размер заполненного раздела или автоматически переместить данные на другой диск. Некоторые типы файловых систем позволяют вам автоматически создавать виртуальную файловую систему, обычно выделяя свободный диск и присоединяя его к разделу. Это не сильно помогает, если диск был заполнен из-за неуправляемого процесса, создающего бесконечное количество данных, потому что новый диск будет заполнен так же быстро. Однако это устранит ежедневную рабочую проблему заполнения дисков. Вы можете добавить в систему пустые диски – и автоматизация обеспечит их присоединение к очередным практически заполненным виртуальным разделам. Это не заменяет хорошее планирование использования дискового пространства, но будет неплохим средством в качестве элемента вашей системы управления дисковым пространством.

Решением являются политика и поддержание порядка, выполнение которых, возможно, обеспечивается программами. Устранение проблем вместо их игнорирования требует поддержания порядка.

Иногда создание автоматизации требует много времени. Однако порой ее можно создать быстро. Основные этапы 5-минутной задачи можно интегрировать в скрипт. Затем можно добавить другие элементы задачи. Это может выглядеть как трата часа на автоматизацию 5-минутных задач, но в долгосрочной перспективе вы сэкономите время.

Пример: makefile

Makefile – это несколько инструкций, которые указывают системе, как перестроить файл, если файлы, использованные при его создании, были изменены. Например, если программа создана из пяти файлов C++, легко указать, что при обновлении любого из этих файлов программа должна быть перекомпилирована для создания нового объектного файла. Если будут изменены какие-либо объектные файлы, они должны быть перекомпонованы для сборки программы. Таким образом, можно сосредоточиться на редактировании файлов исходного кода, а не на том, чтобы запоминать, как перекомпилировать и собирать программу.

Системные администраторы часто забывают, что это средство разработки может принести им большую пользу. Например, вы можете создать makefile, который указывает, что, если был изменен файл /etc/aliases, нужно запустить программу `newaliases` для обновления индексированной

версии файла. Если этот файл нужно скопировать на другие серверы, инструкции в этом makefile могут включать команду для такого копирования. Теперь вы сможете сосредоточиться на редактировании нужных файлов, а последующие обновления будут автоматизированы.

Это отличный способ зафиксировать базовые данные о процессах, чтобы другим людям не приходилось им учиться.

16.3. Заключение

Лучше исправить что-то один раз, чем исправлять постоянно. В конечном итоге меры должны быть постоянными, а не временными. Вы не должны изобретать велосипед – старайтесь по возможности копировать решения, работоспособность которых известна. Лучше предупреждать проблемы: если вы обнаружите проблему в одном месте, исправьте ее на всех похожих узлах или во всех местах. Системному администратору легко привыкнуть к ситуации и забыть, что проблемы нужно устранять правильно. Однако иногда ограниченные ресурсы не позволяют системному администратору ничего другого, кроме как принять временные меры и запланировать окончательное решение на будущее. С другой стороны, системный администратор должен избегать привычки откладывать такие меры и следовать по пути повторного применения небольших «заплаток», который является психологически комфортным. Вместо этого следует найти время для реализации полного решения. В конце концов, лучше всего устранять проблемы правильным методом и своевременно.

Данная глава была чуть более философской, чем остальные. В первом примере мы увидели, как важно с самого начала усвоить основы. Если обеспечена автоматизация первоначальной загрузки и конфигурации ОС, большинства проблем просто не возникло бы. Во многих случаях постоянной мерой является обеспечение автоматизации. Однако у автоматизации есть свои недостатки. Создание автоматизации решения может занять много времени, и в ожидании завершения автоматизации у системного администратора могут появиться плохие привычки или невосприимчивость к напоминаниям о необходимости принятия постоянных мер. Тем не менее хорошая автоматизация может существенно снизить вашу загруженность работой и повысить надежность ваших систем.

Задания

1. Что вы часто исправляете, вместо того чтобы принять постоянные меры? Почему постоянные меры не были приняты?
2. Как вы пользуетесь подходом плотников, описанным в разделе 16.1.3?
3. Опишите ситуацию, в которой вам пришлось отложить принятие постоянных мер из-за ограниченных ресурсов.
4. Похожа ли ваша система мониторинга на «мальчика, который кричал про волка»?

Глава 17

Управление изменениями

Управление изменениями – это процесс, который обеспечивает эффективное планирование, реализацию и последующий анализ изменений, внесенных в систему. Это означает, что изменения хорошо документируются, имеют план отмены и возможность воспроизводства. Управление изменениями касается управления риском. Изменения, которые вносят системные администраторы, приводят к риску сбоя обслуживания их пользователей. Управление изменениями означает оценку этих рисков и управление ими посредством стратегий смягчения рисков. Оно включает заблаговременное планирование изменений, доведение информации до сотрудников, согласование графика, план проверки, план отмены и набор условий, определяющих, нужно ли реализовывать план отмены и когда. В данной главе рассмотрен базовый процесс, а дальнейшие главы показывают, как применяется управление изменениями в различных аспектах работы системного администратора.

Управление изменениями создает отчетные данные, которые могут быть использованы для определения, что было сделано, когда и почему. Элементом управления изменениями является обсуждение проекта с пользователями и другими группами системных администраторов до его реализации. Контроль версий, другой компонент управления изменениями, является процессом низкого уровня для контроля изменений в отдельных файлах конфигурации.

Управление изменениями – один из основных процессов развитой группы системного администрирования. Это механизм, посредством которого группа может обеспечить уверенность в том, что изменения, которые могут влиять на другие изменения, не произойдут одновременно. Это механизм снижения количества сбоев или проблем за счет того, что системные администраторы вынуждены продумывать различные аспекты изменения перед его реализацией. Это способ связи, который обеспечивает уверенность в том, что при внесении изменений все будут действовать согласованно. Другими словами, это означает снижение уровня ошибок и возможность быстрее справиться с ошибкой, когда она произойдет. Управление изменениями критически важно для компаний электронной коммерции, чьи доходы основаны на доступности в режиме 24/7.

17.1. Основы

В данном разделе мы рассмотрим, как управление изменениями связано с управлением риском, и покажем четыре основных компонента управления изменениями для системных администраторов:

1. *Общение и составление графика.* Общайтесь с пользователями и другими системными администраторами, чтобы они знали, что происходит, и составляйте график изменений, чтобы влияние было наименьшим.
2. *Планирование и проверка.* Планируйте, как и когда вносить изменение, как проверить, что все работает, и как и когда отменить изменение, если будут проблемы.
3. *Процессы и документация.* Изменения должны соответствовать стандартным процессам и хорошо планироваться, с рассмотрением всех возможных последствий. Изменения должны быть документированы и одобрены перед их реализацией.
4. *Контроль версий и автоматизация.* Используйте контроль версий для отслеживания изменений и облегчения отмены проблемных обновлений. По возможности автоматизируйте изменения, чтобы обеспечить точное и воспроизводимое выполнение всех процессов.

Мы покажем, как все вместе эти компоненты могут обеспечить плавное обновление системы с минимумом проблем.

Управление изменениями предполагает учет различных категорий изменяемых систем, типов вносимых изменений и особых процедур для каждой комбинации. Например, категории машин могут включать рабочие станции, серверы подразделений, системы корпоративной инфраструктуры, критические для бизнеса системы, присутствие в Интернете и рабочие системы электронной коммерции. Категории изменений могут включать управление учетными записями и доступом, обновление директорий, установку новой службы или программы, модернизацию существующей службы или программы, изменения оборудования, изменения политики безопасности или конфигурации.

Небольшие изменения могут выпасть из процесса компании по управлению изменениями и часто будут из него выпадать, наличие слишком громоздкого процесса для небольших изменений не позволит системным администраторам эффективно работать. Но значительные изменения должны быть предметом процесса полного управления изменениями. Наличие такого процесса означает, что системный администратор не может внести значительное изменение, не соблюдая правильную процедуру, которая предполагает общение с нужными людьми и планирование изменения на приемлемое время. В критических системах это может включать написание небольшого плана проекта с процедурами тестирования и планом отмены, который просматривается равными по должности или старшими системными администраторами, а также может предполагать назначение помощника для наблюдения и помощи с изменением. В разделах 17.1.2 и 17.1.3 структура связи и составление графика изменений рассмотрены более подробно.

Компания должна определить, какой уровень процесса управления изменениями должен быть у каждого элемента матрицы категорий машин/типов изменений. Очевидно, что критически важные для бизнеса системы нужно жестко контролировать. Изменения в отдельном компьютере могут не требовать такого контроля. Изменения в каждом компьютере в компании, скорее всего, будут его требовать. Наличие достаточного количества процессов для изменений и возможностей обзора изменений в более важных системах приводит к снижению числа потенциально затратных ошибок. Библиотека инфраструктуры информационных технологий (ITIL – Information Technology Infrastructure

Library) – ценный ресурс для дальнейшего изучения области управления изменениями и рабочих процессов системных администраторов. Процессы передовых методик ITIL становятся широко распространенными стандартами.

17.1.1. Управление риском

Управление риском – часть деятельности системного администратора. Основные риски, которые нас касаются, связаны с невыполненным обслуживанием, подклассом которого является потеря данных. Один из основных способов, при помощи которых системные администраторы управляют риском, – это создание резервных копий. Резервные копии являются элементом стратегии смягчения рисков, защищающим от потери данных и невыполненного обслуживания. В главе 25 мы более подробно рассмотрим, как различные технологии, такие как RAID, помогают нам смягчить риск невыполненного обслуживания из-за потери данных.

Первые шаги по управлению риском – это выявление рисков и количественная оценка рисков. На какие системы и службы может повлиять изменение? Каковы наихудшие возможные сценарии развития событий? Скольких ваших пользователей могут затронуть эти сценарии? Это помогает разделить машины по профилям использования, таким как инфраструктурные машины, серверы подразделения, критичные для бизнеса, или рабочие станции, и подсчитать количество машин, на которые влияет изменение.

Следующий шаг после оценки риска изменения – определить, как смягчить риск. Смягчение имеет пять основных компонентов. Первый из них – провести консультацию по изменению: касается ли это изменение удовлетворения потребностей бизнеса, влияет ли он на другие события и изменения, когда оно должно быть реализовано? Второй – это план тестирования: как оценить, было ли изменение успешным? Третий – план отмены: как вернуть старую службу или систему, если изменение не было успешным? Четвертый компонент – момент решения: как и когда нужно принимать решение о реализации плана отмены? Последний компонент – это подготовка: что вы можете сделать и проверить заранее, чтобы убедиться, что изменение проходит плавно и в минимальные сроки?

Важно заранее решить, при каких условиях обновление системы будет полностью остановлено. Остановка должна обеспечить достаточное время для реализации плана отмены до того, как служба снова должна начать работать. Время, к которому служба снова должна начать работать, может быть основано на обязательстве перед пользователями, потребностях бизнеса или обусловлено тем, что данное изменение является элементом большей последовательности изменений, которые будут затронуты, если служба не будет вовремя восстановлена.

Точка принятия решения часто является самым сложным элементом для системного администратора, который вносит изменение. Мы часто считаем, что можем потратить «еще только 5 минут», чтобы все заработало. Часто полезно, чтобы другой системный администратор или руководитель разделял вашу ответственность и обеспечивал, чтобы план отмены был реализован по графику, если изменение было неудачным.

В идеальном случае лучше всего внести и проверить изменение заблаговременно в тестовой лаборатории. Также может быть возможность заранее внести из-

менение на дополнительной машине, которой можно заменить нужную машину. Однако тестовые лаборатории и дополнительные машины – это роскошь, которую не все компании могут себе позволить, а некоторые изменения непригодны для тестирования в лабораторной среде.

17.1.2. Структура распространения информации

Распространение информации об изменении имеет два аспекта: обеспечение того, что вся группа системного администрирования знает о происходящем, и того, что об этом знают ваши пользователи. Когда каждый в группе хорошо информирован об изменениях, все системные администраторы смогут внимательно следить за проблемами, которые могут быть вызваны изменениями. Любые проблемы будут обнаружены раньше и смогут быть быстрее устранены.

Вам также потребуется разработать структуру распространения информации для информирования ваших пользователей об изменениях, которые вы вносите. Если изменения предполагают резкий переход, после которого старая служба, система или программа больше не будет доступна, вы должны обеспечить, чтобы все ваши пользователи, работающие со старой версией, смогли продолжить работу с новой версией. Если предполагается плавный переход и старая версия некоторое время будет доступна, вы должны обеспечить, чтобы все заранее знали, когда это произойдет, как им воспользоваться старой версией при необходимости и когда старая версия будет недоступна, если будет. Если вы добавляете службу, вы должны обеспечить, чтобы все люди, которые ее запрашивали, а также те, кому она может быть полезна, знали, как ею пользоваться, когда она будет доступной. Во всех трех случаях информируйте своих пользователей, когда работа будет успешно завершена и как сообщать о любых возможных проблемах.

Несмотря на то что информировать об изменениях и графике их реализации пользователей, чья работа может быть ими затронута, необходимо и правильно, вы должны постараться не заваливать пользователей слишком большим количеством сообщений. Если вы так поступите, пользователи их проигнорируют, посчитав неважными. Выбор нужных групп для сообщения о каждой службе требует понимания своей пользовательской базы и своих служб. Например, если вы знаете, что группа A пользуется службами A–K, а группа B – службами B, D и L–P, то вам нужно сообщить об изменениях в службе A только группе A, но об изменениях в службе B нужно проинформировать обе группы. Эта задача может показаться трудной, но ее правильное выполнение очень существенно для ваших пользователей.

Наиболее эффективный метод распространения информации отличается в разных компаниях и зависит от культуры компании. Например, в некоторых компаниях самым эффективным средством может быть новостная группа, на которую люди подписываются, где можно быстро просматривать заголовки сообщений на наличие важных тем. Однако другие компании могут не пользоваться новостными группами, поэтому электронная почта может быть более эффективной. В случае значительных изменений мы рекомендуем отправлять людям сообщение («толкать»), а не требовать, чтобы ваши пользователи каждые несколько дней проверяли определенную веб-страницу («тянуть»). Значительное изменение, как рассмотрено в разделе 17.1.3, – это крупномасштабное или критическое изменение.

Пример: график презентаций в Bell Labs

В исследовательском подразделении Bell Labs была очень мягкая компьютерная среда, которая не требовала слишком серьезного управления изменениями. Однако во время презентаций требовалась очень высокая стабильность. Поэтому исследовательский отдел пользовался простым календарным графиком презентаций с помощью UNIX-команды `calendar`.

Исследователи уведомляли системных администраторов о презентациях посредством обычной процедуры обращения в службу поддержки, и системные администраторы учитывали этот календарь при планировании времени отключения. Кроме того, в эти дни они избегали слишком рискованных изменений и совместных обедов, при которых много системных администраторов могли находиться далеко от здания. Если на презентации присутствовали члены совета директоров или члены правительства, системный администратор стоял наготове за дверью.

17.1.3. Составление графика

Распределение времени – ключевой компонент управления изменениями. Время внесения изменения может быть значительным фактором, влияющим на ваших пользователей. Мы кратко рассмотрим три типа изменений: штатные, критические и крупномасштабные обновления.

Штатное обновление может произойти в любое время и в основном незаметно для большей части пользовательской базы. Эти изменения происходят все время: обновление содержимого сервера директорий или базы данных аутентификации, помощь отдельному пользователю в настройке его системы, устранение проблемы с рабочей станцией или принтером либо изменение скрипта, обрабатывающего файлы логов для предоставления статистических данных. Вам не нужно планировать график штатного обновления; масштаб проблемы, которую может вызвать ошибка, очень ограничен в силу сущности задачи.

Крупномасштабные обновления затрагивают многие системы или требуют серьезного нарушения работы системы, сети либо службы. Что считается крупномасштабным – зависит от компании. Для большинства компаний все, что затрагивает 30% систем или более, является крупномасштабным обновлением. Крупномасштабные изменения включают модернизацию системы аутентификации, изменение инфраструктуры электронной почты или печати либо модернизацию базовой сетевой инфраструктуры. График этих изменений должен быть тщательно согласован с пользовательской базой при помощи механизма «толкания», например электронной почты. Крупномасштабные обновления не должны проходить все время. Если это происходит, проверьте, не стоит ли вам изменить классификацию тех или иных обновлений. В некоторых компаниях хотят, чтобы эти обновления происходили вне временных интервалов пиковой нагрузки, а в других может требоваться, чтобы все крупномасштабные обновления происходили в течение одного технического перерыва (см. главу 20).

Критические обновления могут не показаться масштабными или даже особенно заметными для ваших пользователей, но способны вызвать серьезное нарушение работы системы в случае проблемы. Критические обновления включают

изменение конфигурации маршрутизаторов, глобальных политик доступа, конфигурации межсетевых экранов или внесение изменений в критический сервер. У вас должен быть определенный способ заблаговременного сообщения вашим пользователям о критическом обновлении на случай проблем. Эти обновления будут происходить достаточно часто, и вам не требуется распространять слишком много информации, поэтому допустим механизм «вытягивания», например веб-страница или новостная группа. Службе поддержки нужно сообщить об изменении, проблемах, которые оно может вызвать, времени начала и окончания работы и с кем связаться в случае проблемы.

Критические обновления должны происходить вне интервалов максимальной загрузки, чтобы предоставить вам время на обнаружение и устранение любых проблем, прежде чем они затронут ваших пользователей. Время пиковой загрузки может различаться в зависимости от того, кто ваши пользователи. Если вы работаете в компании электронной коммерции, чей сайт используется в основном физическими лицами по вечерам или в выходные, лучшим временем для внесения изменений может быть 9 часов утра. Кроме того, человек, который внес критические изменения, не должен сразу уходить с работы домой после их внесения. Если вы делаете критическое изменение, подождите пару часов – ваше присутствие может понадобиться для устранения возможных проблем.

Пример: никаких изменений по пятницам

Один из пользователей Тома выполнял многие задачи системных администраторов, и вносимые им изменения и их график затрагивали Тома больше, чем кого-либо еще. Когда пользователь делал ошибку, обвиняли Тома, потому что некоторые системы группы зависели от систем пользователя. Конфронтация Тома и его пользователя заключалась в следующем.

В своей группе Том установил правило, запрещающее вносить изменения по пятницам, потому что в случае обнаружения ошибок в выходные дни будет меньше возможностей для их немедленного исправления, что повысит риск негативного воздействия на работу пользователей. Кроме того, Том не хотел портить себе выходные и считал, что пользователь также должен соблюдать это правило.

Пользователь полагал, что, вне зависимости от того, в какой день группа Тома вносила изменения, системные администраторы должны более тщательно проверять свою работу и поэтому не стоит так бояться изменений перед выходными или отпуском. Хотя его собственные изменения часто вызывали проблемы, он отказался признать, что даже в случае внимательной проверки изменений может случиться что-то непредвиденное или произойти ошибка. Кроме того, он упорно не соглашался с тем, что это повышает риск для других пользователей и что снижение этого риска было бы в интересах каждого.

Также пользователь считал, что системные администраторы должны вносить свои изменения в течение рабочего дня, потому что нет лучшего способа проверить систему, чем позволить реальным пользователям с ней работать. Он считал, что, если изменения будут сделаны в нерабочее

время, системные администраторы не найдут проблему, пока пользователи системы не выйдут на работу после выходных. Он предпочитал вносить изменения во время обеденного перерыва, чтобы их можно было тестировать в течение половины дня, прежде чем уйти домой. В этой компании не было строго определенного времени обеденного перерыва. Буфет был открыт с 11:15 до 13:30, и по крайней мере треть пользователей сети была активна в любое время.

Как у Тома, так и у его пользователя были веские доводы, но ни одно правило не подойдет для любой ситуации. Однако игнорирование рисков других пользователей неприемлемо и довод о том, что достаточно более внимательной проверки, не является убедительным. Более внимательная проверка всегда полезна, но она не является достаточным основанием для того, чтобы игнорировать более высокий риск для пользователей.

Во многих компаниях предпочитают вносить изменения в течение рабочего дня по той же причине, по которой стараются не делать это в пятницу: желательно, чтобы после изменения люди были на месте и смогли заметить и устранить любые проблемы. Однако во многих компаниях для внесения изменений, требующих отключения системы, предпочитают дождаться, чтобы на месте не осталось никого или почти никого.

Вам потребуется выяснить, что правильно в вашем случае. Однако вам следует стараться избегать ситуаций, при которых люди вне организации системных администраторов могут внести изменения, способные негативно повлиять на важные системы.

Разные люди имеют различные взгляды на внесение критических изменений. Более старшие системные администраторы обычно осторожнее младших, поскольку лучше понимают возможное влияние изменений и научены горьким опытом недостаточной осторожности в прошлом. В развитой организации системных администраторов каждый будет знать о документированных, последовательных инструкциях, которые надо соблюдать. Эти инструкции будут включать приемлемое время для внесения определенных типов изменений.

Пытаясь классифицировать обновления как штатные, критические или крупномасштабные, учитывайте, что некоторые изменения могут считаться штатными в одной компании и критическими в другой и даже в различных подразделениях одной компании. Например, в компании электронной коммерции подключение нового узла к корпоративной сети может считаться штатным обновлением, а подключение нового узла к сервисной сети, видимой пользователям, – критическим. Определите, как должны классифицироваться различные виды обновлений в разных областях вашей компании, и создайте методику построения графика, которая отражает ваше решение.

Полезно определить время **запрета на изменения**, когда можно осуществлять только незначительные изменения. Запрет на изменения обычно накладывается в конце квартала и в конце финансового года. На рис. 17.1 изображен пример сообщения о запрете на изменения одной компании, которое было отправлено всем системным администраторам и начальникам отделов.

Тема: К вашему сведению – запрет изменений с 25.09 по 06.10

Уважаемые сотрудники!

Напоминаем вам, что через три недели начнется действие ЗАПРЕТА ИЗМЕНЕНИЙ. Он продлится с 25 сентября по 6 октября. Форма контроля изменения 96739 приведена ниже:

КРАТКОЕ СОДЕРЖАНИЕ	
Класс/очередь уполномоченного лица	ГСНМ
Имя уполномоченного лица	_____
Имя заказчика	ФРЕД/АДДАМС
Имя подавшего заявку	ФРЕД/АДДАМС
Телефон подавшего заявку	(555)555-8765
Класс/очередь подавшего заявку	ГСНМ
Дата/время начала плана	25.09.2000 00:01
Дата/время окончания плана	06.10.2000 24:00
Дата/время подачи	10.04.2000 14:26
Дата/время последнего изменения	22.06.2000 16:02
Дата закрытия	_____
Система	_____
Компонент/приложение	Финансовый отчетный период и запрет изменений
Описание	4Q00/1Q01 Расширение доступности финансовых данных
Изменение системы	_____

ИЗМЕНЕНИЕ: 00096739	
Статус/время изменения	OR/INF
IPL/прерывание обслуживания	N/N
Риск/причина изменения	1/QT
Контроль процедуры	NET/GNS
Проблема исправлена	_____
Подразделение	ВСЕ
Код местоположения	ГЛОБАЛЬНОЕ
COI	ВСЕ
Статус одобрения	ОЖИДАЕТ
Последний изменивший пользователь	NCC0FHA
Связанные документы	N/A

Запрет на изменение процессов обработки финансовых данных, электронной почты и сети для поддержки деятельности по закрытию/открытию квартальных отчетов.

Изменения, которые могут повлиять на доступ к данным, передачу данных между приложениями на серверах или электронную почту, должны быть назначены на другое время. Рассматриваться будут только экстренные изменения для предотвращения или устранения сбоев. Запросы на изменения оформляются в форме на исключительное изменение.

Указания на период запрета изменений и контактную информацию можно найти на странице

http://wwwin.foo.com/gnsc/quiet-time.html

Влияние на пользователей: Нет

План тестирования: Нет

Контактные телефоны и номера пейджеров:

ДЖОН СМИТ	(555)555-1234	
ДЖЕЙН ДЖОНС	(555)555-4321	
ЭЛИС УОЛТЕР	(555)555-7890	800-555-5555 ПИН-код 123456

План отмены: Нет

Рис. 17.1. *Образец сообщения о запрете на изменения*

17.1.4. Процессы и документация

Процессы и документация являются важными элементами управления изменениями. Соблюдение процессов и создание документации заставляет системных администраторов тщательно готовиться к значительным изменениям. Системным администраторам нужно заполнить формы *контроля изменения*, или *предложения изменения*, где подробно описываются изменения, которые они будут вносить, затрагиваемые системы и службы, причины изменения, риски, процедура проверки, план отмены, время реализации изменения и время реализации плана отмены. Иногда системным администраторам требуется перечислить все команды, которые они будут вводить. Необходимый уровень детализации различается в разных компаниях и обычно зависит от того, насколько важна затрагиваемая машина или служба. Для очень важных машин системный администратор не может вводить ничего, что не перечислено в одобренной форме контроля изменения. Однако для менее важных машин требования по соблюдению процессов и документации должны быть менее жесткими, иначе системные администраторы будут ощущать себя связанными ограничениями управления изменениями и не смогут эффективно работать.

Если компания может определить одну или две машины, которые являются критически важными для ведения бизнеса, эти машины должны быть защищены жесткими процессами управления изменениями. Например, в компании электронной коммерции в эту категорию должны входить машины главных баз данных и машины, обрабатывающие данные о кредитных картах. В фармацевтических компаниях строгие требования по управлению изменениями для машин, вовлеченных в процесс разработки лекарств, часто устанавливаются законодательством. Машины в этой категории обычно не являются серверами, которые обеспечивают такие важные службы, как электронная почта, печать, DNS или аутентификация. Машины, которые обеспечивают эти службы, должны быть защищены менее строгими политиками управления изменениями, чтобы найти равновесие между пользой от управления изменениями и от способности системных администраторов быстро ответить на требования пользователей. Однако значительные изменения в этих серверах или службах должны выполняться с соблюдением хорошего процесса управления изменениями, чтобы они проходили плавно, с минимальным количеством неожиданностей.

В последующих главах подробно рассмотрены процессы, связанные с различными типами изменений. В частности, в главе 18 рассмотрена модернизация серверов, в главе 19 – изменение служб, а в главе 20 – технические перерывы.

17.1.5. Технические аспекты

Вам может потребоваться документированная процедура обновления системных файлов конфигурации, которую будет соблюдать каждый системный администратор. Эта процедура должна последовательно применяться везде, где обновляются файлы конфигурации. Она должна быть точно документирована по шагам, включая процедуру, которую нужно соблюдать, если любой из шагов будет неудачным, и должна выдаваться всем системным администраторам при вступлении в группу. Эта процедура должна включать создание историй обновления, блокировку файлов конфигурации, чтобы только один человек мог одновременно их редактировать, запуск автоматизированных проверок формата информации в файлах и, если это допустимо, уведомление других систем или

приложений о том, что произошло обновление. Это принципиально полезный метод, который должен всегда применяться всеми. Он простой и на удивление часто может сэкономить время.

17.1.5.1. История изменений и блокировка

История изменений позволяет любому человеку, обладающему соответствующим доступом, просматривать изменения, внесенные в файл, что очень полезно, если текущая версия становится поврежденной. Обычно в истории изменений также записывается, кто и когда внес изменение, и можно добавлять дополнительный комментарий к изменению. Кроме того, программы контроля версий обычно предоставляют механизм блокировки, который необходимо использовать для предотвращения одновременного изменения одного и того же файла конфигурации двумя людьми.

Прикрепление идентификатора каждого человека к его изменениям полезно. Если младший системный администратор сделает ошибку, то старший сотрудник, который это обнаружит, может позвать этого человека и воспользоваться возможностью немного обучить его в данной области системы.

Для выполнения этих функций вам нужно обратить внимание на системы контроля исходного кода, используемые разработчиками программного обеспечения. Для UNIX такими средствами являются SubVersion, Revision Control System и Source Code Control System (Bolinger 1995), а также Concurrent Versions System (Berliner 1990), которые записывают отличия от версии к версии, идентификаторы пользователя и комментарии, а также обеспечивают блокировку. Примером такой системы под Windows является SourceSafe. Кроме того, есть много коммерческих систем, которые могут уже использоваться разработчиками в конкретных компаниях.

Ведение истории изменений в UNIX

В UNIX легко начать ведение истории изменений файла при помощи Revision Control System (RCS). Начните делать это в следующий раз, когда будете редактировать любой файл, и простая, но полезная история изменений всех ваших важных файлов конфигурации появится у вас прежде, чем вы можете предположить.

Допустим, что нужный файл – это etc/named.conf. Создайте директорию под названием /etc/RCS. Начните ведение истории изменений при помощи команды `ci -l named.conf`. Теперь история изменений файла будет храниться в файле etc/RCS/named.conf.v (обратите внимание на символ .v в конце имени файла). Для редактирования файла запишите его контрольное значение с помощью команды `co -l named.conf`, а затем откорректируйте его в редакторе, с которым вы привыкли работать. Когда необходимые изменения будут внесены, подтвердите изменение командой `ci -u named.conf`. Этот процесс из трех этапов обычно записывается в shell-скрипт под названием `xed` или `vir`. Всегда целесообразно запускать `rcsdiff named.conf` перед запуском `co`.Таким образом, если кто-то внес изменения и забыл воспользоваться RCS, вы увидите это и сможете зафиксировать их в RCS, прежде чем продолжите работу. Для подтверждения

изменений, внесенных кем-либо другим, используйте команду `rcs -l named.conf`, а затем – обычную команду подтверждения изменения `ci -u named.conf`. Дополнительное время, потраченное на то, чтобы убедиться, что вы не уничтожите чьи-то изменения, может сэкономить много нервов и времени отладки в дальнейшем. В RCS есть другие полезные команды: `rlog named.conf` покажет историю изменений файла, а `rcsdiff -r1.1 r1.2` отобразит различия между версиями 1.1 и 1.2. Вы можете увидеть, как выглядела версия 1.2 при помощи такой команды, как `co -p -r1.2 named.conf`.

В хорошем справочнике (например, Bolinger 1995) объясняются более сложные вопросы, в частности отмена изменения. Создайте простой текстовый файл для экспериментов, пока изучаете инструкцию. Вы очень скоро станете экспертом.

История изменений экономит время

В компании среднего размера, занимающейся разработкой программного обеспечения, использовался скрипт, который автоматизировал процесс создания учетных записей. Однажды диск, который содержал базу данных учетных записей, был заполнен, когда программа перезаписывала базу данных. Из-за того что проверка ошибок практически отсутствовала, переполнение диска осталось незамеченным. Скрипт продолжал распространять новую базу данных на все серверы аутентификации, даже несмотря на то, что в ней отсутствовало большинство учетных записей. Системные администраторы быстро поняли, что случилось, и смогли немедленно очистить часть дискового пространства и откатиться к старой версии базы данных учетных записей, существовавшей до запуска скрипта. Если бы у них не было истории изменений, то пришлось бы восстанавливать базу данных с резервной кассеты, что заняло бы гораздо больше времени и означало бы, что все изменения паролей, сделанные пользователями со времени создания резервной копии, были бы потеряны. Автоматизированная программа оставила о себе данные в поле комментария, и таким образом можно было легко узнать человека, ответственного за сокращение базы данных. Впоследствии скрипт был изменен для выполнения большего объема проверок на ошибки.

17.1.5.2. Автоматизированные проверки

Последние этапы обновления файла или набора файлов – проверка того, что каждый файл не содержит синтаксических ошибок, а затем обеспечение того, чтобы все приложения, использующие этот файл, начали использовать новую информацию. Эти этапы должны выполняться автоматизированной программой, которая также обязана сообщать различным серверам, что их файлы конфигурации были изменены, или при необходимости распространять файлы по другим местам.

Иногда вам может потребоваться разделить эти два этапа. Если для того, чтобы приложение начало использовать новую информацию о конфигурации, потребуется небольшое прерывание обслуживания и если обновление может подождать до момента, когда оно вызовет меньшие нарушения работы или не вызовет их совсем, синтаксис нужно проверить немедленно, а процесс обновления перенести на более поздний срок.

Конфигурации некоторых систем трудно проверить автоматизированной программой, и в идеале они должны создаваться программой, чтобы, по крайней мере, не содержать синтаксических ошибок. Создайте какой-нибудь другой способ тестирования этих компонентов, который будет гарантировать вам достаточно высокий уровень уверенности в том, что они работают правильно. Например, под UNIX скрипты загрузки системы часто корректируются вручную, чтобы изменить набор служб, запускаемых во время загрузки, или, возможно, чтобы изменить режим работы сетевых интерфейсов. Важно, чтобы эти скрипты внимательно проверялись, потому что ошибка может не позволить системе завершить цикл перезагрузки. В большинстве коммерческих UNIX-систем загрузочные скрипты разделены на множество небольших элементов, по одному на каждую службу, чтобы каждый из них можно было проверить индивидуально и обеспечить достаточную степень уверенности в том, что изменения и дополнения правильны.

Если скрипты загрузки не проверить заранее, проблемы с ними не будут обнаружены до следующей перезагрузки. Поэтому очень важно обеспечить полную надежность загрузочных скриптов. Машины перезагружаются в самое неудобное время. Сбои систем происходят поздно вечером, во время вашего отпуска и т. д. Если вы только при следующей перезагрузке обнаружите, что скрипт, написанный вами, содержит опечатку, это случится в очень неудобное время. Что еще хуже, хорошие системы могут работать без перезагрузки в течение нескольких месяцев. Очень трудно запомнить, какие изменения были внесены после последней перезагрузки, особенно если она была несколько месяцев назад. Даже если в компании есть политика записи изменений в журнале событий или системе заявок, может быть очень трудно найти нужное изменение, если прошло несколько месяцев.

Проверка путем перезагрузки

До появления распределенных вычислений в большинстве учреждений – иногда в целых корпорациях – был только один большой компьютер, к которому каждый подключался при помощи модема или терминала. Одним из больших компьютеров Тома был VAX 11/750 под операционной системой Digital VMS. Прежде чем молодежь начнет зевать от вида древних технологий 1980-х годов и сразу перейдет к следующему разделу, хотелось бы заметить, что этот урок актуален и сегодня, поэтому прочтите его. Скрипт, выполнявший загрузку, изменялся очень редко. У системных администраторов было правило, что если вы изменили загрузочный скрипт, то должны были в ближайшее время перезагрузить VAX.

Обычно они перезагружали машину раз в месяц во время автономной процедуры резервного копирования. Сначала они перезагружали VAX, чтобы убедиться, что он мог загрузиться сам. Теоретически этот этап не

был необходимым. Затем они вносили необходимые изменения в системные файлы. Еще одна перезагрузка должна была проверить изменения, все обнаруженные ошибки исправлялись и также тестировались с помощью перезагрузки. После этого системные администраторы делали перезагрузку, которая требовалась для процедуры резервного копирования на магнитную ленту. Преимуществом этого метода было то, что ошибки обнаруживались сразу же после их появления, когда системный администратор еще помнил изменения. С развитием распределенных вычислений перезагрузка перестала быть таким значительным явлением. Кроме того, теперь машины перезагружаются быстрее. Однако в наше время перезагрузка машины или какое-нибудь точное тестирование изменений в таком критичном коде еще более важны. Раньше опечатка могла означать, что VAX не будет работать до утра, пока системные администраторы не придут и не исправят ошибку. В современном мире при отключении компьютера останавливается бизнес и такой сбой приведет к тому, что вас, системного администратора, разбудят посреди ночи или вызовут из отпуска, чтобы устранить проблему *прямо сейчас*. Дополнительная перезагрузка – это стратегическое вложение в ваше спокойствие!

Если ваши пользователи предупреждены о том, что конкретный узел будет недоступен в определенное время, используйте эту возможность для дополнительной перезагрузки, когда работа будет закончена.

17.2. Тонкости

Как только у вас будет базовая структура управления изменениями, которая описывает процесс обновления конфигурации, используемые методы распространения информации и составление графика изменений, вы сможете воспользоваться некоторыми другими методами управления изменениями для повышения стабильности вашей компании. В частности, вы можете создать автоматизированные интерфейсы для распространенных изменений конфигурации, которые осуществляют всю блокировку, ведение истории изменений, проверку и обновление за системных администраторов. Вам также нужно устраивать формальные собрания по управлению изменениями с многосторонними консультациями, чтобы рассматривать предложения об изменениях.

17.2.1. Автоматизированные интерфейсы

Автоматическая проверка системных файлов на ошибки формата и синтаксиса перед утверждением изменения обеспечивает для ваших систем более серьезную стабильность. Следующий шаг по этому пути – создать для этих системных файлов оконечный интерфейс, который задает соответствующие вопросы, проверяет ответы на ошибки, ищет пропуски и затем правильно обновляет файл, используя предоставленную информацию. Если каждый станет пользоваться этим интерфейсом, будет только одно место, требующее проверки ошибок.

17.2.2. Собрания по вопросам управления изменениями

Официально одобренные собрания по вопросам управления изменениями для рассмотрения, обсуждения и составления графика предлагаемых изменений являются ценным средством повышения стабильности систем. Это формальный процесс отчета системных администраторов, что и когда они планируют делать, сколько времени это займет, что может не получиться, как это будет проверяться, как отменить изменение и сколько времени займет отмена. Он заставляет системных администраторов думать о последствиях того, что они делают, а также приготовиться к возможным проблемам.

Он также предупреждает об изменениях других людей, чтобы они могли быть в курсе потенциального источника проблем. В число людей, которые одобряют, отклоняют или переносят предлагаемые изменения, должны входить сотрудники из всех подразделений компании, чтобы представители каждой области, которая может быть затронута, могли предупредить свои группы и подготовить их к грядущим изменениям. Участники таких собраний называются **заинтересованными лицами**.

Эти собрания предоставляют заинтересованным лицам общий обзор того, что происходит в компании. Они обеспечивают старшим системным администраторам и руководителям возможность заметить изменение, которое вызовет проблемы, до того, как оно будет внесено, и не позволить этому случиться. Они снижают неупорядоченность и обеспечивают более стабильную среду. Обычно собрания по управлению изменениями проходят раз в неделю или раз в месяц в соответствии с частотой изменений в компании.

Одобрение каждого изменения всеми заинтересованными лицами не только повышает стабильность системы, но и предоставляет системным администратором своего рода «прикрытие». Мы не считаем, что это цинично. Если группы пользователей постоянно жалуются на то, что процесс выходит из-под контроля и сбои происходят в неудобное время, хорошим решением является проведение консультации по пересмотру изменения, чтобы вовлечь в это самих пользователей и получить их одобрение на изменения.

Пример: ежедневные собрания по управлению изменениями

В популярной компании электронной коммерции, которая обрабатывает большие, все время растущие объемы трафика, сервисная сеть постоянно модернизируется, чтобы справляться с растущим спросом. Необычный процесс управления изменениями в этой компании включает ежедневные собрания по управлению изменениями. Предложения об изменениях вносятся каждый день перед окончанием работы. В собраниях участвуют системные администраторы, предлагающие изменения, все руководители системных администраторов и некоторые представители из инженерной и эксплуатационной групп. Предложения об изменениях обсуждаются, одобряются, откладываются или отклоняются с поиском альтернативного решения. Каждое предложение включает предполагаемую

дату и время внесения изменения. Если оно одобряется, изменение должно быть внесено в утвержденное время, иначе его нужно обсудить на другом собрании по управлению изменениями.

Услуги компании в основном используются на потребительском рынке в США. Из-за того что компания располагается на западном побережье США, время наибольшей нагрузки – после 14 ч с понедельника по пятницу, то есть после 17 ч на восточном побережье США, и все дневное время в выходные. Время, указанное в предложении изменения, – это обычно следующее утро, до пиковой нагрузки. Другое решение, которое принимается на собрании по управлению изменениями, – должно ли изменение вноситься вне зависимости от «погоды» или нужно дождаться «хорошей погоды»: рабочего состояния обслуживания. Другими словами, некоторые изменения утверждаются при условии, что в момент, когда системный администратор или инженер хочет внести изменение, услуга будет работать нормально. Другие изменения считаются настолько важными, что они вносятся вне зависимости от того, насколько хорошо или плохо работает услуга.

Данный подход является необычным по ряду причин. Естественно, он лучше, чем отсутствие управления изменениями, потому что имеется по крайней мере минимальный процесс рассмотрения, определенное время вне интервала наибольшей нагрузки, в которое осуществляются изменения, и процесс переноса некоторых из них во избежание возможных проблем при нестабильности системы. Однако частота собраний и внесения изменений в сервисную сеть означает, что сложно оценить целостную картину происходящего с сетью, постоянно вносятся беспорядок и небольшие неоднородности, которые могут взаимно влиять друг на друга, а системные администраторы и инженеры не имеют стимула планировать заранее. Изменения могут вноситься быстро, без тщательного продумывания. Также необычно, что изменения разрешаются в случае нестабильной работы сервисной сети, которая обеспечивает доходы компании. Изменения в такое время могут существенно затруднить решение существующих проблем, особенно если устранение нестабильности требует нескольких дней. Однако формальный процесс сообщения группе операторов об изменении до его выполнения и предоставления им возможности предотвратить по крайней мере некоторые изменения является ценным.

Несмотря на то что компании часто удавалось успешно обрабатывать большие объемы транзакций, некоторое время она была подвержена проблемам со стабильностью и большим, дорогостоящим сбоям, источник которых было трудно отследить из-за быстро меняющейся структуры сети. Было невозможно построить ось времени и сказать: «Проблемы начались после этих изменений, которые были утверждены на этом собрании по управлению изменениям». Это позволило бы сократить область поиска и, возможно, быстрее найти проблему.

Развитый процесс управления изменениями также может приобрести черты управления проектами, при этом предлагаемое изменение будет внимательно изучаться в плане влияния не только на другие системы, но и на сроки выполнения других задач группы. Если внесение изменения вызовет задержку выполнения других, более важных проектов, оно будет отклонено.

Пример: IBM на Олимпиаде в Нагано

IBM строила и эксплуатировала компьютерную инфраструктуру поддержки летних Олимпийских игр 1996 года в Атланте и зимних Олимпийских игр 1998 года в Нагано. На Играх в Атланте в 1996 году у IBM не было процесса управления изменениями и многие изменения вносились программистами, которые не знали о влиянии этих «небольших» изменений на всю остальную систему. Некоторые системы были завершены в последний момент, и времени на их тестирование не было. Другие все еще разрабатывались после начала Игр. Было много проблем, каждая из которых массово освещалась прессой, что создавало определенные сложности для IBM. Сбои препятствовали получению информации о спортивных событиях и оставляли прессе мало тем для репортажей, кроме посвященных нестабильной работе компьютерной системе IBM. В плане общественного мнения это был кошмар для IBM.

Был проведен анализ изначальных причин, чтобы эти проблемы не повторились на зимней Олимпиаде 1998 года. Было определено, что требовалось лучшее управление изменениями. Для рассмотрения предложений изменений IBM создала комитеты по управлению изменениями, в каждом из которых было до десяти представителей из различных областей проекта. Благодаря этому механизму IBM успешно удалось предотвратить реализацию нескольких «небольших» изменений и все оборудование и программное обеспечение было успешно установлено и полностью проверено до начала соревнований, а многие проблемы были обнаружены и устранены заблаговременно. Окончательным результатом был благополучный запуск информационной системы зимней Олимпиады 1998 года с ее началом (Guth and Radosevich 1998).

Пример: управление изменениями обеспечивает успех массовых мероприятий

На первом концерте NetAid в 1999 году у Cisco было примерно 4 недели на построение и запуск распределенной сети, которая должна была обрабатывать 125 тыс. одновременных потоков видеоданных 50 интернет-провайдеров. Cisco пришлось разрабатывать механизмы, которые распространялись на весь мир. В конце концов у Cisco оказалось около 1000 единиц оборудования, которыми нужно было управлять и время от времени изменять их. Компания сделала это силами пяти штатных сотрудников и большого количества добровольцев.

Никто не расширял свои системы до размера, который был необходим Cisco. Поэтому персонал знал, что проблемы функционирования потребуют изменения конфигурации маршрутизаторов и серверов. Из-за большого количества людей и неустойчивой среды персоналу было важно поддерживать управление конфигурацией, особенно потому, что причины определенных конфигураций маршрутизации не были интуитивно очевидны – например, почему Пол ввел именно этот фильтр маршрутов? Кроме того, персонал использовал систему обнаружения втор-

жений для защиты своего сайта электронной коммерции. Каждый раз при настройке такой системы должна осуществляться ее привязка к среде, в которой она будет работать, и обычно этот процесс занимает 4 недели. Было важно отслеживать все изменения, чтобы причины установки таких фильтров были известны. Процесс управления изменениями предоставлял документацию, которая позволяла каждому работающему над системой понимать, что было сделано раньше, почему это было сделано и как эти изменения согласуются с работой других людей. Без этой документации было бы невозможно вовремя обеспечить правильную работу системы. Все подобные процессы внесли свой вклад в успех проекта.

17.2.3. Упрощение процесса

В конце концов, когда вы посчитаете, что все на месте, вам стоит оценить свой процесс с точки зрения возможности упростить его. Есть ли неиспользуемые вопросы в вашей форме предложения изменения? Можно ли более эффективно выполнять элементы процесса, связанные с бумажной работой? Если формы сетевые, есть ли возможность сохранения каждым пользователем значений по умолчанию в некоторых полях, например имени и контактной информации? Какие проблемы есть у людей, использующих систему в ее нынешнем состоянии?

17.3. Заключение

Управление изменениями – это ценное средство, которое используется в развитых учреждениях для повышения надежности системы за счет как ограничения на внесение определенных изменений, так и наличия процесса заблаговременного рассмотрения изменений, позволяющего выявить любое негативное влияние, которое мог упустить системный администратор, или взаимодействие, о котором он мог не знать. Кроме того, управление изменениями помогает с устранением проблем, потому что изменения отслеживаются и в случае появления проблем могут быть пересмотрены.

Частота, с которой нужно устраивать собрания по управлению изменениями, зависит от их охвата и частоты изменений среды, которую они затрагивают. Создание механизма, при помощи которого системные администраторы могут проверить, работает ли система нормально, прежде чем вносить свои изменения, снижает риск того, что изменение, внесенное в процессе устранения существующей проблемы, усложнит процесс отладки или сделает систему даже менее стабильной.

Задания

1. Опишите процесс управления изменениями в вашей организации.
2. Какие временные интервалы вы определили бы как интервалы наименьшей нагрузки вашей системы?
3. Рассмотрите типы задач, которые вы выполняете по работе, и классифицируйте их как штатные, критические или крупномасштабные обновления.

4. Какой тип процесса распространения информации лучше всего работал бы в вашей компании? Были бы у вас как механизмы «толкания», так и механизмы «вытягивания»? Почему? Для чего вы пользовались бы каждым из них?
5. Как бы вы организовали собрания по управлению изменениями в своей компании? Кто, по-вашему, должен в них участвовать? С какой частотой вы их проводили бы?
6. В какой мере управление изменениями влияет на методы вашей работы?
7. Оцените, как различные виды обновлений должны классифицироваться в разных областях вашей системы, и создайте метод составления графика, отражающий ваше решение.
8. Какие проблемы есть у людей, использующих систему в ее нынешнем состоянии?
9. Назовите сторону, которую вы поддерживаете в примере из раздела 17.1.3 о внесении серьезных изменений в пятницу или перед отпуском, и обоснуйте свое решение.

Глава 18

Обновления серверов

Данная глава имеет очень специфичную тему: обновление операционной системы отдельного узла. Эта задача, хотя и выглядит обманчиво простой, на самом деле требует большого объема предварительной подготовки и последующего тестирования. Само по себе обновление может осуществляться различными способами. Чем более критичен узел, тем важнее правильность выполнения обновления. Этот метод является строительным блоком. После его детального изучения вы можете перейти к более крупным проектам по обновлению, рассмотренным в главе 20.

Для успешного выполнения этой задачи требуется единственное средство, вне зависимости от типа операционной системы. Это средство – лист бумаги, который будет использоваться для создания контрольного списка. Использование этого средства обязательно.

Некоторые люди предпочитают имитировать лист бумаги при помощи веб-страницы, википедии или электронной таблицы. Такие высокотехнологичные решения имеют преимущества, которые будут рассмотрены позднее. Однако принцип один: обновлять сервер без контрольного списка недопустимо. Возьмите карандаш, давайте начнем.

18.1. Основы

Принципиальная задача любого обновления ОС состоит в том, чтобы как минимум все службы, которые предоставлялись *до* обновления, работали *после* обновления. Обновление может проводиться для того, чтобы *расширить* функциональность или надежность, но оно не должно их снижать. Учитывая это, процесс имеет следующую структуру.

1. Составьте контрольный список служб:
    a. Какие службы предоставлялись сервером?
    b. Кто является пользователем каждой службы?
    c. Какие программы предоставляли каждую службу?
2. Проверьте, чтобы каждая программа работала с новой ОС, или запланируйте путь обновления программного обеспечения.
3. Для каждой службы разработайте тест на проверку работоспособности.
4. Напишите план отмены с конкретными условиями.

5. Выберите технический перерыв.
6. Объявите об обновлении в необходимом порядке.
7. Выполните ранее разработанные тесты, чтобы убедиться, что они действенны.
8. Заблокируйте пользователей.
9. Проведите обновление с наблюдением/помощью (или под руководством) другого человека.
10. Повторите все ранее разработанные тесты. Соблюдайте стандартный процесс отладки.
11. Если тесты будут неудачными или произойдут другие события, которые являются условиями для выполнения плана отмены, выполните план отмены.
12. Разблокируйте пользователей.
13. Сообщите пользователям о завершении/отмене обновления.
14. Проанализируйте, что прошло правильно, а что нет, измените контрольный список в соответствии с приобретенным опытом.

А вы думали, что нужно всего лишь воспользоваться установочным диском, не так ли? Давайте более подробно рассмотрим каждый этап.

18.1.1. Этап 1: составьте контрольный список служб

Контрольный список служб – это средство, которым вы будете пользоваться для проведения всей процедуры. Список должен отражать, *какие* службы предоставляются узлом, *кто* пользуется каждой службой и *какая* программа предоставляет каждую службу.

Электронные таблицы – отличный способ представления такой информации. Самым большим преимуществом представления этой информации в электронном виде является то, что ее смогут легко совместно использовать персонал и пользователи. Лучше предоставить доступ к файлу через Интернет, чем отправлять его каждому человеку, потому что версию в Сети можно быстро обновить. Люди всегда будут видеть самые последние обновления[1]. Однако Сеть предполагает наличие механизмов активной доставки. Люди не будут искать файл сами. Вы можете включать URL в каждое электронное письмо, касающееся проекта, но это не даст гарантии, что его прочтут. Правильная идея – объявлять о любых значительных обновлениях.

Дважды проверьте свои планы, устройте собрание ключевых представителей затрагиваемого сообщества. Покажите им план, шаг за шагом, попросите их проверить ваши предположения. Наиболее эффективно начать процесс с собрания, а затем пользоваться для обновления электронной почтой, устраивая другие личные встречи, возможно, только в ключевые моменты процесса.

---

[1] Явно укажите в контрольном списке номер версии и дату, чтобы каждый мог легко проверить, является ли его версия последней.

Проверка зависимости пользователей

Один системный администратор устроил собрание десяти опытных системных администраторов, каждый из которых ознакомился с планом и сразу подтвердил, что он не возражает. Когда системный администратор начал разбирать его поэтапно, задавая конкретные вопросы, например: «Что будет, если мы это выключим?», они начали говорить: «Ой, нет, если вы это сделаете, биллинговая система не будет работать. Я думаю, нам нужно добавить этап, на котором мы перенесем биллинговую информацию». В результате получился совершенно другой план, в котором было в три раза больше этапов. Если бы не было личной встречи системных администраторов, на которой был рассмотрен каждый этап в отдельности, первоначальный план вызвал бы масштабную катастрофу.

Включение пользователей в процессы принятия решений и планирования дает им ощущение контроля и участия. Пользователи вкладываются в результат и становятся частью команды, что обычно ведет к более позитивным впечатлениям и лучшим отношениям между системными администраторами и подразделениями бизнеса. Совместный с пользователями доступ к информации о зависимости и состоянии через Сеть и по электронной почте позволяет поддерживать рабочие связи.

Машина может быть выделена для предоставления одной службы или предоставлять много служб. В любом случае предоставление службы в целом может обеспечиваться несколькими программами.

Что находится на машине?

Иногда вы точно знаете, для чего используется машина, и первоначальный контрольный список обновления создать легко. Однако со временем на машину добавляются дополнительные службы, функции и программы (Evard 1997). Мы можем дополнительно проконтролировать себя, если проверим сам узел. Вы можете просмотреть программы, установленные под UNIX, в директориях /opt, /usr/local и других местах, общих для таких систем. Операционные системы Майкрософт обычно размещают программы в папке под названием Program Files, хотя некоторые используют собственные правила, например устанавливают по умолчанию папку C:\apps. Вы можете посмотреть, какие процессы запущены в системе. UNIX- и NT-системы выводят все прослушиваемые порты TCP/IP и UDP/IP по команде `netstat -an`. В UNIX есть различные загрузочные скрипты, которые можно проанализировать. В NT есть консоль Службы. В UNIX есть файлы crontab, которые можно просмотреть. В каждой ОС есть по крайней мере один способ перечислить все установленные программы. Некоторые примеры таких средств — это `pkginfo` (Solaris и SVR4), `swlist` (HP-UX 10 и выше) и `'rpmqa'` (Linux).

Обычно каждая служба напрямую связана с одной программой. Иногда служба связана с несколькими программами, например сервер календаря, который использует сервер LDAP. Зафиксируйте все такие взаимозависимости в контрольном списке.

Кроме того, важно определить ключевых пользователей различных служб. Пользователи могут обращаться к службе напрямую или косвенно, взаимодействуя со службами, которые используют другие службы для получения или ввода данных. Людей нужно привлечь к процессу или, по крайней мере, уведомить о том, что происходит обновление. Если от служб зависят другие машины, надо включить в процесс пользователей этих машин.

Часто вы будете находить службы без прямых или косвенных пользователей, и такие службы можно отключить. Это всегда приятно, но будьте осторожны: вы можете найти зависимость тогда, когда службы уже не будет. Оставьте службу в готовом к запуску, но приостановленном состоянии, чтобы при необходимости ее можно было восстановить. Убедитесь, что вы отметили, почему служба существует, но не работает, чтобы в следующий раз ее можно было удалить, если к тому времени она не будет вновь включена. Лучшее место для такой документации – один из файлов конфигурации, который будет редактироваться при возобновлении служб.

18.1.2. Этап 2: проверьте совместимость программ

Следующий этап – убедиться, что каждая программа сможет работать с новой ОС, и запланировать способ обновления для тех программ, которые не будут работать. Используя список, созданный ранее, свяжитесь с разработчиками и узнайте, будет ли работать версия программы после обновления. Часто разработчики предоставляют такую информацию на своих веб-сайтах.

Вы можете захотеть сами проверить достоверность информации или найти другого пользователя, который уже сделал обновление. Представления разработчиков о том, что значит «версия будет работать», часто не включают функции, которые нужны в вашей компании, или точную конфигурацию, которую вы определите. Самостоятельное тестирование может быть дорогим, но, скорее всего, оно окажется дешевле, чем неудачное обновление, и при этом снижается риск неудачи. Целесообразность определяется из соображений управления риском. Если обновляется только одна система и приложение не является критически важным, его персональная проверка может быть пустой тратой времени. Если обновление автоматизировано и будет повторяться тысячи раз и потенциальная ошибка будет сильно заметна, тестирование необходимо.

Если используемая версия программы будет работать с новой версией ОС, зафиксируйте, где вы нашли эту информацию, для справки в будущем. Если программа не поддерживается новой ОС, у вас есть несколько вариантов.

- *Обновление до версии, которая поддерживается обеими ОС*. Если вам повезет, то программу можно обновить до версии, которая работает как в нынешней, так и в будущей системе. Если это возможно, запланируйте обновление до этой версии до обновления ОС. Здесь могут быть полезны тесты, разработанные на этапе 3.
- *Обновление возможно, но работает только в новой ОС*. В данном случае вы должны запланировать обновление программы после завершения обновле-

ния ОС. В зависимости от требований пользователей, это обновление либо может быть элементом обновления ОС, либо можно договориться о перерыве в работе службы, если пользователям не нужен непрерывный доступ. Например, если узел – загруженный веб-сервер, пользователи могут потребовать немедленной установки нового программного обеспечения, потому что это основная функция узла. Однако, если требуется обновить редко используемый компилятор, пользователи могут просто попросить, чтобы он был обновлен на следующей неделе или перед завершением определенного цикла разработки. Это особенно справедливо, если пока для компиляции можно пользоваться другим узлом.

- *Продукт больше не поддерживается*. Иногда мы только при обновлении операционной системы узнаем, что продукт больше не поддерживается разработчиком. Это может заблокировать обновление, либо пользователи могут пожелать сменить поставщиков или отказаться от этого продукта.

18.1.3. Этап 3: тесты для проверки

После того как будет определена каждая служба, нужно разработать тесты, которые будут использоваться для проверки того, что служба правильно работает после обновления. Лучший сценарий – записать все тесты в виде скриптов, которые могут быть запущены автоматически. Можно создать общий скрипт, который выводит сообщение «OK» или «FAIL» (Неудачное завершение) для каждого теста. Затем можно запускать тесты отдельно по мере устранения конкретных проблем. Для более сложных служб пользователи могут писать тесты или, по крайней мере, просматривать их либо предложить, чтобы их вызвали для выполнения вручную их собственных тестов. Некоторые программы имеют средства тестирования установки, которые могут быть запущены для проверки. Иногда эти средства проверки недоступны пользователям, но их можно получить через представителя разработчика.

Процедуры проверки программ

Все программные пакеты должны иметь процедуры проверки, но так редко бывает на самом деле. Иногда такую процедуру лучше написать самому. Тесты могут простыми, такими как проверка компилятора при помощи компиляции программы `Hello, World`. Один тест гораздо лучше, чем их полное отсутствие.

Иногда процедура проверки предоставляется, но на самом деле не работает. Один из поставщиков суперкомпьютеров был известен наличием плохих проверочных баз данных, особенно в бета-версиях ОС.

В обществе программистов для описания определенного способа проверки используется термин **регрессивное тестирование**. Вы сохраняете выходные данные старой системы, вносите изменение, а затем сохраняете выходные данные новой системы. Результаты должны точно соответствовать. Если ожидается, что новый результат будет немного отличаться, вы можете отредактировать базовый вариант вручную, чтобы он отражал ожидаемые изменения, либо воспользоваться алгоритмом *нечеткого соответствия*. Для сравнения результатов можно

воспользоваться простыми средствами. Например, UNIX-программа `diff` – это очень полезное средство, которое сравнивает два текстовых файла и указывает на различия между ними[1]. Программа `diff` имеет ограниченные возможности по оценке нечеткого соответствия, опция `-w` делает одинаковым все незаполненное пространство. Более сложные средства регрессивного тестирования могут программироваться на игнорирование конкретных изменений, обычно основанных на системе стандартных выражений. Однако такая сложность необязательна. Вы можете вручную изменить старый результат – сначала сделайте резервную копию! – чтобы отразить отличия, ожидаемые в новом результате. Например, вы можете изменять номера версий, чтобы они соответствовали новым программам. Прекрасные примеры регрессивного тестирования приведены в книге Кернигана и Пайка *«The Practice of Programming»* (Kernighan and Pike 1999), как и процедура установки `perl` (посмотрите, как реализованы тесты `make tests`).

Иногда тесты могут быть простыми, как при компиляции и запуске программы `Hello, world!` для проверки работы компилятора. Это может быть определенная последовательность команд или щелчков мышью, после которой можно посмотреть, отображается ли ожидаемый результат. Однако будьте внимательны, чтобы такие тесты не оказались поверхностными.

Hello, World!

Однажды Том отвечал за поддержку большого количества компиляторов для нескольких операционных систем. Он создал библиотеку простых программ, большинство из них только выводило `Hello, World!` и завершалось. Он всегда мог проверить, что новый установленный компилятор был, по крайней мере, принципиально правильным, если компилировались и запускались соответствующие программы. При добавлении новых языков программирования Том часто просил программистов написать тестовую программу. Программистам нравилось, что их просят помочь!

Вы должны проверять тесты так же подробно, как любую другую службу. Вы ведь не захотите, чтобы при запуске тестов были какие-то сомнения в том, закончился ли тест неудачно из-за обновления или из-за ошибки в самом тесте.

Заманчиво выполнить эти тесты вручную. Однако помните, что каждый тест будет выполнен как минимум три раза и даже больше, если возникнут проблемы. В этом преимущество автоматизации тестов. Если тесты достаточно общие, ими можно будет снова воспользоваться при дальнейших обновлениях. В конце концов, ими можно пользоваться регулярно просто для устранения проблем или в качестве средств мониторинга для обнаружения сбоев прежде, чем их обнаружат ваши пользователи.

Автоматизированные тесты хорошо подходят для программ, которые выводят предсказуемые текстовые данные, но их гораздо сложнее использовать для графических программ, сетевых служб, например NFS, или для таких физиче-

[1] Несмотря на то что `diff` впервые появилась в UNIX, есть порты практически на каждую существующую ОС.

ских действий, как печать. В случае с NFS вы можете попытаться осуществить доступ к файлу, а не проверять сам протокол. Тестирование сетевых служб, имеющих простые текстовые протоколы, таких как электронная почта (SMTP, POP, IMAP) или веб-службы (HTTP), может быть автоматизировано при помощи простых скриптов, использующих средства типа `netcat` для отправки и получения текста протокола на соответствующий сетевой порт.

Для других программ и служб вы можете найти специализированные тестовые системы, но они обычно очень дорогие. В таких случаях вам придется тестировать их вручную, документируя несколько ключевых функций для проверки или последовательность операций для выполнения. Рано или поздно каждый оказывается в такой ситуации, и все мы должны жаловаться разработчикам, пока они не обеспечат возможность автоматизированного тестирования своих продуктов.

Несмотря на то что автоматизировать все тесты предпочтительно, это не всегда возможно. Некоторые тесты слишком трудно автоматизировать, либо они требуют физического наблюдения. Даже если вы автоматизировали все тесты, то, если вам покажется, что требуется дополнительное тестирование вручную, выполните его. Иногда человеческий глаз видит то, что не может обнаружить лучшая автоматизация.

Разработка через тестирование

TDD (Test-Driven Development) – это относительно новая тенденция в отрасли. Раньше разработчики писали код, а затем создавали тесты, чтобы его проверить (ну, на самом деле это было не так, редко у кого-то было время создавать тесты). TDD – это обратный процесс. Сначала пишутся тесты, а затем – код. Это обеспечивает создание тестов для всего нового кода. Так как тесты выполняются автоматически, вы строите структуру тестов, которая сохраняется с проектом. По мере развития кода снижается риск того, что изменение нарушит функциональность и это не будет замечено. Разработчики свободно могут переписывать, или *перестраивать*, большие либо маленькие элементы кода, зная, что, если они что-то нарушат, это будет сразу замечено. В результате программы содержат меньше ошибок.

Тесты лучше комментариев в коде (документации), потому что комментарии часто устаревают и никто этого не замечает. Тесты, которые охватывают все граничные условия, гораздо более подробны, чем любая документация. Тесты не устаревают, потому что они могут быть включены как элемент процесса разработки, чтобы предупреждать разработчиков об ошибках, которые те внесли в код.

Нам бы хотелось, чтобы и в области системного администрирования изучали TDD и применяли такие методы.

Сохранение тестов для дальнейшего использования

Владелец крупного бизнеса хотел проверить 400 UNIX-серверов сразу после полуночи 1 января 2000 года, чтобы убедиться в том, что основные функции операционной системы и связанная с ними инфраструктура

работают правильно. Был создан ряд бесконтактных тестов, каждый выводил ответ PASS/FAIL: работает ли система, можем ли мы войти в систему, может ли она видеть NIS-серверы, правильно ли время, может ли система разрешать DNS, может ли она подключаться к NFS-серверам и читать файлы, работает ли автоматическое подключение разделов и т. д. При помощи центральной системы администрирования тесты могли одновременно запускаться на нескольких системах, а результаты – централизованно собираться. Все 400 серверов были проверены в течение 20 мин, и персонал смог сообщить о прохождении тестов группе отслеживания проблемы Y2K раньше других, меньших по размеру подразделений. Тесты приобрели такую популярность в группе системных администраторов, что стали элементом ежедневного мониторинга среды.

Тестам нашлось другое применение. Скрытая ошибка в автоматическом подключении разделов в Solaris 2.5.1 и 2.6 могла проявиться после серьезного сбоя сети, но лишь на нескольких случайных машинах. Запуск этого средства тестирования определял затронутые машины после любого сбоя.

18.1.4. Этап 4: напишите план отмены

Как вы вернетесь к предыдущему состоянию, если в ходе обновления что-то идет не так? Как вы сможете «отменить» его? Сколько времени это займет? Очевидно, мелкую неполадку можно попытаться исправить при помощи обычного процесса отладки. Однако вы можете потратить весь технологический перерыв – время, выделенное на отключение системы, – пытаясь сделать что-нибудь, чтобы обновление заработало. Поэтому важно иметь конкретное время, в которое будет задействован план отмены. Возьмите согласованное время окончания и вычтите время, которое потребуется на отмену, а также время, которое потребуется для проверки того, что отмена завершена. Когда вы исчерпаете это время, вы должны либо признать обновление успешным, либо начать свой план отмены. Полезно, чтобы за временем следил кто-то, не входящий в группу, непосредственно выполняющую обновление, например руководитель. План отмены также может быть задействован в случае неудачного выполнения одного или более ключевых тестов либо непредвиденных ситуаций, связанных с обновлением.

В малых или средних системах перед началом обновления можно создать полную резервную копию. Может быть, даже проще сделать точные копии дисков и выполнять обновление на копиях. В случае серьезных проблем можно вновь установить первоначальные диски. Крупные системы гораздо сложнее воспроизвести. В данном случае может быть достаточно создать копии системных дисков и постоянно делать резервные копии.

Обновление копии

Вопрос: Если вы собираетесь сделать точную копию жесткого диска перед обновлением сервера, где нужно выполнять обновление – на копии или на оригинале?

Ответ: Обновляйте копию. Если обновление пройдет неудачно, то вряд ли вам будет приятно обнаружить, что копия была сделана неправильно. Вы просто уничтожите оригинал. Мы видели это много раз.

Точное копирование дисков легко выполнить неправильно. Иногда данные копируются, а с загрузочным сектором возникает проблема и диск не загружается, иногда данные копируются не полностью либо не копируются совсем.

Чтобы избежать такой ситуации, загрузитесь с копии. Убедитесь, что копия работает. Затем выполните обновление на копии.

18.1.5. Этап 5: выберите технический перерыв

Следующий этап – это проверка ваших технических и нетехнических навыков. Вы должны согласовать со своими пользователями технический перерыв, то есть время, когда будет проходить обновление. Для этого вы должны знать, сколько времени займет процесс, и иметь план на случай неудачного обновления. Это больше касается технических вопросов.

- *Когда?* В ваше SLA должны быть включены положения о том, когда можно осуществлять техническое обслуживание. Обычно пользователи хорошо представляют, когда отключение пройдет для них безболезненно. Большинство систем бизнеса не нужны ночью или в выходные. Однако системные администраторы могут не захотеть работать в это время, а в определенное время может быть недоступна поддержка разработчиков. Нужно найти компромисс. Системы, которые должны работать в режиме 24/7, имеют предусмотренный режимом план обслуживания, возможно, содержащий резервные системы.
- *Сколько времени?* Продолжительность технического перерыва равна времени, которое потребуется на обновление, сложенному с интервалами времени, необходимого для устранения проблем, для выполнения плана отмены и для проверки того, что отмена сработала. Изначально лучше умножить ваши оценки на два или на три, чтобы не переоценить свои возможности. Со временем ваши оценки станут более точными.

  Вне зависимости от того, какую продолжительность вы подсчитали, объявите, что перерыв будет гораздо дольше. Иногда вы можете начать работу позже. Иногда она может потребовать больше времени, чем вы предполагали, по техническим (оборудование, программы или несвязанные либо непредвиденные события) или нетехническим (погода либо автомобильные пробки) причинам. Обратная сторона объявления большего перерыва заключается в том, что, если вы раньше закончите обновление и проверку, вам всегда следует сообщать об этом пользователям.
- *Когда нужно задействовать план отмены?* Хорошая идея – в явном виде указать точное время, в которое будет задействован план отмены, в силу причин, рассмотренных на этапе 4.

Скотти всегда преувеличивает

В серии «Relics» сериала *Star Trek: Next Generation* Джеймс Дуэн (James Doohan) появляется в эпизодах в роли Скотти (Scotty) из оригинального сериала. Одной из интересных находок Скотти было то, что он всегда преувеличивал, когда сообщал свои предположения капитану Джеймсу Т. Керку (Captain James T. Kirk). Таким образом, он всегда выглядел чудесным работником, когда проблемы решались быстрее, чем предполагалось. Теперь мы знаем, почему гиперпространственный привод всегда начинал работать раньше, чем предполагалось, а системы жизнеобеспечения функционировали дольше, чем прогнозировалось. Поступайте, как советует Скотти! Преувеличивайте свои оценки! Но не забывайте соблюдать другой принцип Скотти – сразу же сообщать людям, когда работа будет проверена и завершена.

Пример: карт-бланш в понедельник вечером

Когда Том работал в отделении Mentor Graphics, у системных администраторов была такая роскошь, как еженедельный технический перерыв. Вечер понедельника был карт-бланшем системных администраторов. Ожидалось, что пользователи выйдут из системы к 18 часам и системные администраторы смогут использовать этот вечер для выполнения любых видов серьезных обновлений, которые потребуют отключения служб. Каждый понедельник в 16 часов пользователям сообщали о том, какие изменения произойдут и когда системами снова можно будет пользоваться. В конце концов, пользователи выработали привычку планировать на вечер понедельника дела, не связанные с работой. Ходили слухи, что некоторые из них проводили время со своими семьями.

Несмотря на то что для одобрения такой практики руководством требовались серьезные политические вложения, она была важным фактором обеспечения высокой надежности сети отделения. Редко были причины отменять своевременные обновления системы. О проблемах в течение недели можно было позаботиться при помощи временных мер, но долгосрочные меры эффективно принимались вечером в понедельник. В отличие от некоторых организаций, где долгосрочные меры не принимались никогда, в данном случае они выполнялись относительно быстро.

Когда работы было немного, один администратор настаивал на перезагрузке некоторых критически важных серверов в 18 часов, чтобы «подтолкнуть» пользователей пойти вечером домой. Он верил, что это помогало пользователям поддерживать привычку не планировать ничего критически важного на вечер понедельника. Конечно, системные администраторы придерживались гибкого подхода. Когда приближался срок сдачи важного проекта и сотрудники работали круглосуточно, системные администраторы отменяли технический перерыв вечером в понедельник или согласовывали с пользователями, что можно отключить, не мешая их работе.

18.1.6. Этап 6: сообщите об обновлении в соответствии с установленным порядком

Теперь сообщите об обновлении пользователям. Используйте одинаковый формат для всех объявлений, чтобы пользователи к ним привыкли. В зависимости от культуры вашей организации, сообщение может распространяться по электронной или голосовой почте, в виде бумажной записки, записи новостной группы, веб-страницы, объявления на двери или дымовых сигналов. Вне зависимости от формата, сообщение должно быть кратким и по теме. Многие люди читают только строку «Тема», поэтому составьте текст грамотно, как показано на рис. 18.1.

Кому: Всем пользователям

Тема: ПЕРЕЗАГРУЗКА СЕРВЕРА СЕГОДНЯ В 18.00

От: Группа системного администрирования

Обратный адрес: tom@example.com

Дата: Четверг, 16 июня 2001

КОГО ЭТО ЗАТРОНЕТ:

Все узлы на DEVELOPER-NET, TOWNVILLE-NET и BROCCOLI-NET.

ЧТО ПРОИЗОЙДЕТ:

Все серверы будут перезагружены.

КОГДА?

Сегодня с 18 до 20 часов (должно занять 1 час).

ЗАЧЕМ?

Мы распространяем новые параметры настройки ядра по всем серверам.
Это требует перезагрузки. Риск минимален. Более подробную информацию можно найти на веб-странице http://portal.example.com/sa/news0005.

Я ПРОТИВ!

Отправьте сообщение в службу поддержки, и мы попытаемся изменить время. Пожалуйста, назовите имя сервера, который вы хотите нас попросить не перезагружать сегодня.

***Рис. 18.1.** Образец сообщения об обновлении*

Лучше иметь пустой шаблон, который нужно будет каждый раз заполнять, чем редактировать предыдущие объявления для включения новой информации. Это предотвращает форму от изменения со временем. Это также предотвращает распространенную проблему того, что некоторые части текста забывают заменить. Например, при подготовке рис. 18.1 мы первоначально использовали настоящее объявление о перезагрузке маршрутизатора. Мы изменили его на сообщение о серверах, но забыли отредактировать строку «Тема». Пример про-

шел через четыре корректуры, прежде чем кто-то это заметил. Если бы мы начали с пустого шаблона, то этого бы не произошло.

18.1.7. Этап 7: выполните тесты

Прямо перед началом обновления выполните тесты. Такая проверка в последний момент позволит вам убедиться, что вы не будете после обновления отслеживать проблемы, которые существовали еще до него. Представьте ужас от выполнения плана отмены только для того, чтобы узнать, что неудачный тест все равно не выполняется.

18.1.8. Этап 8: заблокируйте пользователей

Обычно лучше позволить пользователям выйти из системы самостоятельно, чем выбросить их путем перезагрузки или отключения службы. В различных службах для этого есть разные способы. Используйте доступные в ОС средства, чтобы предотвратить вход в систему во время технического перерыва. Многие пользователи делают попытку входа в систему или доступа к ресурсу в целях собственной проверки обновления. После успешной попытки пользователь считает, что система доступна для нормальной работы, даже если об этом не было объявлено. Поэтому важно заблокировать пользователей на время технического перерыва.

18.1.9. Этап 9: выполните обновление под чьим-нибудь наблюдением

С этого начинается большинство книг для системных администраторов. Разве вы не рады, что купили именно эту книгу?

Теперь пришел момент, которого вы все ждали: выполните обновление в соответствии с вашими местными процедурами. Вставьте DVD, перезагрузитесь или сделайте что-то еще.

Обновления системы слишком важны, чтобы выполнять их в одиночку. Во-первых, все мы делаем ошибки и вторая пара глаз всегда полезна. Обновления выполняются не каждый день, поэтому кому угодно может не хватать опыта. Во-вторых, когда два человека вместе обновляют систему, происходит уникальное обучение. Системные обновления часто требуют максимального использования наших технических знаний. Мы используем команды, знания и, возможно, даже части нашего мозга, которые не задействованы в другое время. Вы можете многому научиться, если посмотрите и поймете приемы, которые кто-то будет применять в это время. Метод совместной разработки, или так называемого парного программирования, становится все более популярным и предполагает, что разработчики работают в парах и набирают код по очереди. Это еще один метод разработки, использование которого может принести пользу системным администраторам.

Если обновление окажется неудачным, то никогда нелишне обратиться за помощью к коллеге или к старшему сотруднику вашего подразделения. Вторая пара глаз часто творит чудеса, и никому не должно быть стыдно просить помощи.

18.1.10. Этап 10: проверьте свою работу

Теперь повторите все ранее созданные тесты. В случае их невыполнения действуйте в соответствии с обычным процессом отладки. Тесты можно повторять снова и снова по мере проведения отладки. Вполне естественно снова запускать невыполненный тест после каждой попытки устранить проблему. Однако убедитесь, что вы запустили все тесты, прежде чем объявить об успехе обновления, так как многие процессы серверов взаимосвязаны. Исправление неполадки, которая вызывала невыполнение теста, может привести к невыполнению другого теста, который раньше выполнялся.

На данном этапе нужно привлекать пользователей. Как и в случае с моделью службы поддержки в главе 14, работа не может считаться выполненной, пока пользователи не проверили, что все завершено. Это может означать, что нужно позвать пользователей в заранее назначенное время либо пользователи могут согласиться сообщить вам на следующий день после завершения технического перерыва. В этом случае правильная работа автоматизированных тестов даже более важна.

18.1.11. Этап 11: если ничего не получилось, выполните план отмены

Если человек, который следит за временем, сообщает, что наступило время реализации плана отмены, вы должны начать его выполнение. Это может произойти, если обновление занимает больше времени, чем ожидалось, или если оно завершено, но тесты все еще не выполняются. Решение полностью определяется временем, а не вами или вашей группой. Отмена сложного обновления может разочаровывать или раздражать, но поддержание целостности сервера важнее.

Возвращение системы к предыдущему состоянию не должно быть единственным компонентом плана отмены. Пользователи могут согласиться, что, если не будут выполняться только определенные тесты, они смогут прожить 1–2 дня без службы, пока она восстанавливается. Заранее определите план действий на случай каждой потенциальной ошибки.

После выполнения плана отмены службы снова нужно проверить. На этом этапе важно зафиксировать в вашем контрольном списке результаты изменений. Это полезно для сообщения о состоянии дел руководству, усовершенствования процесса в следующий раз или восстановления цепи событий во время разбора. Записывайте такие особенности, как «реализовано по плану», «реализовано, но превысило заданное время», «частично реализовано, требуется больше работы», «не реализовано, изменение отменено», «не реализовано, служба недоступна, ожидается конец света». По возможности зафиксируйте результаты тестов и храните их вместе с информацией о состоянии. Это очень здорово поможет, если вы попытаетесь вспомнить, что произошло, на следующей неделе, в следующем месяце или в следующем году.

18.1.12. Этап 12: восстановите доступ пользователей

Теперь можно снова позволить пользователям начать работать с системой. У различных служб есть разные способы это разрешить. Однако часто сложно осуществить проверку, не разрешив всем пользователям доступ.

Впрочем, есть ряд способов это сделать. Например, при обновлении сервера электронной почты вы можете настроить другие серверы электронной почты не отправлять сообщения на обновляемый сервер. Пока эти серверы удерживают электронную почту, вы можете вручную проверить обновленный сервер, а затем сразу разрешить окружающим серверам отправку, внимательно наблюдая за только что обновленным сервером.

18.1.13. Этап 13: сообщите о завершении/отмене

На этом этапе сотрудникам сообщается о том, что обновление завершено или, если был задействован план отмены, что было выполнено, что не было выполнено и что системами снова можно пользоваться. Здесь выполняются три задачи. Во-первых, людям сообщают, что службы, к которым у них не было доступа, снова работают. Во-вторых, пользователям напоминают, что изменилось. Наконец, если они обнаружат проблемы, которые не были найдены в ходе вашего тестирования, им дают знать, как сообщить об этих проблемах. Если был задействован план отмены, пользователей следует проинформировать о том, что система должна работать идентично тому, как это было до попытки обновления.

Точно так же, как есть много способов объявить о техническом перерыве, существует много способов сообщить о завершении. Здесь возможна противоречивая ситуация. Пользователи не смогут прочесть сообщение электронной почты, если отключение затронуло службу электронной почты. Однако, если вы будете держаться в рамках своего технического перерыва, после него электронная почта возобновит свою работу и пользователи смогут прочесть отправленное по ней объявление. Если пользователи ничего не услышат, они посчитают, что после окончания объявленного технического перерыва все сделано.

Объявления должны быть краткими. Просто укажите, какие системы или службы снова работают, и предоставьте ссылку, по которой люди могут обратиться для получения более подробной информации, и номер телефона, по которому можно позвонить, если служба не заработает и будет невозможно отправлять электронную почту. Одного или двух предложений будет достаточно.

Самый простой способ сделать сообщение коротким – переслать первоначальное сообщение, которое указывало, какие службы будут отключены, и добавить в начале предложение о том, что службы снова включены, и о том, как информировать о проблемах. Это очень эффективно предоставляет людям контекст того, о чем сообщается.

Большие красные знаки

Пользователи склонны игнорировать сообщения от системных администраторов. Джош Саймон (Josh Simon) рассказал о том, что в одной компании, которую он обслуживал, он пытался оставлять записки, приклеенные к мониторам, – черный текст на ярко-красной бумаге, – где крупным шрифтом было написано «НЕ ВХОДИТЕ В СИСТЕМУ – СНАЧАЛА СВЯЖИТЕСЬ СО СВОИМ СИСТЕМНЫМ АДМИНИСТРАТОРОМ ПО ТЕЛЕФОНУ [номер телефона]!». Более 75% пользователей срывали бумагу и пытались входить в систему, а не звонили по указанному номеру. Из этого следует, что часто лучше действительно отключить службу, чем просить сотрудников не пользоваться ею.

18.2. Тонкости

Что вы можете сделать для развития процесса после того, как овладеете основами обновления сервера?

18.2.1. Добавляйте и удаляйте службы одновременно

В ходе обновления вы иногда должны одновременно добавлять и удалять службы. Это усложняет дело, потому что в один момент времени вносится более одного изменения. Отладка системы с двумя изменениями гораздо труднее, потому что требует особых тестов. Для добавления служб характерны те же самые проблемы, что и для установки новой службы на новом узле, но в данном случае вы будете в новой, возможно нестабильной, среде и не сможете подготовиться, написав соответствующие тесты. Однако, если новая служба также доступна на другом узле, можно разработать тесты и запустить их на нем.

Удаление службы может одновременно быть простым и сложным. Оно может быть простым по той же причине, по которой разрушить здание проще, чем его простроить. Однако сначала вы должны убедиться, что в здании нет людей. Иногда мы устанавливаем анализатор трафика для отслеживания пакетов, который показывает, что кто-то пытается воспользоваться службой на узле. Эта информация может быть полезна для поиска отставших.

Мы предпочитаем отключать службу так, чтобы ее можно было быстро снова активировать, если в дальнейшем будут обнаружены забытые зависимости. Обычно справедливо допущение, что можно удалить программу, если в течение следующего месяца или года не будут обнаружены забытые зависимости. Некоторые службы могут использоваться только раз в квартал или раз в год, особенно те или иные средства финансовой отчетности. Не забывайте вернуться, чтобы их убрать! Создайте заявку в вашей системе службы поддержки, отправьте себе сообщение электронной почты или создайте задание для `at`, которое отправит вам по электронной почте напоминание через некоторое время. Если доступ к узлу есть у нескольких групп системных администраторов или привилегированных пользователей, может быть полезным внести в файл конфигурации комментарий или переименовать его в OFF или DISABLED (ОТКЛЮЧЕНО). Иначе другой системный администратор может предположить, что служба должна работать, и снова ее включит.

18.2.2. Полная установка

Иногда гораздо лучше переустановить систему полностью, чем обновить ее. Выполнение одного обновления за другим может привести к тому, что система будет сильно повреждена. При этом могут остаться файлы от предыдущих обновлений, фрагментированные файловые системы и «богатое наследие» эпохи беспорядка.

Ранее мы рассматривали такую роскошь, как точное копирование определенных дисков и выполнение обновления на копии. Осуществить обновление как полную установку на другой системе – еще большая роскошь, потому что это не требует отключения старой системы. Вы можете выполнить полную установку на временной машине в спокойном темпе, убедиться, что все службы работают, а затем

подключить диски к обновляемой машине и соответствующим образом настроить конфигурацию сети. Имейте в виду, что машина, на которой осуществляется установка, должна быть практически идентична обновляемой машине, чтобы на дисках с новой ОС обеспечивалась вся необходимая поддержка и конфигурация оборудования.

18.2.3. Повторное использование тестов

Если тесты хорошо написаны, их можно интегрировать в систему мониторинга реального времени. На самом деле, если ваша система мониторинга уже выполняет все необходимые тесты, то при обновление вам ничего больше не потребуется (см. в главе 22 более подробное описание мониторинга служб).

Редко все тесты можно автоматизировать и внести в систему мониторинга. Например, тестирование нагрузки – определение того, как работает система под нагрузкой определенного объема работы, – часто нельзя выполнить на работающей системе. Однако возможность запустить эти тесты во время низкой интенсивности использования или по требованию при отладке может упростить отслеживание проблем.

18.2.4. Запись изменений системы

Построение контрольного списка служб гораздо проще, если вы ведете лог того, что было добавлено на машину. Например, в UNIX-системе просто записывайте изменения в файле под названием /var/adm/CHANGES. Чем проще редактировать файл, тем более вероятно, что люди будут его обновлять, поэтому создайте псевдоним оболочки или короткий скрипт, который просто открывает этот файл в текстовом редакторе.

Конечно, если машина не будет работать, логи изменений могут быть недоступны. Хранение лога изменений в википедии или на общем файловом сервере решает эту проблему, но может привести к путанице, если кто-то попытается начать новый лог изменений для узла. Установите правила, где должны храниться логи изменений, и соблюдайте их.

18.2.5. Генеральная репетиция

Учитесь у мира театра: повторение – мать учения. Почему бы перед выполнением обновления не провести генеральную репетицию на другой машине. Это может раскрыть неожиданные препятствия, а также показать вам, сколько займет процесс. Генеральная репетиция требует множества ресурсов. Однако, если вы хотите выполнить первое обновление из многих, она может стать ценным средством для оценки времени, которое для этого понадобится. Полностью завершенная генеральная репетиция приводит к появлению новой машины, которая может просто заменить старую машину. Если у вас есть эти ресурсы, почему бы это не сделать?

В театре также бывают так называемые *технические репетиции*, которые больше касаются людей, ответственных за свет и звук, чем актеров. Актеры читают свои роли в нужном порядке, а параллельно их словам делаются указания по свету и звуку. Эквивалент для системных администраторов – рассмотрение задачи всеми заинтересованными сторонами.

Кроме того, мы заимствуем у театра искусство мимики и жеста. Иногда серьезное изменение в системе предполагает физическую замену большого числа кабелей. Почему бы не рассмотреть все этапы, обращая внимание на такие проблемы, как длина кабелей, несоответствие прямых и перекрестных обжатий, несоответствие коннекторов «папа/мама», неправильные коннекторы и конфликтующие планы? Имитируйте замену в точности так, как она должна быть сделана. Лучше, если рядом с вами будет еще один человек, который станет объяснять задания по мере того, как вы имитируете их выполнение. Дайте другому человеку проверить, что каждый коннектор исправен и т. д. Сначала это может показаться глупым и трудоемким, но проблемы, которые вы предотвратите, того стоят.

18.2.6. Установка старых и новых версий на одной машине

Иногда на машине обновляется одна служба, а не вся ОС. В этой ситуации удобно, если разработчик разрешает, чтобы старые версии оставались на машине в отключенном состоянии, пока устанавливаются и сертифицируются новые программы.

Веб-сервер Apache под UNIX – один из таких продуктов. Мы обычно устанавливаем его в директорию /opt/apache-x.y.x, где x.y.z – это номер версии, но символическую ссылку из /opt/apache мы помещаем в ту версию, которой хотим пользоваться. При загрузке новой версии ссылка /opt/apache меняется, чтобы указывать на новую версию. В случае проблем с новой версией мы восстанавливаем символическую ссылку и перезапускаем демон. Это очень простой план отмены (применение символических ссылок в базе программного обеспечения рассмотрено в разделе 28.1.6).

В некоторых ситуациях старая и новая версии программы могут работать одновременно. Если требуется серьезная отладка, мы можем запустить новую версию Apache на другом порте, не трогая старую версию.

18.2.7. Минимальные изменения первоначальной версии

Обновления становятся проще, если сделать нужно мало. При помощи небольшого планирования все пакеты обновлений UNIX можно загружать в отдельный раздел, таким образом оставляя системные разделы в минимально измененном виде. Такие дополнения системы могут документироваться в файле CHANGELOG. Большинство изменений будет располагаться в директории /etc, которая достаточно мала, чтобы можно было скопировать ее перед началом любых обновлений и пользоваться ею для справки. Это предпочтительнее трудоемкого процесса восстановления файлов с магнитной ленты.

В UNIX-среде без данных на всех машинах есть локальная ОС, но остальные данные загружаются с сервера – обычно требуется сохранить между обновлениями только /var, а затем только задачи `crontabs` и `at`, данные электронной почты и, в таких системах как Solaris, файлы менеджера календаря. Для отслеживания изменений в файлах конфигурации удобно пользоваться системами контроля версий, например RCS.

Пример: обновление критического DNS-сервера

В данном примере объединены многие приемы, рассмотренные в этой главе. В спешке исправляя все ошибки Y2K перед 1 января 2000 года, Том нашел критический DNS-сервер, который работал на оборудовании, не защищенном от ошибки Y2K, и поставщик объявил, что не будет его исправлять. Кроме того, ОС не поддерживала Y2K. Это была прекрасная возможность поставить полностью новую ОС на совершенно новом оборудовании.

Том создал контрольный список служб. Хотя он думал, что узел предоставлял только две службы, при помощи `netstat -a` и перечисления всех запущенных процессов он обнаружил на машине много других служб. Он обнаружил, что многие из этих дополнительных служб больше не использовались, и нашел одну службу, которую никто не смог идентифицировать.

Люди знали, что большинство используемых программ будут работать на новой ОС, потому что они функционировали на других машинах с более новой ОС. Однако многие службы были внутренними разработками, и началась паника, когда не смогли найти исходный код из-за того, что автор, написавший эту программу, больше не работал в компании. К счастью, код был найден.

Том собрал новую машину и воспроизвел на ней все службы. На оригинальном узле было много файлов конфигурации, которые регулярно редактировались. Тому требовалось переписать эти файлы на новую систему, чтобы проверить, будут ли скрипты, которые их обрабатывают, работать на новой машине правильно. Однако из-за того, что обновление должно было занять пару недель, эти файлы могли подвергнуться многократному изменению, прежде чем новый узел будет готов. Тесты были выполнены на устаревших данных. Когда новая система была готова, Том остановил все изменения на старом узле, заново скопировал все файлы на новую систему и проверил, принимает ли новая система новые файлы.

Разработанные тесты запускались не один раз перед переходом, а многократно, по мере того как появлялась возможность пользоваться службами на новой системе. Однако Том оставлял большинство служб отключенными, когда они не тестировались, потому что старые и новые машины могли конфликтовать друг с другом.

Переход был организован следующим образом: старая машина была отключена от сети, но оставалась включенной. IP-адрес новой машины был изменен на адрес старой. Через пять минут срок действия ARP-кэшей локальной сети кончился и новый узел был определен. При возникновении проблемы Том мог отключить новую машину от сети и подключить старую. Старая машина осталась включенной, поэтому для ее возвращения в эксплуатацию не требовалось даже перезагрузки, нужно было только остановить новый сервер и подключить сетевой кабель старого.

Фактический технический перерыв мог быть довольно коротким – хватило бы и пяти минут, если бы все прошло хорошо и машину можно было бы сразу подключить. Однако был объявлен 30-минутный перерыв.

Том решил попросить двух человек посмотреть за его работой во время обновления, потому что он не так хорошо знал эту версию UNIX, как другие, и мало спал предыдущей ночью. Оказалось, что дополнительная пара рук помогла в отключении и подключении проводов.

Группа отрепетировала обновление за несколько часов до технического перерыва. Ничего не меняя, они повторили то, что точно было запланировано. Они убедились, что длина каждого кабеля будет достаточной и что все коннекторы были нужного типа. Этот процесс устранил всю потенциальную путаницу, которая могла бы возникнуть.

Обновление прошло хорошо. Некоторые тесты не были выполнены, но группа в короткие сроки смогла устранить проблемы. Неожиданной проблемой стала невозможность выполнения некоторых обновлений баз данных, пока не был исправлен скрипт. Пользователи, которые зависели от этих обновляемых данных, согласились работать с несколько устаревшими данными, пока на следующий день не исправили скрипт.

18.3. Заключение

Мы описали достаточно полный процесс обновления операционной системы компьютера, не упоминая при этом ОС конкретных разработчиков, конкретных команд, которые надо ввести, или кнопок, по которым нужно щелкнуть. Важнейшие элементы процесса связаны не с технологией (это вопрос чтения руководств), а с распространением информации, вниманием к деталям и тестированием.

Основное средство, которым мы пользовались, – это контрольный список. Мы начали с составления контрольного списка, которым затем пользовались для определения того, какие службы требовали обновления, сколько времени займет обновление и когда мы сможем его выполнить. Контрольный список определяет, какие тесты мы разрабатываем, и эти тесты могут использоваться снова и снова. Мы пользуемся этими тестами до и после обновления, чтобы обеспечить должное качество. Если обновление проходит неудачно, мы задействуем планы отмены, включенные в контрольный список. Когда процесс завершен, мы объявляем это заинтересованным пользователям, перечисленным в контрольном списке.

Контрольный список – это простое средство. Это единственное место, где собрана вся информация. Вне зависимости от того, используете ли вы бумагу, электронную таблицу или веб-страницу, контрольный список является точкой сбора. Он, фигурально выражаясь, поддерживает единство группы, позволяет не упускать из вида детали, помогает пользователям понимать процесс, а руководству – следить за происходящим и позволяет новым сотрудникам быстро входить в курс дела.

Как и многие процессы системного администрирования, обновление требует навыков общения. Переговоры – это процесс общения, и мы используем его, когда определяем, когда произойдет обновление, что должно произойти и каковы приоритеты, если что-то пойдет не так. Мы предоставляем пользователям ощущение завершенности, сообщая им об окончании работы. Это улучшает

отношения пользователей и системных администраторов. Мы не можем переоценить важность размещения контрольного списка на веб-странице. Чем больше людей могут ознакомиться с информацией, тем лучше.

Когда тесты автоматизированы, мы можем точно повторять их и обеспечить полноту их выполнения. Эти тесты должны быть достаточно общими, чтобы ими можно было пользоваться для дальнейших обновлений не только на том же узле, но и на похожих. Фактически тесты должны быть интегрированы в ваши системы мониторинга реального времени. Зачем выполнять эти тесты только после обновлений?

Этот простой процесс легко понять и отработать. Это один из основных процессов, которыми системный администратор должен овладеть, прежде чем переходить к более сложным обновлениям. Все примеры из реальной жизни, которые мы показали, требовали некоторого отклонения от основного процесса, по все же содержали главные элементы.

Некоторые дистрибутивы ОС делают обновление практически безопасным и безболезненным, но другие гораздо более рискованны. Хотя и нет полной гарантии успеха, гораздо лучше, когда в операционной системе можно осуществлять обновления надежно, с возможностью повторения и простого возвращения к предыдущему состоянию. Минимальное количество команд или щелчков мышью снижает вероятность человеческой ошибки. Возможность обновить много машин воспроизводимым методом имеет массу преимуществ; особенно важно то, что она помогает поддерживать целостность систем. Любая возможность вернуться к предыдущему состоянию предоставляет уровень отмены, аналогичный политике страхования: вы надеетесь, что это никогда вам не понадобится, ну а если понадобится, вы будете рады, что обеспечили такую возможность.

Задания

1. Выберите сервер в вашей среде и выясните, какие службы он предоставляет. Если вы поддерживаете документированный список служб, какими системными командами вы пользуетесь для проверки списка? Если службы не документированы, какими ресурсами вы можете воспользоваться для построения полного списка?
2. Как вы узнаете в своей среде, кто какими службами пользуется?
3. Выберите место, до которого легко дойти из вашей серверной или офиса, например магазин неподалеку, банк или какое-то место в другом конце вашего здания, если оно очень большое. Попросите трех-четырех студентов, коллег или друзей оценить, сколько времени займет дорога туда и обратно. Теперь вы все вместе должны пойти туда и записать, сколько времени это заняло. (Сделайте это прямо сейчас, до того, как прочтете оставшуюся часть вопроса. Правда!) Сколько времени это заняло? Вы пошли сразу или задержались? Сколько неожиданных событий по пути – случайных встреч с пользователями, с людьми, которые хотели узнать, чем вы занимаетесь, и т. д. – увеличили время дороги? Посчитайте, насколько точны были ваши оценки, их среднее значение и среднеквадратическое отклонение. Чему вы научились в этом эксперименте? Как вы думаете, насколько лучше будут ваши оценки, если вы повторите эксперимент с тем же местом? С другим местом? Повлияет ли на время привлечение большего количества

людей? Свяжите полученный опыт с процессом планирования технического перерыва.

4. В разделе 18.1.3 утверждается, что разработанные тесты должны быть выполнены как минимум три раза, а при наличии проблем – больше. Что это за минимальные три раза? При каких условиях тесты могут быть запущены повторно?
5. В разделе 18.2.7 есть пример, в котором практически невозможно было найти исходный код службы собственной разработки. Как бы вы поступили в такой ситуации, если бы не смогли найти исходный код?
6. Как вы объявляете планируемые отключения и технические перерывы в своей среде? Каковы преимущества и недостатки этого метода? Какая часть ваших пользователей игнорирует эти сообщения?
7. Пользователи часто игнорируют сообщения от системных администраторов. Что можно сделать, чтобы улучшить положение дел?
8. Выберите узел в вашей среде и обновите его (сначала спросите разрешения!).
9. Какие меры вы предприняли бы, если бы вам потребовалось заменить единственный туалет в вашем здании?

Глава 19

Изменение служб

Иногда вам требуется перевести свою базу пользователей с существующей службы на новую, которая ее заменит. У существующей системы могут отсутствовать возможности расширения, или ее разработчик может объявить о прекращении поддержки и попросить вас оценить новые системы. Либо ваша компания могла слиться с компанией, использующей другие продукты, и обеим частям новой компании требуется интегрировать свои службы друг с другом. Возможно, ваша компания отделяет подразделение в новую, отдельную компанию и вам требуется воспроизвести и разделить службы и сети, чтобы каждая часть была полностью самостоятельной. Вне зависимости от причины перевод пользователей с одной службы на другую является задачей, которую часто выполняют системные администраторы.

Подобно многому другому в системном и сетевом администрировании, ваша цель должна заключаться в том, чтобы переход был плавным и абсолютно незаметным для ваших пользователей. В данной главе рассмотрены некоторые области, заслуживающие внимания в процессе планирования.

Невидимое изменение

Когда AT&T отделила Lucent Technologies, исследовательский отдел Bell Labs был разделен на две части. Системные администраторы, которые обслуживали этот отдел, вынуждены были разделить сеть Bell Labs, чтобы люди, которые должны были войти в Lucent, не имели доступа ни к каким службам AT&T, и наоборот. Через некоторое время после завершения разделения один из исследователей спросил, когда оно должно произойти. Он был очень удивлен, когда ему сказали, что оно уже было завершено, потому что не заметил никаких изменений. Проект был успешным в плане создания минимальных неудобств для пользователей.

19.1. Основы

Как и в случае со многими задачами системного администрирования высокого уровня, успешный переход зависит от наличия надежной инфраструктуры. Распространение изменения по всей компании может быть очень заметным проектом, особенно если возникнут проблемы. Вы можете снизить риск и заметность проблем за счет медленного распространения изменения, начиная

с системных администраторов с последующим переходом к наиболее подходящим пользователям. При любом изменении убедитесь, что у вас есть план отмены и что при необходимости вы сможете быстро и легко вернуться к состоянию до изменения.

Мы видели, как система автоматизированного обновления может использоваться для распространения обновлений программ (глава 3) и как построить службу, применяя некоторые методы, позволяющие упростить ее обновление и поддержку (глава 5). Эти приемы могут быть важными элементами вашего плана распространения.

Распространение информации играет ключевую роль в осуществлении успешного перехода. Неразумно что-то менять, не убедившись, что ваши пользователи знают о происходящем и рассказали вам о своих заботах и временных ограничениях.

В данном разделе мы коснемся каждой из этих областей, а также способов минимизировать вмешательство в работу пользователей и рассмотрим два подхода к изменениям. Вам нужно хорошо спланировать каждый этап перехода заблаговременно, чтобы выполнить его с минимальным влиянием на пользователей. Данный раздел должен задать направление вашего мышления в этом процессе планирования.

19.1.1. Минимизируйте вмешательство

При планировании распространения изменения уделяйте большое внимание влиянию на пользователей. Стремитесь, чтобы переход имел по возможности минимальное влияние. Пытайтесь сделать его плавным.

Требует ли переход прерывания работы службы? Если да, как вы можете минимизировать время недоступности службы? На какое время лучше всего запланировать перерыв в обслуживании, чтобы он имел наименьшее влияние?

Требует ли переход изменений на рабочей станции или в офисе каждого пользователя. Если да, сколько времени они займут и сможете ли вы организовать переход так, чтобы побеспокоить пользователя только один раз?

Требует ли переход какого-либо изменения методов работы пользователей, например, за счет использования нового клиентского программного обеспечения? Можете ли вы избежать изменения клиентского программного обеспечения? Если нет, потребуется ли пользователям обучение? Иногда обучение является более крупным проектом, чем собственно переход. Удобно ли для пользователей новое программное обеспечение? Знакомы ли их системные администраторы и служба поддержки с новыми и старыми программами, чтобы они могли помочь с любыми вопросами пользователей? Были ли обновлены скрипты службы поддержки?

Ищите способы выполнить изменение без прерывания обслуживания, посещения каждого пользователя или изменения рабочего процесса либо пользовательского интерфейса. Убедитесь, что организация поддержки готова предоставлять полную поддержку нового продукта или службы, прежде чем их распространять. Помните, ваша задача – сделать переход настолько плавным, чтобы пользователи даже не поняли, что он произошел. Если вы не можете минимизировать вмешательство, в ваших силах, по крайней мере, сделать его быстрым и хорошо организованным.

Метод протестующей толпы

Когда AT&T разделялась на AT&T, Lucent и NCR, группа системных администраторов Тома отвечала за разделение сетей Bell Labs в Холмделе, Нью-Джерси (Limoncelli et al. 1997). В определенный момент нужно было посетить каждый узел, чтобы выполнить несколько изменений, в том числе поменять IP-адрес. Был объявлен график, в котором было указано, когда какие участки будут переведены. Переходы проходили по понедельникам и средам, по вторникам и четвергам исправлялись возникавшие неполадки, пятницы были не задействованы, чтобы изменения не вызывали проблем, которые могли бы нарушить сон системных администраторов по выходным.

В дни перехода группа пользовалась методом, который она называла «методом протестующей толпы». В 9 утра системные администраторы собирались в одном конце коридора. Они готовились психологически, часто даже с молитвой, и шли по коридору парами. Две пары состояли из специалистов по персональным компьютерам, две пары – из специалистов по UNIX, одна группа обслуживала комнаты с левой стороны коридора, другая – с правой. По мере того как специалисты переходили из одного офиса в другой, они выводили сотрудников и шли от машины к машине, выполняя необходимые изменения. Иногда машины были особенно сложным или имели проблемы. Вместо того чтобы пытаться исправлять их самостоятельно, специалисты вызывали для решения проблем старшего сотрудника группы, а сами переходили к следующей машине. В это время последняя пара сотрудников оставалась в центре управления, куда системные администраторы могли позвонить для запроса IP-адресов и обновления базы данных узлов, а также учетной и других баз данных.

Следующий день тратился на исправление всего, что было нарушено, и обсуждение проблем для совершенствования процесса. Мозговая атака показывала, что было сделано хорошо, а что требовалось улучшить. Специалисты решили, что было бы лучше первый раз проходить по коридору, запрашивая IP-адреса, предоставляя пользователям возможность выйти из системы и определяя нестандартные машины, на которые должны будут обратить внимание старшие системные администраторы. На втором проходе по коридору у каждого был необходимый IP-адрес и дела шли более гладко. Скоро они смогли обрабатывать два участка утром, а все исправления выполнять днем.

Мозговая атака между любыми переводами была важна. То, что специалисты узнавали в первый раз, вызывало радикальные изменения в процессе. В конце концов мозговые атаки перестали приносить какую-либо новую информацию и дни отдыха стали использоваться для планирования следующих дней. Часто день перехода проходил гладко и завершался к обеду, а все проблемы разрешались во второй половине дня. День перерыва становился нормальным рабочим днем.

Сведение вмешательства в работу пользователей к одному дню для каждого отдельного пользователя было очень успешным. Пользователи ожидали какого-то отключения, но посчитали бы неприемлемым, если

бы отключение было длительным или разделенным по многим участкам. Одна группа пользователей воспользовалась днем перехода, чтобы выехать на пикник на целый день.

19.1.2. Горизонтально или вертикально

Проект по переходу, как и любой другой проект, разделен на отдельные задачи; некоторые из них нужно выполнить для каждого пользователя. Например, в случае перехода на новую программу календаря новое клиентское программное обеспечение должно быть распространено по всем рабочим станциям, на сервере нужно создать учетные записи, а существующие графики необходимо перевести в новую систему. В процессе планирования проекта перехода вам потребуется решить, как выполнять эти задачи – горизонтально или вертикально.

При *горизонтальном* подходе вы выполняете одну задачу для всех пользователей прежде чем перейти к другой задаче, и делаете так для всех пользователей.

При *вертикальном* подходе вы сразу выполняете все необходимые задачи для каждого пользователя, а затем переходите к следующему пользователю[1].

Задачи, которые не вмешиваются в работу пользователей, например создание учетных записей на сервере календаря, можно безопасно выполнять горизонтально. Однако задачи, которые вмешиваются в их работу, например установка нового клиентского программного обеспечения, блокировка календаря пользователя и его перевод в новую систему и первоначальное подключение пользователя для определения своего пароля, должны выполняться вертикально.

При вертикальном подходе вы должны выделить на каждого пользователя только один период времени, а не несколько более коротких. Благодаря выполнению всех задач в одно время вы беспокоите каждого пользователя только один раз. Одно вмешательство обычно меньше нарушает работу пользователя, чем несколько более мелких, даже если оно требует немного большего времени.

Комбинированный подход имеет преимущества обоих подходов. Сгруппируйте все перерывы, заметные для пользователей, в минимально возможное количество временных промежутков. Выполняйте все остальные изменения незаметно.

Пример: вертикальный и горизонтальный подходы в Bell Labs

Когда от AT&T отделялась Lucent Technologies и Bell Labs разделялась на две части, на каждой рабочей станции требовалось выполнить много изменений, чтобы вместо машины Bell Labs она стала машиной Lucent

[1] Что вам будет удобнее приготовить: один большой пирог на 12 человек или 12 маленьких пирожков, по одному на каждого человека? Вы, конечно, захотите испечь один большой пирог. А теперь представьте, что вместо пирога вы готовите омлет. Если люди желают добавить в омлет различные ингредиенты, неразумно готовить один большой омлет на всех.

Bell Labs или AT&T Labs. На самых ранних этапах группа системных администраторов, ответственная за реализацию разделения, поняла, что для большинства изменений будет использоваться вертикальный подход, но иногда лучше был бы горизонтальный подход. Например, горизонтальный подход применялся при построении новых веб-прокси-серверов. Новые прокси-серверы были собраны и проверены, а затем пользователи переключились на них. Однако на каждой рабочей станции под UNIX требовалось внести более 30 изменений и было решено, что все они должны быть выполнены за одно посещение и с одной перезагрузкой, чтобы минимизировать неудобство пользователей.

Этот подход был очень рискованным. Что случится, если будет изменена последняя рабочая станция, а затем системные администраторы обнаружат, что одно изменение было сделано неправильно на каждой машине? Для снижения этого риска в наиболее посещаемых местах были размещены машины-образцы с новой конфигурацией и пользователей пригласили испытать их. Таким образом системные администраторы смогли найти и исправить множество проблем, прежде чем изменения были реализованы на рабочей станции каждого пользователя. Этот подход также помог пользователям привыкнуть к изменениям. Некоторые пользователи особенно боялись, потому что они не очень доверяли группе системных администраторов. Каждого из этих пользователей лично привели к общим машинам и попросили войти в систему, а проблемы отлаживались в реальном времени. Это успокоило пользователей и повысило их доверие. Проект по разделению сети подробно описан в работе Limoncelli et al. 1997.

Компании электронной коммерции также могут подумать об изменениях с горизонтальным и вертикальным подходами, несмотря на то что со стороны они кажутся однородными. Небольшое изменение или даже новая версия программы может распространяться вертикально, один узел за раз, если изменение выполняется для более старых систем. Изменения, которые легко осуществлять пакетами, например импорт данных пользователей, могут выполняться горизонтально. Это особенно справедливо для изменений, не требующих нарушения работы, таких как копирование данных на новые серверы.

19.1.3. Распространение информации

Несмотря на то что основным принципом перехода является незаметность для пользователя, вам все-таки требуется показать план перехода вашим пользователям. На самом деле заблаговременное распространение информации об изменении очень важно.

Благодаря общению с пользователями касательно изменений вы найдете людей, которые пользуются службой тем способом, о котором вы не знаете. Вам потребуется поддержать их использование новой системы. Все пользователи, которые широко применяют систему, должны быть привлечены на раннем этапе проекта, чтобы убедиться, что их потребности будут удовлетворены. Вы должны выяснить все важные предельные сроки, которые есть у ваших пользователей, или любые другие моменты времени, когда система должна быть абсолютно стабильной.

Пользователи должны знать, что происходит и как изменение их затронет. У них должна быть возможность задавать вопросы о том, как они будут выполнять свои задачи в новой системе, а все их интересы должны быть учтены. Пользователи должны заранее знать, потребует ли переход отключения службы, изменений в их машинах или посещения их офисов.

Даже если переход должен пройти незаметно, без прерывания обслуживания и без видимого изменения для пользователей, они все-таки должны знать, что он происходит. Пользуясь полученной вами информацией, запланируйте его так, чтобы в случае, если что-то пойдет не так, влияние на пользователей было минимальным.

Высокоуровневые задачи перехода должны быть заранее запланированы и записаны, очень часто пользователи пытаются внести новые функции или службы в качестве требований во время планирования обновления. Внесение новых объектов повышает сложность перехода. Ищите компромисс между необходимостью поддерживать работу и желанием улучшать службы.

19.1.4. Обучение

С распространением информации связано обучение. Если какой-либо аспект работы пользователя планируется изменить, должно предоставляться обучение. Это справедливо вне зависимости от того, будет такое изменение связано с небольшими отличиями в меню или полной сменой процесса работы.

Большинство изменений несущественно, и о них можно сообщить людям по электронной почте. Однако при развертывании новых крупных систем мы постоянно видим, что обучение критически важно для введения их в эксплуатацию. Чем меньше технически подготовлены пользователи, тем важнее включение обучения в ваши планы распространения.

Создание и предоставление обучения обычно не входит в обязанности группы системных администраторов, выполняющих переход, но может потребоваться, чтобы системные администраторы поддерживали обучение сторонними компаниями или разработчиками. Тесно взаимодействуйте с пользователями и руководством, управляющим переходом, чтобы заранее подготовить планы по поддержке обучения. Нетехнические пользователи вряд ли могут представить себе объем работы системных администраторов по созданию учебного класса на 5–15 рабочих станций со специальными настройками брандмауэра для ноутбука инструктора[1].

19.1.5. Начинайте с небольших групп

При выполнении распространения, вне зависимости от того, является ли это переходом, новой службой или обновлением существующей службы, вы должны выполнять его постепенно, чтобы минимизировать потенциальное влияние любых ошибок. Начните с перевода на новую службу своей собственной системы. Проверьте и отточите процесс перехода, а также новую службу, прежде чем переводить на нее другие системы. Когда у вас проблемы больше не будут возни-

[1] Страта слышала, как на выполнение подобного указания давалось всего 3 рабочих дня и заказчик считал, что их «вполне достаточно».

кать, переведите несколько рабочих станций своих коллег, найдите и исправьте все ошибки, которые возникнут в процессе перехода и тестирования новой системы. Расширьте группу тестирования, чтобы она охватывала всех системных администраторов, прежде чем начинать работу со своими пользователями. После успешного перевода системных администраторов начните с пользователей, которые лучше могут справиться с возможными проблемами и согласились быть первыми, и постепенно переходите к более консервативным пользователям. Таким подходом «один, несколько, много» в распространении новых версий и обновлений можно пользоваться более глобально для любых видов изменений, в том числе для переходов на новые службы (см. раздел 3.1.2).

Обновление серверов Google

Веб-ресурсы Google содержат тысячи компьютеров, их реальное количество является коммерческой тайной. При обновлении тысяч дублирующих друг друга серверов в Google применяется мощная автоматизация, которая сначала обновляет один узел, потом – 1% узлов, потом – группы узлов, пока все они не будут обновлены. Между периодами обновлений выполняется тестирование, и у оператора есть возможность остановить и отменить изменения в случае обнаружения проблем. Иногда время между обновлениями исчисляется часами, а порой – днями.

19.1.6. Мгновенные изменения: делать все сразу

По возможности избегайте одновременного перевода всех сотрудников с одной системы на другую. Переход будет гораздо более плавным, если сначала вы для проверки переведете на новую систему нескольких желающих. Недопустимость мгновенного изменения может означать заблаговременное выделение средств на дублирующее оборудование, поэтому при подготовке своего бюджетного запроса не забудьте подумать о том, как вы будете выполнять распространение изменения.

В других случаях у вас может быть возможность воспользоваться функциями имеющихся технологий для медленного распространения изменения. Например, если вы изменяете иерархию сети или разделяете сеть, то можете воспользоваться IP-подключением к нескольким сетям и вторичными IP-адресами совместно с DHCP (см. раздел 3.1.3), чтобы первоначально перевести несколько узлов, не используя дополнительного оборудования.

В качестве альтернативы у вас может быть возможность сделать старую и новую службы доступными одновременно и предложить людям некоторое время переключаться между ними. Таким образом они смогут испытать новую службу, привыкнуть к ней, сообщить о проблемах с ней и вернуться к старой службе, если она им нравится больше. Это предоставляет вашим пользователям период «адаптации». Данный подход обычно используется в телефонной связи при изменении телефонного номера или кода города. В течение последующих нескольких месяцев при звонке по старому номеру воспроизводится сообщение об ошибке, из которого вызывающий абонент узнает новый номер. Затем старый номер перестает работать, и через некоторое время он становится доступным для нового использования.

Перевод физической сети

Когда одна средняя компания переводила свои сетевые кабели с «тонкого» Ethernet на 10Base-T, она разделила проблему на два основных подготовительных элемента и выделила для каждой части планирования проекта отдельную группу. Первая группа должна была обеспечить физическую установку новой кабельной системы в кабельных боксах и на рабочих местах. Вторая группа должна была обеспечить, чтобы каждая машина в здании поддерживала 10Base-T при помощи установки карты или, при необходимости, модернизации машины.

Первая группа проложила кабели по потолку и подключила их в кабельных боксах. Затем сотрудники группы прошли по зданию, вывели кабели из потолка, подключили их в офисах и на рабочих местах и проверили их, посетив каждый офис или рабочее место только один раз.

Когда обе группы закончили свою подготовительную работу, они последовательно прошли по зданию, переводя машины на новые кабели, но оставляя старые кабели на месте, чтобы в случае возникновения проблем можно было снова переключиться на них.

Этот переход был выполнен хорошо с точки зрения предотвращения мгновенного изменения и постепенного перевода людей. Однако пользователи посчитали его слишком навязчивым, потому что их прервали три раза: для прокладки кабелей, для установки нового оборудования на их машины и наконец непосредственно для перевода. Несмотря на то что это было бы очень трудно скоординировать и потребовалось бы серьезное планирование, обе группы могли посетить каждое рабочее место одновременно и выполнить всю работу сразу. Однако в реальности это оказалось бы очень трудным и слишком сильно задержало бы проект. Было бы проще изначально обеспечить лучшее распространение информации, позволяя пользователям узнать все преимущества новой кабельной системы, заранее извиниться за необходимость побеспокоить их три раза (один из которых потребует перезагрузки) и создания графика работы. Пользователи считают вмешательства менее неприятными, если они понимают, что происходит, имеют некоторый контроль над составлением графика и знают, что они в конце концов от этого выиграют.

Иногда переход или один из его элементов должен быть осуществлен одновременно для всех. Например, если вы переходите с одного сервера корпоративного календаря на другой, когда две системы не могут связываться и обмениваться информацией, вам потребуется перевести всех сразу, иначе люди, использующие старую систему, не смогут назначить встречи с людьми, которые работают с новой системой, и наоборот.

Успешное выполнение мгновенного изменения требует серьезного и внимательного планирования, а также определенного целостного тестирования, в том числе тестирования загрузки. Убедите нескольких ключевых пользователей системы проверить, как новая система будет справляться с их ежедневными задачами, прежде чем выполнять переход. Если вы привлечете самых активных пользователей для тестирования новой системы, вы с большей вероятностью найдете все проблемы с ней до ее ввода в эксплуатацию, и люди, которые боль-

ше всего на нее полагаются, привыкнут к ней, прежде чем начнут ею пользоваться всерьез. Люди по-разному пользуются одними и теми же средствами, поэтому большее число участников тестирования обеспечит больший охват тестирования функций.

При мгновенном изменении особенно важен двусторонний обмен информацией. Убедитесь, что ваши пользователи знают, что и когда будет происходить, а вы заранее знаете и учитываете их интересы до срока перехода. Кроме того, приготовьте план отмены, который будет рассмотрен в следующем разделе.

Изменение телефонных номеров

В 2000 году British Telecom перевела Лондон с двух телефонных кодов на один и удлинила телефонные номера с семи цифр до восьми в рамках одного крупного проекта по изменению номеров. Номера, которые выглядели как (171)xxx-xxxx стали выглядеть как (20)7xxx-xxxx, а номера вида (181)xxx-xxxx превратились в (20)8xxx-xxxx. Более чем за полгода до назначенной даты перехода компания начала сообщать о готовящемся изменении, кроме того, стали работать новый код и новые номера телефонов. В течение нескольких месяцев после назначенной даты перехода старые коды и старые номера телефонов продолжали работать, как это обычно бывает при изменении телефонных номеров.

Однако местные звонки на номера в Лондоне, которые начинались с 7 или 8, были переведены с семи на восемь цифр за одну ночь. Из-за того что внезапное изменение точно вызвало бы путаницу, из British Telecom позвонили каждому абоненту, который был затронут изменением, чтобы лично объяснить, в чем заключалось изменение, и ответить на любые вопросы, которые могли возникнуть у абонентов. Вот это забота о клиентах!

19.1.7. План отмены

При переходе очень важно иметь план отмены. По определению, *переход* означает удаление одной службы и замену ее другой. Если новая служба работает неправильно, пользователь будет лишен средства, которым он пользуется в своей работе, что может серьезно повлиять на производительность его труда.

Если переход не удастся, вам потребуется быстро вернуть службу пользователя к состоянию, в котором она была до внесения вами каких-либо изменений, а затем выяснить причину сбоя и исправить неполадку. Практически это означает, что у вас по возможности должны одновременно работать обе службы, а также должен иметься простой, автоматизированный способ переключения пользователя между ними.

Имейте в виду, что сбой может не быть мгновенным и не обнаруживаться в течение какого-то времени. Он может стать результатом проблем с надежностью программного обеспечения, может быть вызван ограничениями по емкости или связан с функцией, которую пользователь применяет редко либо только в определенное время в месяце или году. Поэтому вы должны сохранить свой механизм отмены на некоторое время, пока не будете уверены, что переход прошел успешно. На какое время? Для критических служб мы рекомендуем значительный

отчетный период, например финансовый квартал в компании или семестр в университете.

Основная трудность с планами отмены – решить, когда их выполнять. Когда переход идет неправильно, техники обычно обещают, что все заработает после «еще одного изменения», но руководство склонно подталкивать к выполнению плана отмены. Важно иметь заранее определенный момент, в который будет задействован план отмены. Например, можно заранее решить, что, если перевод не будет завершен в течение двух часов после начала следующего рабочего дня, должен быть выполнен план отмены. Очевидно, что, если в первые минуты перехода появляются непреодолимые проблемы, может быть лучше отменить то, что уже было сделано, и перенести изменение. Однако может быть полезно узнать мнение кого-нибудь другого. То, что нерешаемо для вас, может быть простой задачей для кого-то еще из вашей группы.

Когда обновление не удалось, очень заманчиво вновь и вновь пытаться исправить ошибку. Мы знаем, что у нас есть план отмены, мы знаем, что мы обещали начать отмену, если обновление не будет завершено к определенному времени, но мы продолжаем говорить «еще только 5 минут» и «я просто хочу попробовать кое-что еще». Связано ли это с самонадеянностью? Гордостью? Отчаянием? Мы не знаем. Однако мы знаем, что продолжать попытки естественно. На самом деле это хорошо. Ведь мы вообще сумели добиться чего-то в жизни только потому, что не спасовали перед непреодолимыми проблемами. Однако, когда технологический перерыв заканчивается и нужно отменять изменения, нам нужно их отменять. Часто наша самонадеянность не позволяет нам так поступить, вот почему может быть полезно попросить кого-то, не участвующего в процессе, например нашего руководителя, следить за временем и заставить нас остановиться тогда, когда мы обещали это сделать.

Отмените изменения. Потом еще будет время снова попытаться.

19.2. Тонкости

Когда вы овладеете распространением изменений с минимальным влиянием на своих пользователей, вы должны усвоить две тонкости для дальнейшего снижения влияния переходов на пользователей. Первая из них – наличие плана отмены, позволяющего осуществить мгновенный откат, чтобы не терять время на перевод ваших пользователей обратно на старую систему в случае обнаружения проблемы с новой. Другая тонкость – избегать выполнения переходов вообще. Мы рассмотрим ряд способов снижения количества проектов по переходу, в которых может возникнуть необходимость.

19.2.1. Мгновенный откат

При выполнении перехода хорошо иметь возможность мгновенно вернуть все к известному рабочему состоянию при обнаружении проблемы. Таким образом любое нарушение работы пользователей, связанное с проблемой в новой системе, может быть минимизировано.

То, как вы обеспечите мгновенную отмену, зависит от перехода, который вы выполняете. Один из вариантов выполнения мгновенной отмены – сохранять старые системы. Если вы просто перенаправляете клиенты пользователей на новый сервер, вы можете переключаться между службами, изменяя единствен-

ную DNS-запись. Чтобы выполнить обновления DNS быстрее, установите заблаговременно меньшее значение в поле *времени жизни* (time to live – TTL), например 5 мин. Затем, когда все будет стабильно, установите обычное значение TTL. **Период обновления** записи SOA домена указывает вторичным серверам DNS, с какой частотой они должны проверять, обновился ли главный DNS-сервер. Если в обоих этих полях установлены низкие значения, обновления DNS будут доходить до клиентов быстро и, следовательно, откат будет проходить быстро и легко. *Имейте в виду*: многие клиентские библиотеки DNS игнорируют поле TTL и сохраняют его значение постоянным. Убедитесь, что подключения к старой машине проходят надлежащим образом или отклоняются.

Другой подход в достижении мгновенной отмены – выполнять переход, останавливая одну службу и запуская другую. В некоторых случаях у вас может быть по два различных клиентских приложения на машинах пользователей, одно из которых использует старую службу, а другое – новую. Данный подход особенно хорошо работает, когда новая служба для тестирования запускается на другом порте.

Иногда вносимое изменение заключается в обновлении программы до новой версии. Если во время применения новой программы старая программа может в отключенном виде находиться на сервере, вы можете мгновенно выполнить откат путем переключения на старую программу. Разработчики могут сделать многое, чтобы это затруднить, но у некоторых из них очень хорошо получается упростить это. Например, если версии сервера 1.2 и 1.3 установлены в /opt/example-1.2 и /opt/example-1.3 соответственно, но символическая ссылка /opt/example указывает на единственную используемую версию, вы можете откатиться, просто изменив единственную символическую ссылку (пример хранилища программного обеспечения, в котором используется этот метод, описан в разделе 28.1.6).

Оба этих простых метода нарушают принцип медленного выполнения распространения или делают изменение более заметным для пользователя. Обеспечение мгновенной отмены с минимальным влиянием на пользователей и с применением метода постепенного распространения является более сложным и требует внимательного планирования и конфигурирования. Вы можете установить дополнительные DNS-серверы, которые предоставляют информацию для новых серверов и всю общую информацию для клиентов, использующих их, а затем воспользоваться своим автоматизированным сетевым средством конфигурации клиентов, рассмотренным в главе 3, чтобы за один раз выборочно перевести несколько узлов на альтернативные DNS-серверы. На любом этапе вы можете снова вернуть эти узлы к прежней конфигурации, изменив их сетевые настройки на первоначальные.

19.2.2. Снижение количества изменений

Развитое планирование может снизить необходимость обновлений и изменений. Например, обновления часто требуются для одновременного расширения службы на большее количество пользователей. Некоторых обновлений можно избежать, начав пользоваться системой большей емкости.

Других изменений можно избежать иными способами. Перед покупкой поговорите с разработчиком о перспективах развития продукта и возможности расширения текущих моделей использования в соответствии с вашими предполагаемыми тенденциями роста. При выборе продукта, который легко расширяется

и интегрируется с другими компонентами вашей сети, даже если в момент покупки вы не считаете такую интеграцию необходимой, вы минимизируете вероятность того, что в будущем вам потребуется перейти на другой продукт из-за необходимости новых функций, проблем с расширением или окончания жизненного цикла продукта.

По возможности выбирайте продукты, использующие стандартные протоколы для связи клиента на рабочей станции и сервера, предоставляющего службу. Если клиент и сервер будут использовать собственный протокол разработчика и вы захотите сменить сервер, вам также потребуется перейти на другое клиентское программное обеспечение. Однако, если продукты будут использовать стандартные протоколы, вы сможете выбрать другой сервер, который использует тот же протокол, и избежать перевода ваших пользователей на новое клиентское программное обеспечение.

Кроме того, у вас должна быть возможность избежать трудоемкого изменения конфигураций пользователей за счет применения методов, входящих в состав хорошей инфраструктуры. Например, использование автоматической сетевой конфигурации (глава 3) с хорошей документацией о том, какая служба на каком узле расположена, существенно упрощает разделение сети без необходимости беспокоить пользователей. Применение имен машин, основанных на их службах (глава 5), позволяет вам перенести службу на новую машину или несколько машин без изменения конфигурации клиента.

19.2.3. Изменения веб-служб

Все больше и больше служб становятся веб-службами. В таких ситуациях обновление сервера редко требует обновления клиентского программного обеспечения, потому что служба работает с любым веб-броузером. С другой стороны, мы до сих пор поражаемся тому, как много веб-служб отказываются работать с чем-то еще, кроме Microsoft Internet Explorer. Смысл HTML – в отделении клиента от сервера. Что если я хочу подключиться с броузера на сотовом телефоне, игровой консоли или смарт-панели моего холодильника? Службе должно быть все равно.

Службы, которые тестируются для конкретного веб-броузера и отказываются работать со всеми остальными, в лучшем случае демонстрируют неудачное исполнение, а в худшем – лень программистов. Мы не можем ожидать от разработчиков тестирования их службы на каждой версии каждого броузера. Однако разработчик вполне может иметь список полностью поддерживаемых броузеров (обеспечение качества включает тестирование этих броузеров и серьезное отношение к ошибкам, о которых будет сообщено), список броузеров без гарантии качества работы (служба работает, но ошибки исправляются без гарантии качества), и сообщать, что можно использовать все другие броузеры, но полная функциональность не гарантируется. По возможности служба должна «мягко» снижать функциональность, когда используется неподдерживаемый броузер. Например, анимированные меню могут отключаться, но должен быть другой способ выбирать варианты.

Служба не должна определять, какой броузер используется, и отказываться работать, так как средний пользователь может предпочесть повозиться с форматированием, нежели покупать компьютер только из-за того, что он поддерживает броузер, выбранный разработчиком. Это особенно справедливо для

броузеров под сотовые телефоны – пользователи и не ожидают безупречного форматирования. Отказ работать со всеми броузерами, кроме определенного, – это грубо и потенциально опасно. Многие разработчики пострадали, когда новая версия поддерживаемого ими броузера не определялась и ни один посетитель не мог воспользоваться службой.

19.2.4. Поддержка разработчиков

При масштабных изменениях убедитесь, что у вас есть поддержка разработчика. Свяжитесь с разработчиком, чтобы выяснить, имеются ли какие-либо препятствия. Это может предотвратить серьезные проблемы. Если у вас хорошие отношения с разработчиком, он захочет участвовать в процессе планирования, иногда даже выделяя персонал. Если нет, разработчик может позаботиться о том, чтобы в день вашего перехода на его «горячей линии» технической поддержки было достаточно специалистов либо можно было бы связаться с кем-то, кто особенно хорошо разбирается в вашей среде.

Не бойтесь раскрыть свои планы разработчику. Редко есть причины хранить такие планы в тайне. Не бойтесь спрашивать у разработчика, в какие дни недели лучше всего получать поддержку. Нет ничего страшного в том, чтобы попросить разработчика назначить конкретного человека из его службы поддержки, чтобы тот ознакомился с планами, когда они будут готовы. В этом случае разработчик может быть лучше подготовленным, если во время обновления вы позвоните с сообщением о проблеме. Хорошие разработчики охотнее ознакомятся с вашим планом заранее, чем допустят, чтобы их пользователь, наполовину завершив обновление, столкнулся с проблемой неподдерживаемых методов.

19.3. Заключение

Успешный проект по переходу основывается на серьезном заблаговременном планировании и надежной инфраструктуре. Успех процесса перехода оценивается по тому, насколько слабо было его негативное влияние на пользователей. Переход должен по возможности минимально вмешиваться в их работу.

Принципы любого распространения – обновления, введения новых служб или перехода – одинаковы. Начните с серьезного планирования, затем медленно распространяйте изменение с большим количеством проверок и будьте готовы отменить изменения, если это будет необходимо.

Задания

1. Какие изменения в вашей сети вы можете прогнозировать в будущем? Выберите одно из них и создайте план его выполнения с минимальным влиянием на пользователей.
2. Теперь попытайтесь внести в этот план возможность мгновенной отмены.
3. Если бы вам потребовалось разделить свою сеть, какие службы вам пришлось бы воспроизвести и как бы вы перевели людей с одной сети и набора служб на другую? Рассмотрите каждую службу подробно.
4. Можете ли вы назвать какие-либо изменения, которых вы могли избежать? Как бы вы могли их избежать?

5. Подумайте об изменении службы, которое действительно нужно в вашей среде. Будете ли вы выполнять поэтапное распространение или мгновенный переход? Почему?
6. Представьте, что ваша IT-группа переводила бы всех сотрудников с офисной АТС на IP-телефонию (VoIP). Создайте схему этого процесса с вертикальным подходом, а затем с горизонтальным.
7. Был бы комбинированный подход в предыдущем вопросе более удобным, чем жесткая вертикальная или горизонтальная модель? Если да, то объясните, почему.

Глава 20

Технические перерывы

Если бы вам потребовалось отключить целый вычислительный центр, выполнить масштабное техническое обслуживание, а затем снова ввести его в эксплуатацию, вы смогли бы провести это мероприятие? Некоторым компаниям удается делать это ежеквартально или ежегодно. Системные администраторы откладывают до такого перерыва задачи, которые требуют прерывания обслуживания, например модернизацию оборудования, замену запчастей или изменения сети. Иногда время для рискованных изменений выделяется еженедельно, чтобы свести все отключения в один интервал, когда пользователи будут затронуты минимально. Иногда мы вынуждены делать это из-за мероприятий технического характера, например строительных работ, модернизации системы электропитания или охлаждения либо перемещения офиса. Порой нам это требуется по причине аварии, например из-за сбоя системы охлаждения. В данной главе рассмотрен подход к управлению такими серьезными запланированными отключениями. По ходу изложения будут даваться советы, полезные в менее критических ситуациях. Такие проекты требуют более тщательного планирования, очень четкого исполнения и значительно бóльших объемов тестирования. Мы называем это **подходом руководителя полета**, по аналогии с ролью руководителя полета при запуске космических аппаратов НАСА[1].

Несмотря на то что большинство людей делают уборку в своих домах еженедельно или ежемесячно, ежегодная генеральная уборка определенно является полезной. Точно так же и сетям иногда требуется серьезная уборка. Системы охлаждения нужно отключать, сливать из них воду, очищать их и наполнять заново. Беспорядочные узлы проводов начинают затруднять эффективную работу, и иногда их нужно распутывать. Большие объемы данных должны распределяться между файловыми серверами для оптимизации работы пользователей или просто для предоставления пространства под расширение. Усовершенствования, которые включают множество изменений, можно выполнить гораздо эффективнее, если все пользователи согласятся на долгий перерыв в работе. Подход руководителя полета определяет деятельность до перерыва, во время выполнения и после него (табл. 20.1).

В некоторых компаниях стараются назначить регулярные технические перерывы для обслуживания важнейших систем и сетей для лучшей доступности

[1] Автором приемов, описанных в данной главе, и применяемой здесь терминологии является Пол Эванс (Paul Evans), внимательно следивший за ходом космической программы. Первые руководители полетов носили жилеты, такие как у руководителя полета в фильме «Аполлон-13». Терминология помогла каждому запомнить, что роль системного администратора в жилете отличается от обычной.

Таблица 20.1. Три этапа технического перерыва

Этап	Действие
Подготовка	• Запланируйте время перерыва • Выберите руководителя полета • Подготовьте предложения изменений • Создайте общий план
Выполнение	• Отключите доступ • Выполните последовательность отключений • Выполните план • Выполните проверку
Разрешение	• Объявите о завершении • Включите доступ • Обеспечьте видимое присутствие • Будьте готовы к проблемам

во время нормальной работы. В зависимости от размера компании это может быть один вечер и ночь в месяц или время с вечера пятницы до утра понедельника раз в квартал. Эти технические перерывы всегда требуют очень интенсивной работы, поэтому при принятии решения об их назначении оценивайте как возможности и самочувствие системных администраторов, так и влияние на компанию.

Системные администраторы часто предпочитают технические перерывы, в течение которых они могут отключить все системы и службы, потому что это снижает сложность обслуживания и упрощает тестирование. Трудно сменить шины, когда машина едет по дороге. Например, при переводе служб электронной почты на новую систему вам потребуется перенести существующие почтовые ящики, а также перевести цепочку доставки входящей почты. Перенести существующие почтовые ящики во время доставки новой почты, обеспечивая при этом целостность информации, – очень сложная проблема. Однако, если во время перевода вы сможете отключить серверы электронной почты, это станет гораздо проще. Кроме того, гораздо легче проверить, что система работает правильно, до того, как вы включите доставку почты и доступ на чтение, чем разбираться с отклоненной или недоставленной электронной почтой работающего пользователя, если что-то пошло не так.

Однако вам потребуется представить этот принцип с точки зрения выгоды для компании, а не облегчения жизни системного администратора. Вам придется пообещать лучшую доступность службы в остальное время. Вам потребуется заблаговременное планирование: если у вас один технический перерыв в квартал, то вам нужно обеспечить, чтобы работа, выполненная в этом квартале, позволила вам продержаться до следующего квартала и вам не потребовалось бы снова отключать систему. Чтобы это работало, все сотрудники группы должны обеспечить высокую доступность своих систем. Вам также следует разработать метрику для оценки ваших заявлений о более высокой доступности по сравнению со временем до разрешения на запланированные технические перерывы (мониторинг для проверки уровней доступности более подробно рассмотрен в главе 22).

Во многих компаниях не согласятся на долгие запланированные отключения для технического обслуживания. В данном случае нужно представить альтернативный план, в котором объясняются результаты разрешения отключений и показывается, что на самом деле они выгодны пользователям, а не системным администраторам. Одно долгое отключение беспокоит пользователей гораздо меньше, чем много коротких (Limoncelli et al. 1997).

В других компаниях длительные отключения невозможны из-за особенностей бизнеса. К данной категории относятся компании электронной коммерции и интернет-провайдеры. Этим компаниям требуется обеспечивать высокую доступность для своих пользователей, которые обычно находятся вне компании и с которыми трудно связаться. Однако им все-таки нужны технические перерывы. В конце данной главы рассмотрено, как принципы, изложенные в ней, применяются для компаний высокой доступности.

Эти подходы также актуальны для одиночных, крупных и запланированных перерывов в работе, например, при перемещении компании в новое здание.

20.1. Основы

По определению **технический перерыв** – это короткий промежуток времени, в который должно быть выполнено большое количество работы по обслуживанию систем; он очень неудобен для всей компании, поэтому его время должно определяться совместно с пользователями. Группа системных администраторов должна выполнять различные задачи, и эта работа должна координироваться руководителем полета.

Некоторые основы, необходимые для достижения успеха в этом деле, – это координация определения времени технического перерыва, создания общего плана всего изменения, организация подготовительной работы, общение со всеми затрагиваемыми пользователями и выполнение полного теста системы после завершения работы. В данной главе мы рассмотрим роль и действия руководителя полета и механизмы обеспечения работы во время технического перерыва, связанные с этими элементами.

20.1.1. Планирование времени

При планировании периодических технических перерывов вы должны работать с остальной компанией для координации дат. В частности, вам почти наверняка потребуется избегать дней в конце месяца, в конце квартала и в конце финансового года, чтобы группа продаж могла вводить срочные заказы, а бухгалтерия – предоставлять финансовую отчетность за этот период. Вам также потребуется избегать дней выпуска продуктов, если это актуально для вашего бизнеса. В университетах есть другие ограничения в течение учебного года. В некоторых отраслях, например в производстве игрушек и открыток, могут быть сезонные ограничения. Вы должны заблаговременно установить и опубликовать график, лучше всего более чем на год, чтобы остальная часть компании могла планировать свою деятельность в соответствии с этими датами. Если вы участвуете в создании новой компании, сделайте регулярно планируемые технические перерывы элементом культуры компании.

Пример: планирование времени технического перерыва

В средней компании по разработке программного обеспечения ежеквартальные технические перерывы не должны были попадать на различные дни непосредственно до и после запланированных дат выпуска, которые чаще всего были три раза в год, так как инженерному отделу и отделу операторов требовалась работоспособность систем для осуществления выпуска. Дней, предшествующих основной выставке продуктов компании, и дней во время нее нужно было избегать, потому что инженерный отдел обычно создавал для выставки новые альфа-версии, а презентации на выставке могли полагаться на оборудование офиса. Дней в конце месяца, конце квартала и конце года, когда финансовому отделу и отделу поддержки продаж требовалась полная доступность ввода цифровых данных, тоже нужно было избегать. События, которые могли вызвать пик звонков в службу поддержки пользователей, например представление специального продукта, должны были координироваться с отключениями систем, хотя обычно они назначались после того, как устанавливались технические перерывы.

Как вы можете видеть, выделение свободного времени было трудной задачей. Однако графики техобслуживания устанавливались по крайней мере за год и хорошо освещались, чтобы остальная часть компании могла планировать свои действия в соответствии с ними.

Когда даты были установлены, за 6 недель до каждого перерыва начинали отправляться еженедельные напоминания с дополнительными замечаниями на последней неделе. В конце каждого сообщения располагался график всех последующих технических перерывов на все время, на которое они были установлены.

В сообщении о техническом перерыве выделялись главные из запланированных мероприятия, чтобы показать выгодность отключения для компании в целом, например о вводе в эксплуатацию нового вычислительного центра или модернизации инфраструктуры электронной почты. Это помогало пользователям понимать выгоду, которую они получали от прерывания обслуживания.

К несчастью для группы системных администраторов, остальная часть компании считала выходные дни, в которые проводилось техобслуживание, лучшим временем для корпоративных пикников и других мероприятий, потому что никто не чувствовал себя обязанным работать в это время – конечно, кроме системных администраторов.

Такова жизнь.

Еженедельные технические перерывы в Lumeta

Получить разрешение на периодическое запланированное отключение может быть трудно. Поэтому для Тома было важно начать такую традицию при создании Lumeta, а не пытаться бороться за это впоследствии. Он выгодно представил эту идею, объяснив, что, пока компания будет молодой, рост и непостоянство инфраструктуры будут очень значитель-

ными. Вместо того чтобы беспокоить всех постоянными требованиями отключений, он обещал назначать все запланированные отключения на вечер в среду после 17 часов. После такого объяснения реакция была в высшей степени позитивной. Из-за того что он воспользовался фразой «пока компания будет молодой», а не конкретным временным периодом, он смог поддерживать эту традицию по вечерам в среду годами.

В первые несколько месяцев Том всегда придумывал веские причины для отключения систем в среду вечером, чтобы это стало частью корпоративной культуры. Перезагрузка важного сервера была достаточной причиной, чтобы заставить людей уйти домой, несмотря на то что занимала она лишь несколько минут. Подразделения планировали свой график, учитывая вечер среды и зная, что он не был подходящим временем для задержек на работе и предельных сроков выполнения. При этом Том обеспечил впечатление гибкости, откладывая технический перерыв по малейшей просьбе. Люди привыкли проводить время по вечерам в среду со своими семьями.

Как только инфраструктура приобрела стабильность, такие технические перерывы стали требоваться редко. Люди больше жаловались тогда, когда сообщение «на этой неделе технического перерыва не будет» приходило ближе к вечеру в среду. Том установил правило, чтобы каждое мероприятие по техобслуживанию, которое требовало заметного отключения, объявлялось вечером в понедельник, а отсутствие объявления означало отсутствие перерыва. Несмотря на то что в этом не было необходимости, еженедельная отправка электронного письма, объявляющего об отсутствии заметных пользователям отключений, не позволяла группе Тома стать незаметной и поддерживала осведомленность людей о возможных отключениях в среду вечером. Для этих объявлений применялось различное форматирование, и люди обращали на них внимание, когда отключение действительно должно было состояться.

20.1.2. Планирование

Как и в случае с любым запланированным обслуживанием важных систем, задачи должны планироваться людьми, которые их выполняют, чтобы выполнение задачи во время перерыва не приводило к нестандартному мышлению или решению проблем. Непредвиденных событий быть не должно, только запланированные.

Однако планирование технического перерыва также имеет еще один аспект. Из-за того что технические перерывы происходят только время от времени, системные администраторы должны заблаговременно планировать их с достаточным запасом времени, чтобы иметь время на оценку, подачу и одобрение заказов на покупку, а также обеспечить, чтобы все новое оборудование было доставлено приблизительно за неделю до технического перерыва. Время доставки некоторого оборудования может составлять 6 недель или более, и это значит, что нужно начинать планировать следующий технический перерыв практически сразу после завершения предыдущего.

20.1.3. Руководство

Руководитель полета отвечает за создание объявлений, обеспечение их своевременной рассылки, планирование графика полученных запросов на выполнение работ на основе взаимного влияния требований и необходимого персонала, принятие решений о любых отключениях в рамках технического перерыва, мониторинг выполнения задач во время технического перерыва, обеспечение правильного прохождения проверки и сообщение о состоянии дел остальной части компании в конце перерыва. Человек, играющий роль руководителя полета, должен быть старшим системным администратором, который может оценить предложения по выполнению работ от других сотрудников группы системного администрирования и заметить зависимости и эффекты, которые могли быть упущены. Кроме того, руководитель полета должен иметь возможность принимать решения о том, соответствует ли уровень риска некоторых более важных задач, затрагивающих инфраструктуру, их необходимости. Этот человек должен иметь хорошее представление о компании, понимать смысл всей работы – и хорошо выглядеть в жилете.

Кроме того, руководитель полета не может выполнять во время технического перерыва никакой технической работы. Обычно руководитель полета является членом группы из нескольких человек: остальные сотрудники группы выполняют работу, за которую этот человек отвечает. Из-за требований к навыкам руководитель полета обычно не является менеджером, если это не бывший старший системный администратор, недавно повышенный до менеджера.

В зависимости от структуры группы системных администраторов, можно выделить несколько человек, из которых каждый раз выбирается новый руководитель полета. В рассмотренной выше средней компании по разработке программного обеспечения большинство из 60 системных администраторов отвечали за одно подразделение компании. Около 10 системных администраторов входили в состав отдела базовых служб и отвечали за центральные службы и инфраструктуру, общие для всей компании, например за безопасность, сети, электронную почту, печать и службы имен. Системные администраторы в этом подразделении предоставляли услуги каждому из остальных подразделений бизнеса и поэтому имели хорошее представление о корпоративной инфраструктуре и о том, как подразделения бизнеса строились на ее основе. Обычно руководитель полета был сотрудником этого подразделения и уже проработал в компании некоторое время.

Также требовалось учитывать другие факторы, например каковы отношения этого человека с остальными системными администраторами, будет ли он достаточно строгим в соблюдении сроков выполнения, но способным принять правильное решение о том, где можно сделать исключение, и как будет действовать под давлением или когда устанет. В ходе нашего применения этого подхода мы обнаружили, что некоторые прекрасные старшие системные администраторы выполняли обязанности руководителя полета один раз и больше не хотели этим заниматься. В дальнейшем нам пришлось быть более внимательными, чтобы иметь уверенность в том, что у выбранного нами руководителя полета будет желание выполнять эту работу.

20.1.4. Управление предложениями изменений

Все предложения изменений должны быть поданы за неделю до технического перерыва. Хороший способ управлять этим процессом – подавать эти предложения по сети в область с контролем версий. Каждый системный администратор редактирует документы в директории со своим именем. Документы предоставляют всю необходимую информацию. За неделю до изменения эта область с контролем версий блокируется, и все последующие запросы на изменения в документы должны делаться через руководителя полета. Форма предложения изменения должна отвечать, по крайней мере, на следующие вопросы:

- Какие изменения планируется внести?
- На каких машинах вы будете работать?
- Какие условия должны быть выполнены до технического перерыва и каковы сроки их выполнения?
- Что должно работать, чтобы изменение было успешным?
- Что будет затронуто изменением?
- Кто выполняет работу?
- Сколько времени непосредственной работы займет изменение, сколько времени на него будет выделено, включая тестирование, и сколько потребуется помощников?
- Каковы процедуры тестирования? Какое оборудование для них требуется?
- Какова процедура отмены и сколько времени она займет?

20.1.4.1. Предложение изменения: пример 1

- *Какое изменение планируется выполнить?*

  Обновить программу сервера аутентификации SecurID с версии 1.4 до версии 2.1.

- *На каких машинах вы будете работать?*

  `tsunayoshi` и `shingen`.

- *Какие условия должны быть выполнены до технического перерыва и каковы сроки их выполнения?*

  Программа и лицензионные ключи версии 2.1 должны быть доставлены разработчиком к 14 сентября. В последний вечер перед перерывом нужно сделать резервные копии.

- *Зависимости от других систем?*

  Сеть, служба командной строки и службы внутренней аутентификации (NIS).

- *Что будет затронуто изменением?*

  Весь удаленный доступ и доступ к защищенным областям, который требует аутентификации по маркерам.

- *Сколько времени займет изменение?*

  Время: 3 ч работы, 3 ч выделено.

- *Кто выполняет работу?*

  Джейн Смит.
- *Дополнительные помощники?*

  Нет.
- *Процедура тестирования?*

  Попытаться набрать номер, установить VPN-соединение, соединиться через ISDN и осуществить доступ к каждой защищенной области. Проверить создание нового пользователя, удаление пользователя и изменение атрибутов пользователя; убедиться, что каждое изменение прошло успешно.
- *Необходимое оборудование?*

  Ноутбук с модемом и программой VPN, аналоговая линия, учетная запись внешнего интернет-провайдера, ISDN-модем и интерфейс базового уровня (Base Rate Interface – BRI).
- *Процедура отмены?*

  Установка нового программного обеспечения в параллельную директорию и копирование базы данных в новое место. Не удалять старую программу и базу данных, пока не пройдет неделя успешной работы. Для отмены (занимает 5 мин плюс тестирование) нужно изменить ссылки, чтобы они указывали на старую программу.

20.1.4.2. Предложение изменения: пример 2

- *Какие изменения планируется выполнить?*

  Переместить /home/de105 и /db/gene237 с `anaconda` на `anachronism`.
- *На каких машинах вы будете работать?*

  `anaconda`, `anachronism` и `shingen`.
- *Какие условия должны быть выполнены до технического перерыва и каковы сроки их выполнения?*

  Дополнительные диски для `anachronism` должны быть доставлены 17 сентября и установлены к 21 сентября. В последний вечер перед перерывом нужно сделать резервные копии.
- *Зависимость от других систем?*

  Сеть, служба командной строки и службы внутренней аутентификации (NIS).
- *Что будет затронуто изменением?*

  Сетевой трафик в сети 172.29.100.x, все учетные записи с домашними директориями в /home/de105 и доступ к базе данных /db/gene237.
- *Сколько времени займет изменение?*

  Время: 1 ч работы, 12 ч выделено.
- *Кто выполняет работу?*

  Грег Джонс.
- *Дополнительные помощники?*

  Нет.
- *Процедура тестирования?*

  Попытаться подключиться к этим директориям с некоторых подходящих узлов, загрузиться на рабочей станции под учетной записью с домашней

директорией в /home/de105, убедиться, что она работает, создать базу данных gene, проверить на ошибки, запустить скрипт тестового доступа к базе данных из /usr/local/tests/gene/access-test.

- *Необходимое оборудование?*

  Доступ к узлу, не принадлежащему системному администратору.

- *Процедура отмены?*

  Старые данные удаляются после успешного тестирования, изменить указанные местоположения директорий обратно на старые значения и перестроить таблицы. Отмена занимает 10 мин.

20.1.5. Разработка общего плана

За неделю до технического перерыва руководитель полета блокирует предложения изменений и начинает работать над общим планом, который учитывает все условия, а также выделенное время и время работы из предложений изменений. В результате получается набор таблиц, по одной на человека, которые показывают, какую задачу должен выполнить человек и в какое время, а также определяют координатора для этой задачи. В общем плане перечислены все задачи, выполняемые в течение всего времени перерыва, исполнители, руководитель группы и взаимосвязи. Кроме того, в общем плане учитывается полное тестирование всей системы после завершения работы.

Если предложений изменений слишком много, руководитель полета обнаружит, что их планирование по времени вызывает недопустимое количество конфликтов в плане либо доступности машин, либо необходимого персонала. Вам потребуется запас в графике на случай, если дела пойдут не так. Трудные решения о том, какие проекты должны быть первыми, а какие могут подождать, должны приниматься заблаговременно, а не во время работы, когда что-то требует слишком много времени и нарушает график, а все уже устали и напряжены. Руководитель полета принимает решения об отмене некоторых предложений изменений и помогает вовлеченным сторонам выбрать лучший для компании вариант.

Пример: шаблон общего плана

После того как мы провели несколько технических перерывов, мы выработали формулу, которая была нам очень полезна. С системами, от которых зависела деятельность большинства людей, мы работали вечером в пятницу. Первым, что мы обновляли или изменяли, была сеть. Далее по списку шла служба консоли, а затем – серверы аутентификации. В ходе этих работ все остальные системные администраторы помогали с задачами по оборудованию, такими как модернизация памяти, дисков или процессоров, замена сломанного оборудования или перемещение оборудования между вычислительными центрами. Последнее, что делалось вечером в пятницу, – начиналось перемещение данных, чтобы его можно было завершить за ночь.

Затем оставшиеся задачи планировались на субботу, а некоторые сотрудники в промежутках между своими задачами назначались в помощь другим. Воскресенье было выделено на полное тестирование и отладку всей системы, поскольку важность тестирования была очень высока.

20.1.6. Отключение доступа

Самая первая задача в ходе технического перерыва – отключить или предотвратить доступ к системе и предоставить оповещение о том, что идет технический перерыв. В зависимости от характера компании и доступных средств данный процесс может включать:

- Размещение на всех входных дверях комплекса зданий заметных объявлений с указанием времени технического перерыва.
- Отключение всего удаленного доступа к системе: через VPN, модемные пулы, выделенные линии или беспроводного.
- Объявление по системе оповещения комплекса зданий, напоминающее всем, что системы скоро будут отключены.
- Изменение сообщения ящика голосовой почты службы поддержки, чтобы в нем объявлялось о техническом перерыве и упоминалось, когда будет восстановлено нормальное обслуживание.

Эти меры снижают возможность того, что люди будут пытаться пользоваться системами во время технического перерыва, – ведь это может вызвать нарушение целостности, порчу или потерю их данных. Это также снижает вероятность того, что человеку с пейджером, принимающим сообщения службы поддержки, придется на них отвечать, что сеть не работает.

Перед началом технического перерыва мы рекомендуем вам проверить консольные серверы и другие средства, которыми вы будете пользоваться во время перерыва. Некоторые из этих средств используются достаточно редко, поэтому никто может не заметить, что они не работают. Убедитесь, что у вас есть достаточно времени, чтобы исправить все неработающее до начала технического перерыва.

20.1.7. Обеспечение механизмов и координации

Некоторые ключевые технологии обеспечивают плавное течение технического перерыва. Эти аспекты полезны для технических перерывов и критически важны для их успешного проведения.

20.1.7.1. Последовательность отключения/загрузки

В большинстве компаний некоторые системы или группы систем должны быть доступны другим системам для нормального отключения или загрузки. Машина, которая пытается загрузиться, когда недоступны машины и службы, используемые ею, не сможет нормально загрузиться. Обычно машина загрузится, но не сможет запустить некоторые программы, которые она обычно запускает при загрузке. Эти программы могут быть службами, которые используют другие, или программы, запускаемые локально на чьей-то рабочей станции. В любом случае машина не будет работать правильно, причем может быть непонятно, почему. При отключении машины ей может требоваться связь с используемыми файловыми серверами, серверами лицензий или баз данных, чтобы правильно завершить соединение. Если машина не способна связаться с этими серверами, она может надолго зависнуть, пытаясь связаться с ним до завершения процесса отключения. Важно понимать и отслеживать взаимосвязи машин в ходе загруз-

ки и отключения. Вы ведь не хотите, чтобы вам пришлось впервые выяснять их, когда в серверной неожиданно отключится электропитание.

Наиболее важные системы, такие как консольные серверы, серверы аутентификации, машины службы имен, серверы лицензий, серверы приложений и серверы данных, обычно нужно загружать до вычислительных серверов и рабочих станций. Кроме того, следует иметь в виду взаимосвязи между критическими серверами. Очень важно иметь список последовательности загрузки всех машин вычислительного центра с одной или несколькими машинами на каждом этапе. Обычно на первой паре этапов будет мало машин, может быть по одной, но на последующих этапах машин будет много. Все машины вычислительного центра должны загружаться до любых машин, не принадлежащих вычислительному центру, потому что ни одна машина из вычислительного центра не должна полагаться на какую-либо машину вне вычислительного центра (см. раздел 5.1.7).

В одной компании создали список отключения/загрузки, представленный в табл. 20.2. Последовательность отключения обычно очень близка к обратному

Таблица 20.2. Шаблон последовательности загрузки

Этап	Функция	Причина
1	Консольный сервер	Позволяет системным администраторам наблюдать за другими серверами во время загрузками
2	Главный сервер аутентификации	Дополнительные серверы аутентификации связываются с главным при загрузке
	Главный сервер имен	Дополнительные серверы имен связываются с главным
3	Дополнительные серверы аутентификации	• Позволяют системным администраторам входить в систему на других серверах после их загрузки • UNIX-узлы связываются с серверами NIS при загрузке • Не зависят ни от чего, кроме главного сервера аутентификации
	Дополнительные серверы имен	• Почти все службы используют службу имен • Не зависят ни от чего, кроме главного сервера имен
4	Серверы данных	• Приложения и домашние директории зависят от серверов данных • Большинство других машин зависят от серверов данных • Зависят от службы имен
	Серверы конфигурации сети	Зависят от службы имен
	Серверы логов	Зависят от службы имен
	Серверы директорий	Зависят от службы имен

Таблица 20.2. Шаблон последовательности загрузки (окончание)

Этап	Функция	Причина
5	Серверы печати	Зависят от службы имен и серверов логов
	Серверы лицензий	Зависят от службы имен, серверов данных и серверов логов
	Межсетевые экраны	Зависят от серверов логов
	Удаленный доступ	Зависит от службы аутентификации, службы имен, службы логов
	Служба электронной почты	Зависит от службы имен, службы логов и службы директорий, а также серверов данных
6	Все остальные серверы	Зависят от ранее загруженных серверов и не зависят друг от друга
7	Рабочие станции	Зависят от серверов

порядку загрузки, если не точно его повторяет. Может иметься пара несущественных отличий.

Последовательность отключения – важнейший компонент начальной работы во время технического перерыва. Машины, с которыми работают в начале технического перерыва, обычно имеют много зависимых объектов, поэтому любая машина, которую нужно отключить для обслуживания/обновления оборудования или перемещения, должна быть отключена до того, как начнется работа на критических машинах. Важно выключать машины в правильном порядке, чтобы избежать траты времени на повторное включение машин для нормального отключения других машин. Последовательность загрузки также важна для полного тестирования системы, выполняемого в конце технического перерыва.

Последовательность выключения может быть частью более крупной процедуры аварийного отключения питания. Аварийное отключение питания – это план решений и действий для экстренных случаев, требующих быстрых действий. В частности, может требоваться действовать быстрее, потому что это одобряет руководство. Считайте это предварительной подготовкой решений для дальнейшего исполнения. В плане аварийного отключения питания должны быть перечислены ситуации, в которых требуется его выполнение, – пожар, наводнение, перегрев без ответа от оборудования – и даны указания, как проверять эти ситуации. Дерево решений является наилучшим способом записи этой информации. Кроме того, в плане аварийного отключения питания должны даваться указания о том, как переводить службы в другие вычислительные центры, кого уведомлять и т. д. Документируйте процессы для ситуаций, когда нужно копировать критические данные из вычислительного центра и когда это не нужно. Наконец, в плане должна присутствовать последовательность отключения машин. В случае перегрева нужно документировать способы отключения некоторых машин или их перевода в режим потребления меньшей мощности, чтобы они создавали меньше тепла, работая медленнее, но все же предоставляя службы. Эти меры должны быть документированы таким образом, чтобы они могли быть выполнены любым системным администратором группы. Наличие такого плана поможет вам сохранить оборудование, службы и доходы.

Экстренное применение последовательности отключения

Одна компания посчитала, что последовательность отключения была полезна даже для незапланированных отключений. В вычислительном центре был фальшпол с обычным беспорядком воздуховодов кондиционирования, электрических распределительных щитов и сетевых кабелей, скрытых от взгляда. Как-то раз в пятницу один системный администратор устанавливал новую машину и ему потребовалось провести под полом кабель. Он достал инструмент, поднял несколько блоков и увидел, что под полом была вода, уже подходившая к некоторым электрическим распределительным щитам. Системный администратор, обнаруживший воду, оповестил свое руководство – по радиосвязи, – и после быстрого принятия решения последовало радиосообщение для системных администраторов, а затем быстрая передача для всей компании. Далее был озвучен список отключения и «руководитель полета» следующего технического перерыва провел репетицию отключения всего оборудования в серверной. Все прошло гладко из-за наличия списка отключения.

Фактически руководство предпочло упорядоченное отключение моментальному экстренному отключению питания в помещении, зная о наличии актуального списка отключения и имея оценку времени, за которое вода достигнет электрических цепей. Без списка руководству пришлось бы отключить питание во всем помещении, что могло иметь разрушительные последствия.

20.1.7.2. KBM и служба консоли

Два элемента вычислительных центра, которые облегчают управление, – это коммутаторы KBM и последовательные консольные серверы. Оба они могут быть полезны для облегчения работы во время технических перерывов за счет предоставления возможности удаленного доступа к консоли машины.

Коммутатор KBM (Keyboard Video and Mouse – клавиатура, видео и мышь) позволяет нескольким компьютерам совместно использовать одни и те же клавиатуру, монитор и мышь. Коммутатор KBM экономит место в вычислительном центре – мониторы и клавиатуры занимают много места – и делает доступ более удобным, на самом деле более сложные системы доступа к консоли могут предоставить доступ из любой точки сети.

Последовательный консольный сервер подключает устройства с последовательными консолями – системы без видеовыхода, например сетевые маршрутизаторы, коммутаторы и многие UNIX-серверы, – к одному центральному устройству с несколькими последовательными входами. Подключившись к консольному серверу, пользователь затем может подключиться к последовательным консолям других устройств. Все оборудование серверной, которое поддерживает последовательные консоли, должно быть подключено к какому-либо консольному концентратору, например сетевому терминальному серверу.

Значительная часть работы во время технического перерыва требует прямого доступа к консоли. Применение устройств с доступом к консоли позволяет лю-

дям трудиться на своих рабочих местах, тем самым устраняя необходимость координировать доступ большого числа людей к очень ограниченному количеству мониторов в серверной или траты места, электроэнергии и ресурсов охлаждения на дополнительные мониторы. Кроме того, некоторым системным администраторам удобнее работать со своих рабочих мест, где есть подготовительные записи и справочные материалы.

20.1.7.3. Радиостанции

Из-за плотного графика технического перерыва, большого количества взаимосвязей и возможной непредсказуемости работы по системному администрированию все системные администраторы должны иметь возможность сообщать руководителю полета о выполнении задачи, а перед началом выполнения новой задачи – убедиться, что все необходимые предыдущие этапы были завершены. Мы рекомендуем использовать для связи в группе портативные радиостанции. Вместо того чтобы искать руководителя полета, системный администратор может просто вызвать его по рации. Таким же образом руководитель полета может связываться с системными администраторами для выяснения состояния работы, а руководители групп и их сотрудники могут находить друг друга и общаться по рации. Если системным администраторам потребуется дополнительная помощь, они также могут запросить ее по рации. Есть несколько радиоканалов, и длинные разговоры можно переводить на другой канал, чтобы основной канал оставался свободным. Кроме того, радиостанции необходимы для тестирования всей системы в конце технического перерыва (см. раздел 20.1.9).

Удобно пользоваться радиостанциями, сотовыми телефонами или какой-либо другой эффективной формой двусторонней связи для переговоров между системными администраторами внутри комплекса зданий. Мы рекомендуем пользоваться радиостанциями, потому что разговор не нужно оплачивать и обычно в обстановке вычислительного центра они работают лучше сотовых телефонов. Помните: все, что передается в эфир, может быть подслушано другими, поэтому важную информацию, например пароли, нельзя передавать по рации, сотовому телефону или пейджеру.

Есть несколько вариантов выбора радиостанций, и предпочтительный для вас вариант зависит от площади покрытия, типа местности на этой площади, доступности и уровня ваших навыков. Удобно иметь портативные радиостанции с несколькими каналами, или частотами, чтобы долгие разговоры можно было переключить на другой канал, а основной канал оставить открытым для других (табл. 20.3).

Радиосвязь прямой видимости является самой распространенной и обычно имеет максимальное расстояние связи около 25 км, в зависимости от окружающей местности и зданий. Продавец должен иметь возможность предоставить вам одну или несколько частот и набор радиостанций, использующих эти частоты. Убедитесь, что продавец знает, что вам нужны радиостанции для работы в зданиях и на необходимых вам расстояниях.

Для увеличения дальности передачи радиосигнала могут использоваться ретрансляторы, которые особенно полезны, если горы между зданиями комплекса блокируют связь прямой видимости. В любом случае может быть полезно наличие ретранслятора и антенны на крыше одного из зданий, чтобы ретранслятор использовался по крайней мере на основном канале. Обычно такая конфигурация требует, чтобы оборудование устанавливалось и эксплуатировалось кем-либо с лицензией радиолюбителя. Изучите ваше местное законодательство.

Таблица 20.3. Сравнение технологий радиосвязи

Тип	Требования	Преимущества	Недостатки
Прямая видимость	• Лицензия на частоту[1] • Передача через стены	Простота	• Ограниченное расстояние • Не передает через горы
Ретранслятор	• Лицензия на частоту • Лицензия радиооператора	• Большее расстояние • Ретранслятор на горе позволяет связываться через горы	• Сложнее в эксплуатации • Требует специальных навыков
Сотовая связь	Доступность обслуживания	• Простота • Большие расстояния • Не зависит от местности • Меньший вес аппарата	• Более высокая стоимость • Доступна только в зоне покрытия сетей сотовых операторов • Контракты могут ограничивать возможности • Многоканальная связь может быть недоступна

[1] В свободной продаже есть рации с нелицензируемым диапазоном до 64 каналов. – *Примеч. науч. ред.*

Некоторые операторы сотовой связи предоставляют услугу громкой связи на сотовых телефонах, чтобы они работали подобно рациям. Эта услуга будет доступна везде, где работают телефоны. Оператор должен предоставить карты покрытия сети. Компания должна предоставить каждому системному администратору сотовый телефон с такой услугой. Преимущество этого подхода в том, что системный администратор должен носить с собой только телефон, а не телефон и рацию. Это может быть быстрым и удобным способом обеспечить радиосвязью новую группу, но может и оказаться нереальным, если потребуется, чтобы все перешли на одного оператора сотовой связи.

Если в вашем вычислительном центре радиостанции не работают или работают плохо из-за радиочастотного экранирования, разместите в конце каждого ряда дополнительный аппарат внутренней телефонной связи с длинным проводом, изображенный на рис. 6.14. Таким образом, системные администраторы в вычислительном центре все-таки смогут связываться друг с другом. В худшем случае они смогут выйти из вычислительного центра, связаться с кем-то по рации и договориться, чтобы этот человек позвонил на конкретный телефон внутри вычислительного центра.

Конференц-связь, при которой каждый может позвонить и присоединиться, помимо всех преимуществ радиосвязи позволяет людям звонить и участвовать в процессе из любой точки мира. Наличие постоянного номера для конференц-связи, принадлежащего группе, упрощает его запоминание и может сэкономить критические минуты в экстренных случаях.

Связь в экстренных случаях

Во время атак 11 сентября 2001 года один крупный новостной веб-сайт был перегружен. Запрос и получение номера конференц-связи требовали много времени, а получение указаний по набору номера ключевыми участниками – еще больше.

20.1.8. Предельные сроки завершения изменения

Критическая роль руководителя полета – отслеживать ход выполнения различных задач и решать, когда нужно прервать выполнение конкретной задачи и перейти к плану по ее отмене. Для задачи общего характера, с которой не связаны никакие другие задачи, а выполняющие ее люди не имеют других заданий, в случае технического перерыва в выходные таким временем может быть 23.00 в субботу минус время, необходимое для выполнения плана отмены. Кроме того, руководитель полета должен учитывать уровень производительности группы системных администраторов. Если ее сотрудники раздражены и измотаны, руководитель полета может разрешить им сделать перерыв или приказать начать выполнять план отмены раньше, если они не смогут выполнить его так же продуктивно, как в случае хорошего самочувствия.

Если от работы системы или службы зависят другие задачи, то особенно важно предварительно определить предельный срок выполнения задачи. Например, если обновление консольного сервера идет плохо, оно может затронуть время, обычно выделяемое на перемещение крупных файлов данных. Как только вы перейдете временную границу, цепная реакция взаимосвязей может привести к полной катастрофе, которую можно будет исправить только во время следующего технического перерыва, возможно, еще через неделю. Запишите, какие другие задачи обычно планируются близко к техническому перерыву или во время него, чтобы вы могли определить, когда начать отмену проблемного изменения.

20.1.9. Полное тестирование системы

Завершающий этап технического перерыва – это полное тестирование системы. Если перерыв короткий, вам может потребоваться протестировать лишь немногие компоненты, над которыми вы работали. Однако, если вы потратили свой технический перерыв, который длился все выходные, на разбор различных сложных элементов аппаратуры, а затем на их обратное объединение в ограниченных временных рамках, вы должны выделить все воскресенье на тестирование системы.

Воскресное тестирование системы начинается с отключения всех машин в вычислительном центре, чтобы затем вы смогли выполнить вашу последовательность загрузки. Назначьте человека к каждой машине в вашем списке загрузки. Руководитель полета объявляет этапы отключения по рации, и каждый человек отвечает, когда вверенная ему машина будет полностью отключена. Когда все машины на текущем этапе будут отключены, руководитель полета объявляет следующий этап. Когда все будет отключено, порядок меняется на обратный и руководитель полета проводит всех по этапам загрузки. Если на любом из

этапов с какой-либо машиной происходят проблемы, вся последовательность приостанавливается, пока неполадки не будут обнаружены и исправлены. Каждый человек, назначенный к машине, отвечает за то, чтобы она была полностью отключена, прежде чем он об этом сообщит, и чтобы все службы были корректно запущены, прежде чем он доложит о том, что машина загружена и работает.

Наконец, когда все машины в вычислительном центре будут успешно загружены в правильном порядке, руководитель полета разделяет системных администраторов на группы. Каждая группа имеет руководителя и область ответственности в одном из зданий комплекса. Группам даются указания о том, за какие машины они отвечают и какие тесты на них нужно выполнить. Эти указания всегда включают перезагрузку каждой машины, чтобы убедиться в том, что она работает нормально. Тесты также могут включать вход в систему, проверку конкретной службы или попытку запустить то или иное приложение. У каждого сотрудника группы должно быть несколько цветных наклеек, чтобы после завершения работы отмечать офисы и рабочие места как проверенные и пригодные для работы. Кроме того, у системных администраторов должны быть наклейки другого цвета, чтобы отмечать рабочие места, на которых присутствуют проблемы. По завершении работы в своей области группа направляется в другую область, чтобы помочь другой группе выполнить свою задачу, – и так до завершения всего комплекса зданий.

Одновременно руководитель полета и старшие системные администраторы, отвечающие за устранение неполадок, отслеживают проблемы, отмечая их на доске, и решают, кто какой проблемой займется, на основании вероятной причины и доступности. К концу тестирования все офисы и рабочие места должны иметь отметки, предпочтительно показывающие успешную работу. Если в каких-то офисах или на рабочих местах все еще будут отметки, свидетельствующие о проблеме, нужно оставить сообщение для пользователя и назначить кого-нибудь для встречи с ним утром и попытки решить эту проблему в первую очередь.

Системный подход помогает обнаружить проблемы до того, как на следующий день люди придут на работу. Вне зависимости от того, будет ли это плохое подключение сегмента сети, неудачное размещение хранилища программного обеспечения или проблемы со службой, у вас имеется хорошая возможность обнаружить проблему до того, как она причинит неудобства кому-то еще. Однако имейте в виду, что некоторые машины могли не работать с самого начала. Группы перезагрузки всегда должны отмечать, когда машина не выглядит рабочей до перезагрузки. Конечно, они могут уделить время исправлению неполадки, но эта работа имеет меньший приоритет и не должна выполняться до завершения технического перерыва.

В идеале тестирование системы и полномасштабная перезагрузка должны быть завершены в воскресенье днем. Это дает системным администраторам время для отдыха после тяжелых выходных, прежде чем на следующий день прийти на работу.

20.1.10. Общение после обслуживания

После завершения работ по техобслуживанию и тестированию системы руководитель полета рассылает по компании сообщение, информируя всех, что теперь служба полностью восстановлена. В сообщении кратко отмечаются основные задачи, выполненные во время технического перерыва, а также приводится краткий список служб, которые точно не работают, и время их исправления.

Это сообщение должно иметь заданный формат и составляться заблаговременно, потому что руководитель полета может слишком сильно устать, чтобы получить удовольствие от подготовки этого сообщения в конце долгих «выходных». Также невелик шанс того, что сообщение, написанное на этом этапе, не будет содержать ошибок.

Скрытая инфраструктура

Иногда пользователи зависят от сервера или службы, но не информируют нас об этом, возможно, из-за того, что создали их сами. Мы называем это скрытой инфраструктурой.

В одной компании было запланировано отключение и все электропитание здания было выключено. Серверы были отключены упорядоченно и успешно загружены снова. На следующее утро произошла такая переписка по электронной почте:

```
От: IT
Кому: Всем сотрудникам компании
Все серверы в офисе Берлингтона включены и работают. При любых проблемах
с серверами оставьте, пожалуйста, заявку на веб-странице поддержки.

От: Разработчик
Кому: IT
Devwin8 отключен.

От: IT
Кому: Всем сотрудникам компании
У кого под столом стоит devwin8, включите его, пожалуйста.
```

20.1.11. Возобновите удаленный доступ

Последним действием перед уходом из здания должно быть возобновление удаленного доступа и восстановление сообщения на автоответчике телефона службы поддержки к нормальному виду. Убедитесь, что это входит в общий план и в индивидуальные планы ответственных сотрудников. После напряженных выходных об этом легко можно забыть. Но это слишком заметная, неудобная и досадная деталь, чтобы вы могли себе позволить о ней забыть, особенно потому, что ее нельзя исправить удаленно, если весь удаленный доступ был успешно отключен.

20.1.12. Будьте на виду следующим утром

Очень важно, чтобы вся группа системных администраторов пришла на работу рано и была на виду в компании на следующее после технического перерыва утро, вне зависимости от того, насколько тяжелой была работа во время пере-

рыва. Если у всех есть футболки с логотипом компании или группы, заблаговременно до технического перерыва договоритесь, чтобы в день после отключения все надели эти футболки. Пусть люди, ответственные за конкретные подразделения, ходят по их коридорам, готовые к решению проблем.

Пусть руководитель полета и некоторые старшие системные администраторы из центральной группы основных служб, если такая существует, находятся в помещении службы поддержки, чтобы следить за звонками и выявлять проблемы, которые могут быть связаны с техническим перерывом. Эти люди должны уметь обнаружить и исправить их быстрее, чем обычный персонал службы поддержки, у которого не будет такого широкого представления о происшедшем.

Видимое всем присутствие в то время, когда компания возвращается к работе, символизирует вашу позицию: «Нам не все равно, и мы здесь для того, чтобы убедиться, что ничто из сделанного нами не нарушает вашу работу». Кроме того, это означает, что любые необнаруженные проблемы могут быть решены быстро и эффективно, поскольку весь нужный персонал будет на месте и его не придется будить. Оба этих фактора важны для общего удовлетворения компании итогами технического перерыва. Если компания не будет удовлетворена тем, как проходят технические перерывы, они будут отменены, что сделает превентивное обслуживание более трудным.

20.1.13. Обсуждение итогов

Приблизительно к обеду в день после технического перерыва должно быть обнаружено большинство оставшихся проблем. На этом этапе, если будет достаточно тихо, руководитель полета и некоторые старшие системные администраторы должны собраться и обсудить, что прошло не так, почему и что можно изменить. Все это нужно записать и позднее на неделе обсудить со всей группой. Благодаря обсуждению итогов со временем технические перерывы будут проходить более легко и гладко. Распространенными ошибками на ранних этапах являются планирование слишком большого объема работ, отсутствие достаточной предварительной работы и недооценка времени, которого могут потребовать различные задачи.

20.2. Тонкости

Несмотря на то что для успешного масштабного технического перерыва должны быть выполнены основные действия, полезно иметь еще кое-что. После успешного завершения нескольких технических перерывов вам нужно подумать о тонкостях, позволяющих усовершенствовать этот процесс.

20.2.1. Обучение нового руководителя полета

Для дальнейших технических перерывов может быть полезно обучать новых руководителей полета. Таким образом, руководителей полета можно будет выбирать заблаговременно, чтобы руководитель следующего технического перерыва мог работать с нынешним.

Обучаемый руководитель полета может создать первый набросок общего плана, пользуясь поданными запросами на изменения, добавляя любые недостающие взаимосвязи и отмечая эти добавления. Затем руководитель полета рассматривает план вместе с обучаемым, вносит или убирает взаимосвязи и реорганизует

задачи и назначения персонала должным образом, объясняя причины. В качестве альтернативы руководитель полета может создать первый черновой вариант вместе с обучаемым, объясняя процесс по ходу. Обучаемый руководитель полета также может помогать в ходе технического перерыва при наличии времени, работая вместе с нынешним руководителем полета, отслеживая состояние определенных проектов и предлагая изменение выделения ресурсов, если это требуется. Кроме того, обучаемый может помочь перед отключением, обсуждая проекты с некоторыми системными администраторами, если у руководителя полета будут вопросы о проекте, и обеспечивая заблаговременное соблюдение всех требований, указанных в предложении изменения.

20.2.2. Анализ тенденций в данных истории

Полезно отслеживать, сколько времени занимают те или иные задачи, а затем анализировать данные и улучшать оценки в процессе распределения задач и планирования. Например, если вы обнаружите, что перемещение определенного объема данных между двумя машинами заняло 8 ч и в другой раз вам нужно будет переместить большой объем данных между двумя идентичными машинами в похожей сети, вы сможете более точно предсказать, сколько времени это займет. Если конкретный программный пакет всегда трудно обновлять и обновление занимает больше времени, чем предполагалось, это можно отследить, спрогнозировать и заложить в график, а затем внимательно наблюдать во время технического перерыва.

Анализ тенденций особенно полезен при рассмотрении данных истории. Когда кто-то, выполнявший определенную функцию, покинет группу, человек, который придет на его место, сможет ознакомиться с данными предыдущих технических перерывов, чтобы посмотреть, какие типы задач обычно выполняются в этой области и сколько времени они занимают. Эти данные могут предоставить новым сотрудникам группы, незнакомым с планированием технических перерывов, ценную начальную информацию, чтобы они не упускали возможности для техобслуживания и не отставали.

Для каждого запроса на изменение записывайте фактическое время выполнения, чтобы использовать его для оценки времени в следующий раз. Кроме того, записывайте любые другие данные, которые в следующий раз смогут помочь улучшить процесс.

20.2.3. Предоставление ограниченной доступности

Есть большая вероятность, что на каком-то этапе вас попросят поддерживать доступность службы для определенной группы во время технического перерыва. Это может быть связано с чем-то непредвиденным, например недавно обнаруженной ошибкой, над которой инженерам нужно будет работать все выходные, либо с новым графиком работы подразделения, например переходом поддержки пользователей на обслуживание в режиме 24/7 и необходимостью постоянного доступа к ее системам для соблюдения контрактов. Интернет-службы, удаленный доступ, глобальные сети и давление новых конкурентов снижают вероятность разрешения полных отключений.

Планирование для соблюдения этого требования может предполагать изменение архитектуры некоторых служб или внесение в систему дополнительных уровней

избыточности. Оно может включать обеспечение большей автономности групп или их отделения друг от друга. Внесение таких изменений в вашу сеть может быть сложной задачей само по себе и, скорее всего, также потребует технического перерыва. Лучше всего быть готовым к этим требованиям до их появления, или вы можете остаться без времени на подготовку.

Чтобы начать выполнение этой задачи, выясните, каким пользователям потребуется возможность работы во время технического перерыва. Задавайте много вопросов и используйте свое знание систем, чтобы занести эти потребности в список требований доступности служб. Например, пользователям почти наверняка понадобятся службы имен и аутентификации. Им может потребоваться возможность печати на определенных принтерах и обмена электронной почтой внутри компании или с клиентами. Им может быть нужен доступ к службам через глобальные соединения или Интернет. Им могут потребоваться конкретные базы данных – выясните, от чего зависят эти машины. Рассмотрите способы, при помощи которых машины баз данных можно сделать избыточными, чтобы их можно было нормально обслуживать без потери функциональности. Убедитесь, что службы, от которых они зависят, также избыточны. Определите, какие элементы сети должны быть доступны для работы служб. Рассмотрите способы снижения количества сетей, которые должны быть доступны, за счет снижения числа сетей, используемых группой, и размещения избыточных серверов имен, идентификации и печати в сетях группы. Выясните, приемлемы ли небольшие отключения, например два 10-минутных отключения для перезагрузки сетевого оборудования. Если нет, компании нужно вкладывать средства в избыточное сетевое оборудование.

Создайте подробный план доступности, который точно описывает, какие службы и компоненты должны быть доступны этой группе. Пытайтесь упростить его за счет объединения сетевой топологии и введения избыточных систем для этих сетей. Введите планирование доступности в общий план, обеспечивая, чтобы избыточные серверы не отключались одновременно.

20.2.4. Компании высокой доступности

В силу самой природы своего бизнеса компании высокой доступности не могут себе позволить крупные запланированные отключения[1]. Кроме того, это означает, что они не могут себе позволить *не* делать крупных вложений, необходимых для предоставления высокой доступности. Компании, имеющие требования по высокой доступности, должны иметь много избыточных систем, которые будут продолжать предоставлять обслуживание в случае сбоя одного из компонентов. Чем выше требования по доступности, тем больше избыточных систем требуется для ее обеспечения[2].

---

[1] Высокой считается доступность выше 99,9%. Обычно компании будут стремиться к 99,9% (9 ч отключения в год), 99,99% (1 ч в год) или 99,999% (5 мин в год). Стоимость обеспечения доступности 99,9999% (менее одной минуты в год) дороже, чем могут позволить себе большинство компаний.

[2] Помните, что избыточность $n + 1$ используется для служб, в которых один компонент может отказать без сбоя службы, $n + 2$ означает, что отказать могут любые два компонента, и т. д.

Однако этим компаниям все же нужно обслуживать работающие системы. Впрочем, гарантии доступности, предоставляемые этими компаниями своим клиентам, обычно исключают технические перерывы – в случае крупных запланированных отключений компании потеряют клиентов.

20.2.4.1. Сходства

Большинство рассмотренных здесь принципов проведения технических перерывов в корпоративных системах справедливо и для компаний высокой доступности.

- Им требуется планировать время технического перерыва, чтобы он минимально влиял на их пользователей. Например, интернет-провайдеры часто выбирают 14:00 (местное время) в середине недели, компаниям электронной коммерции нужно выбрать время, когда они заключают меньше всего сделок. Обычно эти перерывы будут довольно частыми, например раз в неделю, и более короткими, возможно от 4 до 6 ч.
- Им требуется сообщать своим пользователям о том, на какое время назначен технический перерыв. Для интернет-провайдера это означает рассылку электронной почты пользователям. Для компании электронной коммерции это означает наличие баннера на сайте. В обоих случаях сообщение должно быть отправлено только тем клиентам, которые могут быть затронуты, и должно содержать предупреждение о том, что во время технического перерыва возможны небольшие сбои или ухудшение обслуживания, с указанием времени этого перерыва. О перерыве должно быть разослано только одно сообщение.
- Планирование и выполнение максимально возможного объема работ предварительно является критически важным, потому что технические перерывы должны быть как можно короче.
- Необходимо иметь руководителя полета, который координирует планирование времени и отслеживает выполнение задач. Если перерывы еженедельные, это может быть работа на четверть ставки или с частичной занятостью.
- Каждое действие должно иметь предложение по изменению. В предложении по изменению должны быть перечислены избыточные системы и должен иметься тест для проверки того, что избыточные системы включились и служба по-прежнему доступна.
- Им нужно жесткое планирование технического перерыва. Технические перерывы обычно у́же по охвату и короче. Задачи, запланированные на данный перерыв различными людьми, не должны иметь взаимных зависимостей. Нужен небольшой общий план, который будет показывать, кто какие задачи выполняет и время их выполнения.
- Руководитель полета должен очень строго следить за предельными сроками выполнения изменений.
- Все должно быть полностью проверено, прежде чем сообщать о завершении.
- Удаленный доступ к KVM и консолям полезен для всех компаний.
- Системные администраторы должны быть на месте, когда компания начинает работу. Они должны быть готовы быстро справиться с любыми проблемами, которые могут возникнуть в результате обслуживания.

- Полезно краткое подведение итогов на следующий день для обсуждения оставшихся проблем или возникших вопросов.

20.2.4.2. Различия

У технических перерывов в компаниях высокой доступности также есть несколько отличий.

- Необходимость избыточных систем для наличия высокой доступности.
- Нет необходимости в отключении доступа. Службы должны оставаться доступными.
- Нет необходимости в наличии полного списка отключения/загрузки, потому что полное отключение/перезагрузка не выполняется. Однако при наличии каких-либо взаимных зависимостей между машинами должен иметься список этих зависимостей[1].
- Из-за того что у интернет-провайдеров и компаний электронной коммерции нет локальных пользователей, физическая доступность на следующее утро неактуальна. Однако ваша доступность и готовность помочь все-таки важны. Найдите способ увеличить свою заметность и обеспечьте хорошую помощь. Распространите информацию о том, что было изменено, как сообщать о проблемах и т. д. Создайте блог или поместите баннер на своих внутренних веб-сайтах, чтобы рассказать о последних изменениях.
- Общение после техобслуживания обычно не требуется, если пользователям не нужно сообщать об оставшихся проблемах. Пользователям не нужна масса электронной почты от их провайдеров.
- Самое важное отличие состоит в том, что при планировании технического перерыва нужно учитывать избыточную архитектуру компании. Руководитель полета должен обеспечить, чтобы никакая запланированная работа не нарушила работу службы. Системные администраторы должны убедиться, что они знают, как долго продлится восстановление после отказа, например сколько времени требуется системе маршрутизации для синхронизации таблиц при отключении или включении одного из маршрутизаторов. Если избыточность реализована на одной машине, системным администраторам нужно знать, как работать над одной частью машины, сохраняя нормальную работу системы.
- В течение технического перерыва нужно внимательно следить за доступностью обслуживания в целом. Должен быть план, как работать в случае любых ошибок, которые вызывают сбой в результате временного недостатка избыточности.

20.3. Заключение

Основы успешного выполнения запланированного технического перерыва делятся на три категории: подготовка, выполнение и работа с пользователями после техобслуживания. Заблаговременная подготовка к техническому перерыву больше всего способствует его спокойному протеканию. Ключом к этому

[1] Обычно компании высокой доступности по возможности избегают взаимных зависимостей машин.

являются планирование и предварительное выполнение максимально возможного объема работ. Группе нужно назначить походящего руководителя полета для каждого технического перерыва. Предложения изменений должны подаваться руководителю, который затем использует их для создания общего плана и установки предельных сроков выполнения каждой задачи.

Во время технического перерыва необходимо отключение удаленного доступа и наличие инфраструктуры, такой как консольные серверы и радиосвязь. План должен быть выполнен с минимально возможным количеством отклонений. График должен строго соблюдаться, он должен завершаться полным тестированием системы.

Хорошая работа с пользователями после технического перерыва очень важна для его успеха. Ключом к ней является распространение информации о перерыве и видимое присутствие на следующее утро.

Интеграция процесса обучения, хранение данных истории и анализ тенденций для улучшения оценок, обеспечение возможности продолжения работы и предоставление ограниченной доступности для групп, которым она необходима, могут быть реализованы позже. Правильное планирование, хорошие планы отмены, строгое соблюдение предельных сроков выполнения изменений и полное тестирование должны предотвратить любые неприятности, кроме несущественных. Некоторые задачи могут быть не выполнены, и эти изменения потребуется отменить. По своему опыту мы можем сказать, что хорошо спланированный и правильно выполненный технический перерыв никогда не приводит к катастрофе. Однако плохо спланированный или выполненный технический перерыв может к ней привести. Такие масштабные отключения являются сложными и рискованными. Мы надеемся, что вам будут полезны методы планирования, рассмотренные в данной главе.

Задания

1. Прочитайте статью о разделении сети AT&T/Lucent (Limoncelli et al. 1997) и скажите, как наличие технического перерыва в выходные могло бы изменить процесс. Какие части этого проекта могут быть выполнены заблаговременно в качестве подготовительной работы, какие части стали бы проще, а какие – сложнее? Оцените риски вашего подхода.
2. Пример в разделе 20.1.1 описывает процесс планирования графика в конкретной компании по разработке программного обеспечения. Каких дат или событий потребовалось бы избегать при проведении технического перерыва в вашей компании? Попытайтесь составить список дат, приблизительно на три месяца, который актуален для вашей компании.
3. Оцените системных администраторов своей компании. Кто из них мог бы стать хорошим руководителем полета и почему?
4. Как вы думаете, какие задачи или проекты вашей компании подходят для выполнения во время технического перерыва? Создайте и заполните форму запроса на изменение. Какую подготовку к этому изменению вы можете выполнить заблаговременно до технического перерыва?
5. В разделе 20.1.6 рассматривается отключение доступа к системе. Какие особые задачи нужно было бы выполнить для этого в вашей компании и как бы вы возобновили этот доступ?

6. В разделе 20.1.7.1 рассмотрена последовательность отключения и перезагрузки. Создайте подходящий список для вашей компании. Проверьте его, если у вас есть разрешение.
7. В разделе 20.2.3 рассмотрено предоставление ограниченной доступности некоторым людям, чтобы позволить им продолжить работу. Какие группы, скорее всего, потребуют доступности в режиме 24/7? Какие изменения вам нужно внести в свою инфраструктуру сети и служб, чтобы службы были доступны каждой из этих групп?
8. Изучите методики управления полетами, используемые в НАСА. Соотнесите то, что вы узнали, с работой по системному администрированию.

Глава 21

Централизация и децентрализация

Данная глава направлена на то, чтобы помочь системному администратору решить, какая степень централизации является приемлемой для конкретной компании или службы и как изменять степень централизации.

Централизация означает наличие одной точки управления. В каждом подразделении компании может быть два DNS-сервера, но они оба могут контролироваться единым объектом. **Децентрализованные** системы, напротив, распределяют контроль по нескольким элементам. В нашем примере с DNS каждое из этих подразделений может обслуживать и контролировать свой собственный DNS-сервер, отвечая за поддержание квалификации для соответствия последним технологиям, создания подходящих, по его мнению, систем и мониторинга службы. Централизация также касается нетехнического управления. Компании могут организовывать централизованную или децентрализованную структуру IT.

Централизация – это попытка увеличить эффективность за счет использования преимуществ потенциальной экономии масштаба: улучшение среднего. Кроме того, она может повысить надежность за счет снижения возможностей для совершения ошибки. Децентрализация – это попытка повысить скорость и гибкость за счет реорганизации с усилением локальных контроля и обслуживания: усовершенствование наилучшего случая. Ни один из подходов не является однозначно лучшим во всех случаях, и ни один из них невозможен в чистом виде. При хорошей организации каждого из них можно реализовать преимущества другого подхода: странный парадокс, правда?

Децентрализация означает отказ от единой власти, восстание против раздражающих бюрократических методов прошлого. В традиционном смысле она означает такую неудовлетворенность централизованным обслуживанием, что его самостоятельное выполнение может быть лучше. В современной среде децентрализация часто является осознанной реакцией на ускорение темпа бизнеса и ожидания пользователей, связанные с высокой степенью автономности.

Централизация означает объединение групп для обеспечения порядка и поддержания рабочего процесса. Это сотрудничество ради высшего блага. Это процесс выравнивания. Он стремится к устранению бесполезной траты денег на дублирующие системы, дополнительную работу и ручные процессы. Новые технологии часто предоставляют возможности для централизации. Например, несмотря на то что наличие своих, немного отличающихся процессов обработки бумажных форм в каждом подразделении может иметь смысл, ни одно подразделение не сможет финансировать построение целостной системы веб-форм. Таким образом, революционная веб-технология создает возможность замены большого количества старых систем единой, более эффективной централизо-

ванной системой. С другой стороны, основанная на стандартах веб-технология может предоставить высокую степень местной автономии под эгидой централизованной системы, например делегированное администрирование.

21.1. Основы

Кажется, что каждую пару лет руководство решает централизовать все, что децентрализовано, и наоборот, особенно в крупных компаниях. Организации меньшего размера сталкиваются с похожими изменениями, вызванными слияниями или открытием новых комплексов зданий или филиалов. В данном разделе мы рассмотрим руководящие принципы, которые вы должны учитывать перед осуществлением таких широких изменений. Затем мы рассмотрим несколько служб, которые являются подходящими кандидатами для централизации и децентрализации.

21.1.1. Руководящие принципы

Есть несколько руководящих принципов, связанных с централизацией и децентрализацией. Они схожи с принципами, которые должны учитываться при любых крупных структурных изменениях.

- **Решение проблем**: *ясно представляйте себе, какую конкретную проблему вы пытаетесь решить*. Четко определите, какую проблему вы пытаетесь устранить. «Система нестабильна, потому что каждое подразделение использует оборудование различных марок». «Службы отказывают, когда отключаются сетевые соединения с офисами продаж». Запишите конкретную проблему (или проблемы) и расскажите о ней своей группе. Используйте этот список для проверки текущей ситуации в процессе дальнейшей работы над проектом, чтобы убедиться, что вы не потеряли цель из виду. Если вы не решаете конкретную проблему или не выполняете прямое указание руководства, остановитесь прямо сейчас. Почему вы собираетесь вносить эти изменения? Вы уверены, что это реальный приоритет?
- **Мотивация**: *понимайте свою мотивацию внесения изменения*. Возможно, вы пытаетесь сэкономить деньги, увеличить скорость или гибкость. Возможно, ваши причины являются политическими: вы защищаете свою территорию или своего начальника, создаете хорошее представление о своей группе или проводите в жизнь чью-то личную философию бизнеса. Может быть, вы делаете это просто для того, чтобы облегчить свою жизнь, – это тоже уместно. Запишите свою мотивацию и напоминайте себе о ней время от времени, чтобы удостовериться, что вы от нее не отклонились.
- **Опыт имеет значение**: *полагайтесь на здравый смысл*. Иногда вам нужно полагаться на опыт и интуицию, а не на конкретные научные оценки. Например, при централизации серверов электронной почты мы вывели на своем опыте следующее правило. Малым компаниям – пять отделов и 100 человек – обычно требуется один сервер электронной почты. Более крупные компании могут существовать с одним сервером электронной почты на тысячи людей, особенно если они состоят из одного крупного центра и большого количества относительно небольших офисов продаж. Когда компания дорастает до нескольких отдельных офисов, каждому из них обычно требуется свой сервер электронной почты, но вряд ли нужен собственный интер-

нет-шлюз. Очень крупным или географически распределенным компаниям требуются свои интернет-шлюзы для каждого местоположения.

- **Участие:** *прислушивайтесь к просьбам пользователей*. Консультируйтесь с пользователями, чтобы понимать их ожидания. Сохраняйте хорошее и устраняйте плохое. Сосредоточьтесь на принципах, которые они упоминают, а не на их реализации. Люди могут говорить, что им хочется, чтобы «Карен всегда была рядом, когда нам нужно установить новый настольный компьютер». Это реализация. Однако новая система может не предполагать наличие персонала. В этом случае нужно сохранить упомянутый принцип системы – быструю реакцию на запросы пользователей, такую же, какая была тогда, когда Карен всегда находилась рядом. Это может означать использование служб экспресс-доставки, или предварительно настроенных и «готовых к употреблению»[1] систем, которые хранятся в здании, или чего угодно, необходимого для соответствия этому ожиданию. С другой стороны, вы должны сформировать иные ожидания, если новая система не будет соответствовать прежним ожиданиям. Может быть, людям придется планировать все заранее и запрашивать рабочие станции за день.
- **Будьте реалистом:** *будьте осторожны с нереальными обещаниями*. Вы должны тщательно проверять любые заявления о том, что вы сэкономите деньги за счет децентрализации, внесете гибкость за счет централизации или получите полностью новую систему без труда, – обычно бывает наоборот. Если разработчик обещает, что новый продукт будет творить чудеса, но требует от вас централизации (или децентрализации) нынешней организации какой-либо структуры, возможно, преимущества обеспечивает как раз изменение организации, а не продукт!
- **Баланс:** *централизуйте настолько, насколько это имеет смысл на данный момент, и смотрите в будущее*. Вы должны найти баланс между централизацией и децентрализацией. Существуют временные ограничения: построение совершенной системы может длиться вечно. Вы должны ставить реальные задачи и учитывать перспективные потребности. Допустим, через полгода новая система будет завершена и предполагается, что она будет обрабатывать миллион объектов в день. Однако для обработки двух миллионов объектов в день – уровня, который ожидается еще через год, – потребуется другая архитектура и значительно больше времени на ее реализацию. Вы должны найти равновесие между преимуществом получения новой системы через полгода – с необходимостью сразу же начать строить систему следующего поколения – и возможностью более долгого периода построения системы, однако без необходимости такой быстрой замены.
- **Доступ:** *чем больше что-то будет централизовано, тем выше вероятность, что некоторым пользователям потребуются специальные функции или какая-либо индивидуализация*. Старая пословица бизнеса гласит: «Все наши клиенты одинаковы: у каждого есть уникальные требования». Один размер никогда не подходит всем. Вы не сможете выполнить разумную централизацию, не обеспечивая при этом гибкость, иначе ваш проект будет обречен. Лучше подумайте о небольшом количестве моделей. Некоторым пользователям нужна автономность. Другим может потребоваться выполнение собственных обновлений, что означает создание системы контро-

[1] Не пытайтесь съесть компьютер. «Готовые к употреблению» системы являются средствами для быстрой замены, которые после включения будут работать в полном объеме без какого-либо изменения файлов конфигурации и т. д.

ля доступа, чтобы пользователи могли изменять свои участки, не затрагивая других.

- **Отсутствие давления:** *аналогично распространению любой новой службы*. Несмотря на то что в этом случае возможно гораздо большее эмоциональное воздействие по сравнению с другими изменениями, проекты как по централизации, так и по децентрализации имеют вопросы, аналогичные созданию новой службы. При этом для достижения успеха новые службы требуют внимательной координации, планирования и понимания потребностей пользователя.
- **110%:** *у вас есть только один шанс произвести хорошее первое впечатление*. Новой системе никогда не будут доверять, пока она не подтвердит свою успешность, и первые впечатления от новой системы зададут настроение всей дальнейшей работе пользователей. Сделайте все правильно с первого раза, даже если это означает первоначальную трату большего количества денег или дополнительное время тестирования. Внимательно выбирайте пользователей для тестирования, вы должны пригласить только тех, которые верят, что вы исправите любые ошибки, найденные в ходе тестирования, и не будут болтать о них около кофейного автомата. Предоставляйте превосходное обслуживание в течение первого месяца – и люди простят ошибки в будущем. Если вы провалитесь с самого начала, восстановление репутации практически невозможно.
- **Право вето:** *слушайте пользователей, но помните о решениях руководства*. Организационная структура может влиять на допустимый или возможный уровень централизации. Самым серьезным препятствием для централизации часто являются решения руководства или политика. Недостаток доверия затрудняет централизацию. Если группа системных администраторов не проявила себя положительно, руководство может не захотеть поддержать серьезное изменение. Руководство может не хотеть финансировать изменения, обычно это означает, что изменение для них неважно. Например, если компания не оплатит центральную группу центральной инфраструктуры, системные администраторы будут децентрализованы. Наличие группы центральной инфраструктуры может быть лучше, однако без поддержки руководства оптимальным выходом из ситуации может стать обеспечение собственной инфраструктуры, реализованной наилучшим образом, – в идеальном случае формальная или неформальная координация для установки стандартов, совместные закупки и т. д. В любом случае конечной целью является предоставление вашим пользователям отличного обслуживания.

21.1.2. Кандидатуры для централизации

Системные администраторы постоянно находят новые возможности для централизации процессов и служб. Централизация сама по себе не повышает эффективность. Она предоставляет возможность внести в процесс дополнительную экономию масштаба. Эффективность повышает стандартизация, которая обычно является побочным продуктом централизации. Они находятся в тесном взаимодействии.

Экономия при централизации вызвана допущением, что накладные расходы будут меньше, чем сумма накладных расходов для каждого децентрализованного объекта. Централизация может обеспечить более простую и легкую в управ-

лении архитектуру. Один системный администратор может управлять гораздо бóльшим количеством машин, если для каждой из них процессы одинаковы.

Для предыдущих владельцев централизуемой службы централизация связана с потерей контроля. Подразделения, которые раньше выполняли обслуживание сами, теперь вынуждены полагаться на обслуживание централизованной группы. Системные администраторы, которые раньше выполняли задачи сами, по-своему, теперь вынуждены делать запросы кому-то еще, кто может применять другие методы. Системные администраторы захотят узнать, сможет ли новый поставщик услуг работать лучше.

Прежде чем лишить контроля предыдущего системного администратора или пользователя, задайте себе вопрос: какой будет его психологическая реакция? Будут ли попытки сопротивляться нововведениям? Как вы можете убедить людей, что новая система будет лучше старой? Как будут осуществляться контроль ущерба и контроль слухов? Как лучше всего произвести хорошее первое впечатление?

Лучший способ достичь успеха в программе централизации – выбрать для централизации правильные службы. Вот некоторые подходящие кандидатуры.

- **Распределенные системы**: *управление распределенными системами*. Так исторически сложилось, что каждое подразделение организации само настраивало и эксплуатировало свои веб-серверы. По мере развития технологий возникла необходимость ограничить независимость серверов. В конце концов, не было никаких доводов против того, чтобы сделать конфигурацию всех веб-серверов одинаковой, а необходимость быстрого обновления интерфейсов стала вопросом безопасности. Мотивация заключалась в экономии денег за счет отсутствия необходимости иметь высококвалифицированных специалистов для обслуживания веб-серверов в каждом подразделении. Решаемая проблема заключалась в том, что все серверы имели разную конфигурацию. Была создана система для поддержания центрального хранилища конфигураций, которое обновляло бы каждый сервер управляемым и безопасным методом. Затронутыми пользователями стали системные администраторы подразделений – они были рады сбросить с плеч задачи, которые не всегда понимали. За счет централизации веб-служб организация также смогла себе позволить содержать одного или нескольких системных администраторов, имеющих лучшие знания конкретно в этой сфере, чтобы предоставлять более эффективную внутреннюю поддержку пользователям.
- **Консолидация**: *объединение служб на меньшем количестве узлов*. Раньше ради надежности на каждом физическом узле располагалась одна служба. Однако по мере развития технологий может стать целесообразным размещение нескольких служб на одной машине. Мотивация заключается в снижении стоимости. Решаемая проблема состоит в том, что каждый узел предполагает накладные расходы, например, на электропитание, охлаждение, администрирование, пространство серверной и контракты на обслуживание. Обычно одна более мощная машина дешевле в эксплуатации, чем несколько меньших узлов. По мере консолидации служб нужно уделять внимание группировке пользователей с похожими потребностями.

  С конца 1990-х годов модной тенденцией стала **консолидация хранилищ информации**. За счет построения одной крупной сети для хранения информации, к которой имеет доступ каждый сервер, становится меньше «разоб-

щенных хранилищ» – частично заполненных дисков – на каждом сервере. Часто консолидация хранилищ информации предполагает выведение из эксплуатации старых, медленных или подверженных сбоям дисков и перемещение данных в сеть хранения данных (Storage Area Network – SAN), что обеспечивает лучшую производительность и надежность.

Более новая тенденция, **виртуализация серверов**, предполагает использование виртуальных узлов для экономии расходов на оборудование и лицензии. Например, в финансовых учреждениях были дорогие серверы и множество резервных машин для запуска вычислительных процессов в определенное время дня, например осуществления операций в конце рабочего дня после закрытия фондовых рынков. Вместо этого незадолго до закрытия рынка может быть запущена виртуальная машина, которая выполняет свои задачи, а затем отключается. После этого сервер может запускать другие виртуальные машины, выполняющие другие периодические задачи.

Используя глобальную файловую систему, например SAN, можно построить **кластер виртуализации**. Так как к образам виртуальных машин – записанным на диске данным, определяющим состояние виртуальной машины, – можно осуществлять доступ со многих физических серверов, развитое программное обеспечение по управлению виртуализацией может передавать виртуальные машины между физическими машинами за практически незаметное время. Часто компании понимают, что им требуется много машин, выполняющих определенную функцию, ни одна из которых не требует такой мощности процессора, которая оправдала бы стоимость выделенного оборудования. Вместо этого виртуальные машины могут совместно использовать кластер физических машин. Так как виртуальные машины можно передавать между различными аппаратными узлами, рабочую загрузку возможно перераспределять. Виртуальные машины можно переместить с перегруженной физической машины. Обслуживание также упрощается. Если одна из физических машин показывает признаки проблем с оборудованием, можно передать виртуальные машины на свободную машину без потери обслуживания, а затем отремонтировать или модернизировать физическую машину.

- **Администрирование**: *системное администрирование*. При изменении структуры вашей организации (см. главу 30) ваша мотивация может заключаться в снижении издержек, повышении скорости или последовательном предоставлении услуг в масштабах всей компании. Проблема может быть в лишних расходах на техническое управление для каждой группы или в том, что из-за распределенной модели некоторые подразделения обслуживаются хуже других. Централизация группы системного администрирования может исправить эти недостатки.

  Для обеспечения индивидуального подхода и «теплоты» персонального внимания подгруппы могут сосредоточиться на конкретных сегментах пользователей. Прекрасным примером является группа «послов САПР» в одной крупной компании по производству оборудования – группа системных администраторов, которая специализируется на независимой от подразделений поддержке систем автоматизированного проектирования и управления производством во всей компании. Однако распространенной ошибкой является доведение централизации до крайности. Мы видели по крайней мере одну очень большую компанию, которая довела централизацию до такого уровня, что для поддержания отношений с группами пользователей нанимались специальные сотрудники, а пользователи нанимали сотрудников для связи с централизо-

ванной группой системных администраторов. Скоро таких сотрудников стало более 100. На этом этапе экономия за счет снижения накладных расходов, конечно же, сошла на нет. Регулярное напоминание и соблюдение первоначальной мотивации могли бы предотвратить эту проблему.

- **Специализация**: *компетентность*. В децентрализованных организациях несколько групп, скорее всего, будут более компетентными в определенных областях, чем остальные. Хорошо, если они поддерживают неформальные отношения и помогают друг другу. Однако определенные знания могут быть критическими для бизнеса и поэтому неформальные отношения становятся неприемлемым риском для бизнеса. В данном случае может иметь смысл объединить все эти знания в одной группе. Мотивация заключается в обеспечении доступа всех подразделений к минимальному уровню компетентности в определенной области (или областях). Проблема заключается в том, что недостаток такой компетентности вызывает неравномерные уровни обслуживания, например в одном подразделении может быть ненадежная DNS, а в других – нет или одно подразделение может иметь хорошую интернет-службу электронной почты, а другие – все еще пользоваться адресами UUCP (UNIX-to-UNIX Copy Protocol). (Если вы слишком молоды и не помните адресов UUCP, считайте, что вам повезло.) Это было бы несправедливо!

  Организация централизованной группы для определенной службы может внести единообразие и повысить средний уровень обслуживания в компании в целом. В качестве примера можно упомянуть такие узкоспециализированные навыки, как обслуживание интернет-шлюза, хранилища программного обеспечения, различных средств безопасности – службы VPN, обнаружения вторжений, сканирования уязвимостей в безопасности и т. д., – DNS и службы электронной почты. Для более крупных компаний характерно создание группы «обслуживания» или «инфраструктуры» для объединения знаний в этих областях и обеспечения инфраструктурой всей организации.

- **Левая рука, правая рука**: *инфраструктурные решения*. Создание инфраструктуры и стандартов платформ может осуществляться централизованно. Это подвид централизации знаний. В одной компании мотивация заключалась в том, что расходы на инфраструктуру были высокими, а возможности по взаимодействию между подразделениями – низкими. Нужно было решить много конкретных проблем. В каждом подразделении была группа людей, разрабатывавших новые технологии и принимавших решения независимо. Разработки каждой группы дублировали усилия других. Невозможно было заключать контракты на оптовые поставки, потому что каждое подразделение было для этого слишком маленьким. Даже когда подразделениям было нужно приобрести одни и те же запчасти, последние все равно покупались по отдельности, потому что координация и сотрудничество отсутствовали. Решение состояло в снижении дублирования работы благодаря созданию одной комиссии по стандартам инфраструктуры и стандартам платформ. Раньше новые технологии часто внедрялись в компании фрагментарно: поскольку некоторые подразделения были менее подвержены риску, они и осуществляли пробную эксплуатацию продукта или становились первыми пользователями новых технологий.

  Последний пример показывает другое преимущество централизации. Расширение возможностей по закупке означает, что за те же деньги можно приобрести лучшее оборудование. Разработчики могут предоставлять лучшее

обслуживание, а также более низкие цены, когда они работают с централизованной группой закупки, от которой можно ожидать постоянный объем заказов. Иногда за счет централизации можно просто сэкономить деньги. В других случаях лучше воспользоваться сэкономленными деньгами для вложения в новое оборудование.

- **Массовость**: *если что-то стало массовым, осуществляйте централизацию*. Подходящее время для централизации чего-либо – когда технологии становятся массовыми. Сетевая печать, средства обработки файлов, серверы электронной почты и даже обслуживание рабочих станций когда-то были уникальными, редкими технологиями. Однако теперь все это стало массовым и хорошо подходит для централизации.

Пример: большие файловые серверы

Пользователи Тома и даже его коллеги, системные администраторы, долго и упорно боролись против принципа крупных, централизованных файловых серверов. Пользователи жаловались на потерю контроля и создавали непродуманные, по мнению Тома, модели ценообразования, которые показывали, что старые файловые серверы под UNIX были лучше. На самом деле они боролись против мнения о том, что сетевые средства обработки файлов больше не были чем-то особым, они стали массовыми, а следовательно, подходящими кандидатами для централизации. В конце концов было выполнено сравнение в сопоставимых оценках. Оно содержало общую модель расходов на эксплуатацию, которая включала время работы системных администраторов и электроэнергию, необходимые для поддержки старых систем. Ценность некоторых уникальных черт выделенных файловых серверов, например образа файловой системы, было трудно оценить количественно. Однако, даже когда модель расходов показала, что расходы на гигабайт используемого пространства для обеих систем были примерно одинаковыми, выделенные файловые серверы имели преимущества над старыми системами за счет целостности и поддержки. Старые системы представляли собой смесь аппаратуры от различных производителей – узлов, RAID-контроллеров, дисков, кабелей, сетевых плат и иногда даже стоек, в которых это все располагалось! Для эффективного обслуживания каждого из этих объектов требовался определенный уровень знаний и опыта, и ни один разработчик не мог поддерживать этих чудовищ Франкенштейна в одиночку. Обычно, когда системный администратор, который покупал конкретное RAID-устройство, уходил из группы, знания уходили вместе с ним. Стандартизация конкретных продуктов привела к повышению уровня обслуживания, потому что сэкономленные деньги использовались для покупки самых лучших систем, которые имели меньше проблем, чем их недорогие конкуренты. Кроме того, наличие единственного телефонного номера поддержки было очень удобным.

Печать – это еще одна массовая служба, имеющая много возможностей для централизации как при проектировании самой службы, так и при покупке оборудования. В разделе 24.1.1 предоставлено больше примеров.

21.1.3. Кандидатуры для децентрализации

Децентрализация не снижает время реакции автоматически. Но при правильном выполнении она создает для этого предпосылки. Даже если новый процесс будет менее эффективным или неэффективным по каким-то другим параметрам, люди могут быть удовлетворены просто наличием контроля. Мы обнаружили, что люди более терпимы к посредственным процессам, если чувствуют их управляемость.

Децентрализация часто жертвует эффективностью расходов ради чего-нибудь более ценного. В этих примерах мы осуществляем децентрализацию для демократизации контроля, обеспечения устойчивости к ошибкам, получения возможности создания индивидуального решения или отделения от недостаточно компетентных центральных органов («Они идиоты, но они идиоты из *нашего* отдела»). Нужно сохранять все хорошее в старой системе, исправляя при этом плохое.

Децентрализация демократизирует контроль. Новым людям, получающим возможность управления, может потребоваться обучение – это касается как пользователей, так и системных администраторов. Целью может быть автономность, способность контролировать собственную судьбу или работать при отключении от сети. Последнее также называется **расчленением**, способностью достичь разных уровней надежности для различных сегментов сообщества. Вот некоторые подходящие кандидатуры для децентрализации.

- *Устойчивость к отказам.* Дублирование работы, связанное с децентрализацией, может устранять одиночные точки отказов. В компании с растущей сетью филиалов требовалось, чтобы все сотрудники читали электронную почту с серверов, расположенных в центральном офисе. Во время сбоев сети были постоянные жалобы, люди не могли читать и даже писать сообщения, потому что это требовало доступа к серверам директорий, которые также располагались в центральном офисе. Подразделения в других часовых поясах были особенно недовольны тем, что технические перерывы в центральном офисе приходились на их основное рабочее время. Мотивация заключалась в повышении надежности, в частности, доступа во время отключений. Проблема состояла в том, что люди не могли пользоваться электронной почтой при отключении соединений глобальной сети. Решение заключалось в установке буферов LDAP и серверов электронной почты в каждом основном местоположении. Кроме того, было удобно и эффективно использовать эти узлы для DNS, аутентификации и других служб. Несмотря на то что во время отключения электронная почта не могла передаваться из одного места в другое, пользователи получили доступ к своей электронной почте, стала возможной доставка локальной электронной почты, а сообщения, отправляемые в другие места, незаметно для пользователя помещались в очередь до восстановления соединения глобальной сети. Если бы в каждом месте обладали необходимой подготовкой для конфигурирования и поддержки таких систем или создавали бы свои стандарты, это было бы катастрофой для управления. Но в данном случае все было успешно, потому что управление было централизовано. Каждый филиал получил предварительно настроенное оборудование с программным обеспечением, которое нужно было просто включить. Обновления выполнялись через централизованную систему. При необходимости удаленно можно было даже сделать резервную копию.

- *Индивидуализация*. Иногда некоторым группам пользователей необходимо в интересах бизнеса быть на пике прогрессивных технологий, в то время как другие требуют стабильности. Исследовательской группе требовался ранний доступ к технологиям, обычно до их одобрения комиссиями по стандартам корпоративной инфраструктуры. Мотивация главным образом была политической, потому что группа поддерживала определенный статус, будучи впереди всех остальных как в компании, так и в отрасли. Кроме того, имелась деловая мотивация: проекты группы были долгосрочными и футуристическими и группе требовалось «жить в будущем», если она собиралась строить системы, которые будут хорошо работать в сетях будущего. Проблема заключалась в том, что группе не позволяли отклоняться от корпоративных стандартов. Решение состояло в создании для группы специального подразделения системных администраторов. Сотрудники подразделения входили в комиссии, которые создавали корпоративные стандарты и могли предоставить ценную обратную связь, потому что они имели опыт работы с технологиями, которые остальная комиссия только рассматривала. Предоставление этих советов также поддерживало элитный статус групп. Кроме того, их участие гарантировало, что они смогут предоставить указания по взаимодействию между своими «хитрыми» системами и корпоративными стандартами. Эта местная группа системных администраторов могла соответствовать местным требованиям, которые отличались от требований в остальной компании. Они могли обеспечивать особые функции и выбирать иной баланс стабильности и новейших технологий.
- *Удовлетворение потребностей ваших пользователей*. Иногда централизованная группа обслуживания может быть неспособна выполнять требования, предъявляемые к ней некоторыми подразделениями компании. Прежде чем отказываться от централизованного обслуживания, попытайтесь понять причину, по которой центральная группа не может удовлетворить потребности ваших пользователей. Попробуйте поработать с пользователями для поиска решения, которое подойдет как для них, так и для системных администраторов, например подобное описанному выше. В конечном итоге ваша обязанность – выполнять требования пользователей и повышать эффективность их работы. Если вы не способны обеспечить связь с центральной группой, вашей компании может потребоваться осуществить децентрализацию необходимых служб, чтобы вы могли удовлетворять потребности своей группы. Убедитесь, что руководство поддерживает вас в этих действиях, учитывайте возможные трудности децентрализации и попытайтесь их избежать. Помните, почему вы перешли к централизованной модели, и периодически проверяйте, имеет ли она еще смысл.

  Сторонники децентрализации иногда утверждают, что централизованные службы являются единой точкой отказа. Однако, когда централизация выполнена правильно, сэкономленные деньги можно вложить в технологии, которые повышают устойчивость к отказам. Часто результатом децентрализации является множество отдельных точек отказа, распределенных по всей компании, и избыточность снижается. Например, когда отдельные группы создают свои локальные сети, они приобретают опыт только в создании очень простой инфраструктуры локальной сети. Ограниченность служебных обязанностей не позволяет таким людям стать экспертами в современных технологиях локальных сетей. Когда построение локальной сети централизовано, за него отвечают люди, которые специализируются на сетях и работа-

ют с ними постоянно. У них есть время для организации работы резервных протоколов и предварительного мониторинга, которые позволят им исправлять проблемы, соблюдая заключенное соглашение об уровне обслуживания (Service Level Agreement – SLA). Экономия за счет оптовых закупок часто оправдывает отсутствие большей части избыточности. Повышение надежности за счет профессионального проектирования и эксплуатации, основанных на SLA, во многом выгодно компании.

Другой аргумент в пользу децентрализации заключается в том, что существуют преимущества разнообразия ваших систем. Например, различные ОС имеют разные проблемы безопасности. Преимущество здесь заключается в том, что вирус выведет из строя только часть ваших систем. В крупной компании по разработке программного обеспечения как-то произошел сбой DNS, получивший широкую огласку, причиной которого было то, что все DNS-серверы использовали одинаковую ОС и одну и ту же версию программного обеспечения DNS. Если бы компания использовала несколько ОС и программ для DNS, один из серверов мог бы не иметь уязвимости, которая была использована. Если вы предоставляете услуги централизованно, учтите, что иногда могут быть необходимы элементы децентрализации.

21.2. Тонкости

Централизация и децентрализация могут потребовать серьезной перестройки. Если вы просите людей потерпеть временные неудобства из-за перехода на новую систему, то должны предлагать систему, которая не только дешевле, но и лучше для них.

Есть старый афоризм, который часто пишут на значках и наклейках на бамперы: «Дешево, быстро, хорошо: выберите два». Это меткое выражение передает проверенную временем истину. Обычно вам нужно пожертвовать одной из трех характеристик, чтобы получить две другие. На самом деле, если кто-то утверждает, что обеспечивает все три характеристики одновременно, проверьте как следует, не прячет ли он что-нибудь в рукаве. В данном разделе приведены некоторые примеры, когда были сделаны попытки обеспечить все три преимущества. Какие-то из них, как в примере с закупками в разделе 21.2.1, в целом оказались очень успешными. В других случаях результаты были неоднозначными.

21.2.1. Объединение закупок

В данном примере централизация привела к более быстрой доставке лучших продуктов за меньшие деньги. Группа системных администраторов смогла добиться права на одобрение всех закупок своего подразделения, связанных с компьютерами. На самом деле группа смогла получить в свой состав агента по закупкам и поэтому была способна тесно взаимодействовать по контрактам, соглашениям на техническое обслуживание и т. д. В результате группа смогла отслеживать закупки. Планирование определенных закупок, например покупки серверов, позволяло системным администраторам заблаговременно связываться с пользователями, чтобы выяснить, какие особые требования связаны с сервером: нужно ли ему дополнительное место в серверной, особое подключение к сети или специальная конфигурация. Это решало проблему того, что пользователи могли предъявить системным администраторам неожиданные требования

при реализации главных проектов. Теперь системные администраторы могли связаться с пользователями и спланировать эти проекты должным образом.

В качестве дополнительного преимущества группа получила возможность лучше управлять активами. Из-за того что все закупки проходили через одну систему, существовало единое место, где сохранялись серийные номера нового оборудования. Предыдущие попытки отслеживания активов были неудачными, потому что сбор таких данных зависел от людей, у которых были другие приоритеты.

Самым большим преимуществом централизованных закупок было то, что теперь системные администраторы знали, какие продукты приобретаются. Если они замечали, что те или иные продукты покупаются часто, то заключали контракты на их оптовые поставки. Некоторые программы предварительно заказывались оптом. Представьте удивление пользователей, когда они, попытавшись заказать какую-то программу, получают извещение о том, что их подразделению нужно заплатить за одну пятидесятую программы с лицензией на 50 пользователей, уже купленной в этом году, после чего им будет выдан пароль для загрузки программы и руководств. Это определенно будет отличным сюрпризом!

Централизованная закупка компьютеров стала очень популярной практикой экономии. Раньше пользователи сами заказывали свои компьютеры и тратили несколько дней на изучение каталогов и подбор каждого отдельного компонента для своих особых нужд. В результате центр по ремонту компьютеров вынужден был работать с различными типами материнских плат, карт расширения и драйверов. Хотя пользователь мог гордиться тем, что сэкономил 10 долларов за счет выбора нестандартной видеокарты, это преимущество сводилось на нет, когда технику по ремонту компьютеров приходилось возиться полдня, чтобы эта видеокарта заработала. Так как группа ремонта не могла хранить так много разных запчастей, пользователи были вынуждены ждать по нескольку недель, пока их запчасти будут доставлены.

Среднее время доставки компьютера по старой системе составляло 6 недель. Неделю занимало определение заказа и его оформление. Поставщик тратил две недели на сборку компьютера по заказу и его доставку. Наконец, пока у системных администраторов появлялось время на установку ОС, проходила еще одна неделя, а возможно и две, если были какие-то проблемы. Компания не может работать быстро, если для доставки каждого компьютера требуется больше месяца. Что еще хуже, новые сотрудники ждали получения компьютера по несколько недель. Это подрывало моральное состояние и негативно отражалось на компании. Временное решение заключалось в том, что руководство умоляло системных администраторов собрать для сотрудника компьютер из имеющихся запчастей на время, пока не придет заказанный. Таким образом, выполнялось вдвое больше работы, потому что требовалась доставка двух компьютеров.

Группа централизованной закупки смогла решить эти проблемы. Группа обнаружила, что за счет стандартизации конфигураций можно снизить расходы благодаря оптовым скидкам. На самом деле группа смогла получить хорошую цену даже несмотря на то, что запрашивала 4 конфигурации: сервер, рабочую станцию, сверхлегкий ноутбук и сверхмощный ноутбук. Опасаясь того, что люди все же будут предпочитать индивидуальную конфигурацию, группа использовала часть сэкономленных средств для обеспечения большей мощности стандартной конфигурации, с лучшими аудио- и видеосредствами, чем в любом ранее купленном персональном компьютере. Даже если группа не добивалась цены ниже предыдущей, экономия для подразделения по ремонту компьютеров

была значительной. Возможность хранения достаточного количества запчастей снижала потери в производительности пользователей, ожидающих ремонта своих машин.

Группа закупок поняла, что она не сможет распространить стандарт среди пользователей, которые просто предпочтут полностью индивидуальную конфигурацию, если стандарт придется им не по нраву. Поэтому группа закупок обеспечила высокую привлекательность своего стандарта для пользователей, сделав его очень хорошим. За счет оптовых скидок цена была такой низкой, а качество таким высоким, что большинство оставшихся возможностей индивидуализации привело бы к приобретению менее мощной машины за большие деньги. Как же можно было отказаться от стандарта? Такая методика – это использование пряника, а не кнута.

Было достигнуто еще одно преимущество. За счет того что поток новых закупаемых машин был относительно постоянным, группа закупок смогла предварительно заказывать по несколько машин, на которых системные администраторы сразу устанавливали ОС. Новые сотрудники получали на свой стол компьютер высшего качества за день до выхода на работу. Они работали эффективно начиная с самого первого дня.

Время заказа компьютеров снизилось с 6 недель до 6 минут. Оказавшись перед выбором между тем, чтобы заказывать компьютер точной желаемой конфигурации и ждать его 6 недель, и тем, чтобы ждать 6 минут и получить компьютер, который часто был более мощным, чем требовалось, пользователи, естественно, не отказывались от второго предложения.

Любая компания, которая быстро растет и покупает много компьютерной техники, должна рассмотреть такие подходы. Другие советы по быстрой установке компьютеров можно найти в главе 3. Более подробная информация о том, как поставщики компьютеров устанавливают цены на свою продукцию, приведена в разделе 4.1.3.

21.2.2. Аутсорсинг

Аутсорсинг (привлечение сторонних исполнителей) часто является формой централизации. **Аутсорсинг** – это процесс, при котором сторонней компании платят за предоставление компании определенных технических услуг. Некоторыми типичными задачами, для которых часто привлекаются сторонние исполнители, являются организация корпоративной компьютерной службы поддержки, удаленный доступ, обслуживание локальных и глобальных сетей, а также работа по установке компьютеров. Для некоторых специфических задач, например построения инфраструктуры для поддержки конкретного приложения – вебсервера, сайта электронной коммерции, системы управления предприятием, – привлекаются сторонние исполнители, хотя обычно поставщики называют этот процесс «профессиональными услугами».

Аутсорсинг обычно предполагает централизацию для снижения избыточного обслуживания и стандартизации процессов. Привлечение сторонних исполнителей может сэкономить деньги за счет устранения внутренних политических конфликтов, которые обычно не позволяют достичь такой эффективности. Когда руководители не могут отказаться от своих политических принципов в пользу хорошего управления, привлечение сторонних исполнителей может быть особо полезным.

Сторонники подчеркивают, что привлечение внешних исполнителей позволяет компании сосредоточиться на основном профиле, а не на технологической инфраструктуре, необходимой для поддержки этой основы. Некоторые компании застревают в поддержке своей инфраструктуры в ущерб задачам бизнеса. В этой ситуации аутсорсинг может быть привлекательным решением.

Ключевой вопрос при привлечении сторонних исполнителей – знать, чего вы хотите, и убедиться, что это указано в контракте. Сторонний исполнитель не обязан делать ничего, что не указано в контракте. Несмотря на то что продавцы могут нарисовать красочную картину, после подписания контракта вам следует ожидать только того, что указано на бумаге. Это может быть особенно важной проблемой, когда обслуживание, для которого привлекаются сторонние исполнители, раньше осуществлялось собственными силами.

Мы встречались с тремя проблемами, возникающими при подписании контракта со сторонним исполнителем. Все вместе они создают интересный парадокс. Привлечение сторонних исполнителей для получения новых технических знаний означает, что люди, с которыми вы ведете переговоры, будут иметь больше технических знаний, чем вы. Это дает сторонней фирме сильное преимущество в переговорах. Во-вторых, для точного указания своих требований в контракте вы должны хорошо понимать свои технические потребности, однако, если ваше руководство хорошо представляет, что нужно, и способно рассказать вам об этом, вам не потребуется привлекать сторонних исполнителей. Наконец, компании иногда не решаются прибегнуть к аутсорсингу, пока их компьютерная инфраструктура не ухудшится до такой степени, что привлечение сторонних исполнителей для ее обслуживания выполняется как экстренная мера. В этом случае компании часто слишком спешат или впадают в панику, теряя ведущую роль в переговорах. Компании не знают, чего они хотят или как об этом попросить, и не имеют ни времени, ни выдержки, чтобы провести адекватное исследование. Как вы понимаете, это предвещает неприятности. Компания-заказчик, желающая купить технологические знания, никогда не должна себя так вести.

Вы должны ознакомиться с процессом аутсорсинга, обсудить его тонкости с коллегами из других компаний и пообщаться со справочными службами для клиентов. Убедитесь, что контракт предусматривает полный цикл жизни служб (проектирование, установку, обслуживание и поддержку, вывод из эксплуатации, целостность данных и аварийное восстановление), санкции за несоблюдение требований по производительности и процесс внесения и удаления служб из контракта. Переговоры по заключению контракта на привлечение сторонних исполнителей являются очень трудными и требуют гораздо более сложных навыков, чем описано в нашем введении в теорию переговоров (раздел 32.2.1).

Некоторые аутсорсинговые контракты предлагают расценки ниже реальной стоимости – это прием, к которому прибегает исполнитель для привлечения заказчиков; однако работа над такими «убыточными» проектами приносит этим исполнителям немалые деньги. В таких контрактах обычно указано, что «входит» в объем обязательных работ, и вскользь упомянуто, что все остальные работы, которые в него «не входят», будут выполняться по стандартным расценкам. Стандартные расценки обычно очень высоки, и организация, которая будет выполнять проект, постарается добиться максимально возможного объема работ, не входящих в контракт. Клиенты обычно не думают о том, чтобы оговорить выполнение таких работ в контракте, – а ведь тогда цена была бы ниже.

Есть консультанты по аутсорсингу, которые могут помочь вам в процессе переговоров. Убедитесь, что работающий с вами консультант не имеет финансовых связей с фирмами-исполнителями, которые вы рассматриваете.

Не скрывайте переговоры

Когда одна компания из списка Fortune 500 привлекла сторонних исполнителей для обслуживания инфраструктуры своей компьютерной поддержки, высшее руководство боялось серьезного неприятия этого действия со стороны как компьютерных гуру компании, так и офисных работников, которым предоставлялась поддержка. Поэтому сделка была проведена быстро и без консультаций с людьми, которые предоставляли поддержку. В результате компании не хватало ключевых элементов, таких как резервные копии данных, меры оценки качества и четкое определение уровня обслуживания. Компания не могла перезаключить контракт без серьезных санкций. Когда после заключения контракта были сделаны резервные копии, расходы на эту работу, не входящую в контракт, оказались очень высокими.

Не ведите переговоры по заключению контракта на привлечение сторонних исполнителей тайно, получите одобрение заинтересованных пользователей.

Когда вы для чего-то привлекаете сторонних исполнителей, вашей обязанностью становится обеспечение качества. Некоторые думают, что после привлечения сторонних исполнителей контракт «сам о себе позаботится». На самом деле теперь вы должны научиться отслеживать соблюдение соглашений об уровне обслуживания, чтобы убедиться, что вы получаете по контракту все. Часто такие вещи, как документация или схемы архитектуры службы/сети, указываются в контракте, но не предоставляются, пока об этом не попросят.

Критически оценивайте показатели

Руководители одной компании очень гордились своим решением привлечь сторонних исполнителей, когда после года обслуживания исследование качества показало, что запросы в службу поддержки выполнялись в среднем за 5 мин. Это звучало хорошо, но почему-то сотрудники все-таки жаловались на предоставляемое обслуживание. Кто-то решил спросить, откуда были получены такие статистические данные, если многие запросы требовали посещения техником рабочего места сотрудника. Даже при умеренном количестве таких вызовов статистика не могла быть настолько радужной. Оказалось, что у техников, которые занимались поддержкой на рабочих местах, была своя очередь запросов со своей мерой времени выполнения. Запрос в службу поддержки считался закрытым, когда заявка направлялась в очередь техникам по поддержке на рабочих местах, таким образом искусственно улучшая показатели службы поддержки. Всегда просите подробного объяснения любых показателей, которые вы получаете от поставщика услуг, чтобы вы могли четко привязать их к соглашениям об уровне обслуживания.

Пока вы пытаетесь выжать максимум из своего контракта, компания-исполнитель старается сделать то же самое. Если контракт заключен «на сумму до 5 млн долларов за 5 лет», вы можете быть уверены, что менеджер исполнителя не позволит вам потратить только 4,5 млн долларов. Большинство компаний-исполнителей проводят еженедельные собрания, чтобы определить, идут ли они по графику в плане максимально быстрого использования стоимости контракта; они штрафуют свои группы продаж, когда те «не дотягивают до контракта». Контракт требует оплаты 1000 долларов в месяц за сервер? Вопросы типа «Как мы можем убедить их, что новая служба, которую они попросили, требует выделенного узла, а не загрузки на имеющуюся машину?» будут задаваться на каждом шагу. А вот самое интересное: если они смогут заставить вас потратить 5 млн долларов, оговоренные в пятилетнем контракте, за 4,5 года, работа в последние полгода вряд ли будет оплачиваться по согласованной вами сниженной стоимости. Как можно предсказать, каковы будут потребности в плане IT на такой долгий срок? Это самый опасный аспект долгосрочных аутсорсинговых контрактов.

Убедитесь, что в вашем контракте указана стратегия выхода. При заключении долгосрочного контракта компания-исполнитель обычно получает право нанимать ваш нынешний компьютерный персонал. Однако в контракте никогда не оговаривается, что вы получите его обратно, если решите, что это стороннее обслуживание не для вас. Многие контракты не гарантируют, что ваш бывший персонал будет оставаться на месте в течение всего срока контракта. Компания может решить воспользоваться их знаниями в другом месте! Даже переход на другую компанию-исполнителя является сложным, потому что прежняя компания точно не захочет отдавать своих сотрудников конкуренту. Убедитесь, что в контракте оговорены действия в подобных ситуациях, чтобы вы не попали в ловушку. Обратный переход на собственное обслуживание является очень сложным. Устраните все возможные условия, которые не позволят вам нанять своих людей обратно.

Заметим, что наше рассмотрение аутсорсинга полностью основано на нашем опыте работы в качестве системных администраторов. Во многих книгах представлены другие точки зрения. Некоторые из этих книг посвящены общим вопросам аутсорсинга (Gay and Essinger 2000, Rothery and Robertson 1995). Уильямс (Williams 1998), напротив, предоставляет процесс с точки зрения директора по информационным технологиям. Майлотт (Mylott 1995) рассматривает процесс привлечения сторонних исполнителей с точки зрения перехода обязанностей по управлению информационными системами. Книга Group Staff Outsource 1996 представляет общий обзор аутсорсинга. Куонг (Kuong 2000) рассматривает особый вопрос обеспечения услуг сторонних провайдеров служб веб-приложений. Дженнингса и Пассаро (Jennings and Passaro 1999) интересно почитать, если вы сами хотите заняться оказанием услуг другим компаниям. Наконец, Чэпмен и Эндрейд (Chapman and Andrade 1997) рассматривают, как выйти из контракта по привлечению сторонних исполнителей, и представляют прекрасные примеры связанных с этим страшных историй. Мы снова коснемся темы привлечения сторонних исполнителей в разделе 30.1.8.

Первое издание этой книги было написано в эпоху всеобщего помешательства на аутсорсинге в конце 1990-х годов. Мы сделали множество предостережений о негативных перспективах привлечения сторонних исполнителей, многие из которых подтвердились. Сейчас это помешательство закончилось, но новым

массовым безумием стал **офшоринг** (размещение компанией части своей производственной деятельности за рубежом). Все новое – это хорошо забытое старое.

21.3. Заключение

Централизация и децентрализация являются сложными темами. Ни одна из них не является правильным решением во всех случаях. В терминах централизации и децентрализации могут решаться как технические вопросы, такие как администрирование серверов, так и нетехнические, например организационная структура.

Оба процесса связаны с внесением изменений. При осуществлении таких всесторонних изменений мы рекомендуем вам руководствоваться следующими принципами: знайте, какую проблему вы решаете, понимайте свою мотивацию внесения изменения, централизуйте настолько, насколько это имеет смысл на данный момент, относитесь к этому как к распространению любой новой службы, тщательно планируйте и, самое важное, прислушивайтесь к мнению пользователей.

Полезно учиться на опыте других людей. Было опубликовано много материалов конференции USENIX LISA (Epp and Baines 1992, Ondishko 1989, Schafer 1992b, Schwartz, Cottrell and Dart 1994). Харлэндер (Harlander 1994), а также Миллер и Моррис (Miller and Morris 1996) описывают полезные приемы и опыт, полученный при их использовании.

Централизованные закупки могут быть прекрасным способом контролировать расходы, и наш пример показал, что их можно делать, не лишая людей возможности получать то, чего они хотят, а помогая им делать закупки более эффективно.

Мы закончили рассмотрением аутсорсинга. Привлечение сторонних исполнителей может стать основной силой в централизации и будет значительным элементом системного администрирования очень долго, даже под другими названиями.

Практические правила централизации

Все компании разные, но мы на практике выяснили, что централизация следующих служб предпочтительна, если компания становится достаточно крупной и в ней появляются различные подразделения:

- Сетевая безопасность
- Подключение к Интернету
- Службы глобальных сетей
- Установка и эксплуатация локальных сетей
- Службы электронной почты
- ActiveDirectory/LDAP
- Установка и текущее обслуживание компьютеров
- Хранение данных в центре
- Веб-службы с внешним доступом
- Выделение IP-адресов и управление DNS

Задания

1. Насколько централизована или децентрализована ваша нынешняя среда? Приведите примеры.
2. Приведите пример службы или области вашей организации, которая должна быть централизована. Свяжите руководящие принципы в разделе 21.1.1 с таким проектом.
3. Приведите пример службы или области вашей организации, которая должна быть децентрализована. Свяжите руководящие принципы в разделе 21.1.1 с таким проектом.
4. В разделе 21.1.3 мы рассмотрели децентрализацию серверов электронной почты для достижения лучшей надежности. Как бы вы реализовали подобную архитектуру для серверов печати?
5. Опишите небольшой проект по централизации, который улучшил бы вашу нынешнюю систему.
6. Расскажите вашу любимую страшную историю об аутсорсинге.

Часть IV

Предоставление услуг

Глава 22

Мониторинг служб

Мониторинг – это важный компонент обеспечения надежного, профессионального обслуживания. Два основных типа мониторинга – это мониторинг в реальном времени и исторический мониторинг. Каждый из них имеет свое предназначение. Как говорилось в разделе 5.1.13, мониторинг является основным элементом при создании службы и выполнении ожидаемого или требуемого уровня обслуживания.

«Если вы не можете что-то измерить, вы не можете этим управлять». В области системного администрирования эта полезная аксиома бизнеса превращается в «Если вы не наблюдаете за чем-то, вы не управляете им».

Мониторинг необходим для любой хорошо организованной компании, но является проектом, масштаб которого может постоянно расширяться. Данная глава должна помочь вам подготовиться к этому. Мы рассмотрим основы системы мониторинга, а затем покажем различные способы ее улучшения.

Для некоторых компаний, например предоставляющих услуги через Интернет, полный мониторинг необходим для бизнеса. Этим компаниям нужно наблюдать за всем, чтобы убедиться, что они не теряют прибыль из-за сбоя, который проходит незамеченным. Сайтам электронной коммерции, скорее всего, потребуется реализовать все, что описано в данной главе.

22.1. Основы

Мониторинг систем может применяться для обнаружения и устранения неполадок, определения источника проблем, предвидения и своевременного предотвращения проблем в будущем и предоставления данных о достижениях системных администраторов. Два основных способа мониторинга систем – это (1) сбор исторических данных, связанных с доступностью и применением, и (2) осуществление мониторинга в реальном времени, чтобы обеспечить оповещения о сбоях для системных администраторов.

Исторический мониторинг используется для записи статистических данных долговременной работы, использования и производительности. У него есть два компонента: сбор данных и просмотр данных. Результатами исторического мониторинга являются, например, такие выводы: «Веб-служба работала в прошлом году 99,99% времени, это выше 99,9% в позапрошлом году». Данные по использованию применяются для планирования ресурсов сети. Например, вы можете посмотреть на график использования пропускной способности соединения с Интернетом в прошлом году. График может визуально отображать темпы

роста, показывая, что канал будет заполнен через 4 месяца. Распространенными средствами исторического мониторинга являются Cricket и Orca.

Мониторинг в реальном времени предупреждает группу системного администрирования о сбое сразу же, как только тот происходит, и имеет два элемента: мониторинг, который обнаруживает сбои, и предупреждение, которое оповещает кого-либо о сбое. Знание системы о том, что что-то сломалось, бессмысленно, если она не сообщит кому-то о проблеме. Задача группы системных администраторов – обнаруживать сбои до того, как их заметят пользователи. Это приводит к снижению времени отключения и устранению проблем до их обнаружения пользователями, а также создает впечатление высококачественного обслуживания группы. Распространенными системами мониторинга в реальном времени являются Nagios и Big Brother.

Обычно два типа мониторинга осуществляются различными системами. Задачи, выполняемые при каждом типе мониторинга, сильно различаются. После прочтения этой главы вы должны хорошо представлять себе, чем они различаются, и знать, на что обращать внимание при выборе программ для каждой задачи.

Но сначала несколько предупреждений. Мониторинг использует пропускную способность сети, поэтому убедитесь, что он не требует слишком многого. Мониторинг потребляет ресурсы процессора и памяти; вряд ли вам захочется, чтобы он ухудшал ваше обслуживание. В системах мониторинга важна безопасность.

- В локальной сети *пропускная способность сети* обычно не слишком важна. Однако при низкоскоростных – обычно дальних – соединениях мониторинг может забивать каналы, вызывая снижение быстродействия других приложений. Убедитесь, что вы знаете, какую пропускную способность используете для мониторинга. Практической нормой является использование не более чем 1% доступной пропускной способности. Постарайтесь оптимизировать свою систему мониторинга, чтобы она могла легко работать на низкоскоростных соединениях. Подумайте о размещении станций мониторинга в удаленных местах, где соединения с центром обладают низкой пропускной способностью, или об использовании системы прерываний, где устройства сообщают системе мониторинга о сбоях, а не системы опроса, в которой система мониторинга периодически проверяет состояние.
- В нормальных обстоятельствах разумная система мониторинга не будет потреблять так много *ресурсов процессора и памяти*, чтобы быть заметной. Однако вам следует протестировать ее в условиях сбоя. Что случится, если сервер мониторинга[1] отключится или не будет работать? Что произойдет при отключении сети? Кроме того, будьте осторожны с переходами с одной системы мониторинга на другую: не забудьте отключить старую службу, когда новая будет полностью работоспособной.
- *Безопасность* имеет значение в том смысле, что системы мониторинга могут иметь доступ к машинам или данным, которые могут стать жертвой злоумышленника. Либо злоумышленник может иметь возможность подменить систему мониторинга в реальном времени, посылая сообщения, показывающие проблему с сервером или службой. Лучше всего использовать жесткую аутентификацию между сервером и клиентом. Старые протоколы мониторинга, например SNMPv1, имеют слабую аутентификацию.

[1] Машина, которой сообщают данные все серверы.

22.1.1. Исторический мониторинг

Системы опроса с предварительно определенными интервалами могут применяться для сбора данных об использовании или других статистических данных с различных компонентов системы и для проверки, насколько хорошо работают службы, предоставляемые системой. Информация, получаемая при помощи такого сбора исторических данных, сохраняется и обычно применяется для построения временных графиков производительности системы, чтобы обнаружить или локализовать незначительную проблему, которая имела место в прошлом. В среде с письменно закрепленными нормами SLA исторический мониторинг является методом, используемых для наблюдения за выполнением SLA.

Сбор исторических данных часто используется из-за того, что системных администраторов интересует, нужно ли им модернизировать сеть, добавить серверу больше памяти или поставить более мощный процессор. Они могут интересоваться, когда им понадобится заказать больше дисков для группы, которая быстро потребляет дисковое пространство, или когда нужно увеличить емкость системы резервного копирования. Чтобы ответить на эти вопросы, системным администраторам нужно наблюдать за системами и собирать данные об их использовании за определенный период времени, позволяющие увидеть тенденции и пики использования. Есть много других применений исторических данных, например тарификация по интенсивности использования, обнаружение аномалий (см. раздел 11.1.3.7) и представление данных базе пользователей или руководству (см. главу 31).

Исторические данные могут потреблять большое дисковое пространство. Это можно смягчить при помощи сокращения данных или установки сроков хранения. **Сокращение данных** означает замену подробных данных средними значениями. Например, можно собирать данные об использовании пропускной способности каждые 5 мин. Однако сбор средних значений каждый час требует приблизительно на 90% меньше места. Часто подробные данные хранятся неделю, а для более старых данных детализация снижается до почасовых средних значений.

Установка сроков хранения данных контролирует их удаление. Можно решить, что данные старше двух лет вообще не нужно хранить. В качестве альтернативы такие данные можно хранить на съемных носителях (DVD или магнитных лентах) на случай, если они когда-нибудь понадобятся.

Ограничение потребления дискового пространства за счет сокращения данных или установки сроков их хранения влияет на уровень детализации или исторической перспективы, который вы можете обеспечить. Имейте в виду это соотношение, когда будете искать систему для сбора исторических данных.

В зависимости от того, как вы будете применять данные, собранные при историческом мониторинге, следует определить, какой уровень детализации вам необходимо поддерживать и в течение какого времени. Например, если вы используете данные для тарификации на основе интенсивности использования и выставляете счета ежемесячно, вам понадобится хранить все подробности в течение нескольких лет на случай жалоб пользователей. Затем вы можете архивировать данные и удалять подробные данные из сети, но сохранять графики, чтобы пользователи могли обратиться к ним для получения справочной информации. Однако, если вы просто применяете графики для анализа тенденций и оценки требований по ресурсам сети, вам может потребоваться система, которая хранит полные данные за последние 48 ч, умеренно подробную инфор-

мацию за последние 2 недели, еще менее подробную информацию за последние 2 месяца и очень сильно сокращенные данные за последние два года, с удалением всего, что старше 2 лет. Учитывайте, для чего вы собираетесь использовать данные и какой объем дискового пространства вам доступен, когда будете решать, насколько сильно сокращать данные. В идеальном случае объемы сокращения, осуществляемые системой, и сроки хранения данных должны быть изменяемыми.

Вам также потребуется учитывать, как система мониторинга собирает свои данные. Обычно система, которая осуществляет сбор исторических данных, будет опрашивать наблюдаемые системы с регулярными интервалами. В идеале интервал опроса должен быть изменяемым. Механизм опроса должен иметь возможность использования стандартной формы связи, например SNMPv2, а также обычные IP-механизмы, такие как эхо-сообщения (ping) протокола управляющих сообщений Интернета ICMP и открытие TCP-соединения на любом порте, отправка определенных данных по этому соединению и проверка полученного ответа на соответствие шаблону. Кроме того, полезно иметь систему мониторинга, которая фиксирует информацию о задержке, или времени транзакции. Задержка тесно связана с ощущениями конечных пользователей. Когда служба отвечает очень медленно – это практически то же самое, как если бы она не отвечала вообще. Система мониторинга должна поддерживать максимально возможное количество других механизмов опроса, предпочтительно включающих механизм получения данных из любого источника и анализа результатов запроса. Важной является возможность добавлять свои собственные тесты, особенно в сильно индивидуализированных системах. С другой стороны, масса предварительно определенных тестов также полезна, чтобы вам не пришлось писать все с нуля.

Результаты, которые обычно требуются вам от этого типа систем мониторинга, – это графики, имеющие четкие единицы измерения по каждой оси. Вы можете применять эти графики, чтобы узнать, каковы тенденции использования, или чтобы обнаружить проблемы, например внезапные, неожиданные пики либо провалы интенсивности использования. Вы можете воспользоваться этими графиками, чтобы предсказать, когда вам потребуется увеличить какой-либо ресурс сети, для помощи в процессе планирования бюджета, который рассмотрен более подробно в главе 34. Кроме того, график является удобной формой документации для передачи по цепи руководства. График четко отображает вашу точку зрения, и ваши руководители оценят наличие у вас надежных данных при поддержке вашего запроса на увеличение пропускной способности, памяти, дискового пространства или чего-либо еще, что вам нужно.

22.1.2. Мониторинг в реальном времени

Системы мониторинга в реальном времени сообщают вам, что узел отключен, служба не отвечает или возникла какая-то другая проблема. Система мониторинга в реальном времени должна иметь возможность наблюдать за всем, что, по вашему мнению, может быть признаком проблемы. Система должна иметь возможность как опрашивать состояние систем и приложений, так и получать от них сообщения напрямую, если они обнаружат проблему в любое время. Как и в случае с историческим мониторингом, система должна иметь возможность использования стандартных механизмов, таких как опрос SNMPv2, прерывания SNMPv2, эхо-сообщения ICMP и TCP, а также предоставлять механизм для внедрения других форм мониторинга.

Система также должна иметь возможность отправлять сообщения различным получателям при помощи разных механизмов, таких как электронная почта, пейджинговая связь, телефон и открытие заявок на устранение неисправности. Сообщения должны отправляться нескольким получателям, потому что сообщение, отправленное одному человеку, может не дойти до него из-за того, что у его пейджера или телефона села батарейка либо он был занят или отвлечен чем-то еще.

Требования по хранению информации в системе мониторинга в реальном времени минимальны. Обычно она хранит предыдущий результат каждого запроса и время, прошедшее после последнего изменения состояния. Иногда система хранит скользящие средние значения или отметки высоких и низких значений, но редко сохраняет что-то большее. В отличие от исторического мониторинга, который используется для предупреждающего системного администрирования, мониторинг в реальном времени применяется для улучшения системного администрирования при реакции на проблемы.

При оценке системы мониторинга обратите внимание на объекты, за которыми она может наблюдать сама по себе, чтобы оценить, насколько она соответствует вашим требованиям. Вы должны рассматривать как мониторинг доступности, так и мониторинг ресурсов. **Мониторинг доступности** означает обнаружение сбоев узлов, приложений, сетевых устройств, других устройств, сетевых интерфейсов или подключений любого вида. **Мониторинг ресурсов** означает обнаружение момента, в который какой-либо компонент вашей инфраструктуры становится перегруженным или приближается к этому состоянию. Таким компонентом может быть, например, процессор, память, дисковое пространство, файл подкачки, резервное устройство, сетевое или любое другое соединение для передачи данных, устройство удаленного доступа, количество процессов, доступные порты, ограничения приложений или число пользователей в системе. Как и в случае с системами исторического мониторинга, система должна быть гибкой, чтобы можно было создавать собственные тестовые модули. Предпочтительно система должна иметь возможность использовать одни и те же модули для мониторинга как в реальном времени, так и исторического.

Наиболее важными компонентами системы мониторинга в реальном времени являются механизм уведомления и процессы, которые создаются в вашей компании для обработки уведомлений или предупреждений.

22.1.2.1. SNMP

SNMP расшифровывается как Simple Network Management Protocol (Простой протокол управления сетью). Но никто не знает точно, относится ли слово *«простой»* (Simple) к *сетям* (Networks) или *протоколу* (Protocol). Проблемы с SNMP затрудняют его использование в сетях, которые не являются простыми. Несмотря на попытку сделать его простым, сам по себе протокол довольно сложный.

В самой простой форме SNMP сетевому устройству, например маршрутизатору, отправляется пакет с вопросом, называемым `GET`. Например, можно спросить «Каково значение `IF-MIB::ifOutOctets.1`?». Эта переменная находится в группе переменных, связанных с интерфейсами (`IF`), и хранит количество байтов (октетов), отправленных через интерфейс (`ifOutOctets`), на интерфейсе номер 1. Маршрутизатор отвечает пакетом, содержащим значение.

Такие переменные существуют практически обо всем и для любых технологий. Группа связанных переменных называется MIB. Существуют стандартные MIB

для устройств Ethernet, DSL, ATM, SONET, T1/E1 и даже для несетевых технологий: дисков, принтеров, процессоров, процессов и т. д.

Можно воспользоваться другими типами пакетов для изменения переменной (`PUT`) и даже специальным пакетом, который означает «ответить на этот пакет, когда конкретная переменная станет выше/ниже определенного значения». Они называются *ловушками* (или прерываниями).

Простота SNMP также является его недостатком. В каждом пакете запрашивается одна переменная. Если вы хотите отслеживать пять переменных для каждого интерфейса и в системе есть десятки интерфейсов и сотни устройств, вы будете отправлять очень много пакетов. В системах мониторинга, основанных на SNMP, для своевременного сбора всей необходимой информации используются сложные схемы. Когда некоторые устройства далеко, а задержка высока, ожидание каждого ответа перед отправкой следующего запроса снижает быстродействие. Более поздние версии SNMP поддерживают запрос нескольких переменных в одном пакете, но не всегда.

Кроме того, с SNMP связаны проблемы безопасности. Устройства, поддерживающие SNMP, запрашивают в пакете пароль, называемый почему-то *строкой имени и пароля*, чтобы не позволить собирать данные любому желающему. `GET` имеет по умолчанию пароль `public`, а `PUT` — пароль `private`. К счастью, большинство производителей не предоставляют важных данных в переменных, которые можно прочитать при помощи `GET` и полностью отключают `PUT`. В версиях SNMP 2 и 3 пароль зашифровывается, что является улучшением. Однако наличие одного и того же пароля для нескольких устройств не очень безопасно. Если бы вам пришлось менять пароль SNMP для каждого маршрутизатора в своей организации каждый раз, когда из компании уходит системный администратор, в крупных компаниях пароли менялись бы постоянно.

Большинство устройств можно настроить таким образом, чтобы разрешать SNMP-запросы только с определенных IP-адресов. Мы рекомендуем выделить один или два определенных диапазона IP-адресов, на которых будут располагаться все SNMP-клиенты, и настроить все устройства с поддержкой SNMP отвечать только устройствам из этих диапазонов.

Данные в SNMP-пакете кодируются в формате, называемом ANS.1. Этот формат очень сложный, и его трудно реализовать. В 2002 году всех сильно напугало, что многие маршрутизаторы в Интернете имели уязвимость безопасности в своих программах по декодированию ANS.1. В некоторых случаях уязвимость безопасности могла быть использована в процессе проверки пароля, поэтому было неважно, знал ли злоумышленник ваши пароли.

Ситуация серьезно улучшилась. Однако мы даем следующие пять рекомендаций для всего оборудования с поддержкой SNMP.

1. Конфигурируйте сеть таким образом, чтобы она обрабатывала SNMP-пакеты только из определенных диапазонов IP-адресов. Целесообразно использовать два диапазона, по одному для каждого из дублирующих друг друга центров сетевого мониторинга.
2. Используйте SNMPv3, когда поставщик его поддерживает. Зашифровывайте все пароли.
3. Изменяйте пароли SNMP раз в год. Предусмотрите период перехода, в течение которого будут приниматься как старые, так и новые пароли.

4. Автоматизируйте еженедельную проверку всех сетевых устройств. Попытайтесь воспользоваться всеми предыдущими паролями SNMP, которые должны быть уничтожены, из одного из проверенных участков сети. Кроме того, попробуйте воспользоваться `public`, `private` и другими паролями по умолчанию. Чтобы найти список паролей по умолчанию для сетевых устройств разработчика, нужен всего лишь небольшой поиск в Интернете. Проверьте их все. Теперь повторите этот тест вне назначенных участков сети.
5. Следите за бюллетенями безопасности разработчика, связанными с SNMP. Новые уязвимости появляются несколько раз в год.

22.1.2.2. Механизм оповещения

В системе мониторинга есть механизм оповещения, чтобы сообщить вам о том, что где-то требуется участие человека. Знание программы о том, что что-то отказало или перегружено, не имеет смысла, если она не сообщает об этом человеку или принимает какие-то меры и информирует об этом, чтобы человек смог проверить позже.

Механизм оповещения системы мониторинга не должен зависеть ни от каких компонентов системы, которая находится под наблюдением. Если какая-либо ошибка не позволяет системе мониторинга сообщить о ней, то структуру механизма оповещения нужно изменить. Электронная почта является популярным механизмом оповещения, но она не должна быть единственным средством. Электронная почта может не дойти или идти долго. Предупреждение должно быть быстрым. Кроме того, учитывайте, может ли механизм оповещения отслеживаться третьими сторонами. Беспроводная связь, например пейджинговая, подвержена перехвату информации третьими лицами. Как минимум, не отправляйте по этим каналам важную информацию, например пароли, и проверяйте, является ли достоверной такая информация, как «Магистральный маршрутизатор отключен на 45 минут».

Вне зависимости от того, какой системой мониторинга вы пользуетесь, вам потребуется политика, которая описывает, как обрабатываются сообщения. Прежде чем вы сможете реализовать мониторинг в реальном времени, эта политика должна ответить на некоторые принципиальные вопросы. Какому количеству людей отправляются предупреждения? Идут ли предупреждения в службу поддержки, или сотрудникам, ответственным за компоненты, в которых обнаруживаются проблемы, или в оба места? Как получатели предупреждений координируют свою работу, чтобы все знали, кто с какой проблемой работает, и не мешали друг другу? Если проблема не будет решена за некоторое предварительно определенное время, захотите ли вы передать ее на более высокий уровень? Если да, по какому пути будет идти эта передача. Насколько часто вы хотите получать информацию о проблеме и зависит ли это от характера проблемы? Как вы хотите получать информацию о проблеме? Какова степень серьезности каждой проблемы? Может ли степень серьезности использоваться для определения политики урегулирования проблемы? Ваши системы мониторинга и оповещения должны иметь возможность реализации вашей политики.

При выборе системы мониторинга в реальном времени обращайте внимание на то, что сказано в вашей политике относительно того, как и насколько часто вы хотите получать сообщения о проблемах. Например, если вы реализуете механизм раннего оповещения о проблемах ресурсов, вам может понадобиться, чтобы он открывал заявку на устранение неисправности в имеющейся у вас системе службы поддержки. Возможно, вы также захотите, чтобы он делал это,

только когда значение наблюдаемого параметра изменяется с приемлемого на неприемлемое, а не каждый раз, когда оно фиксируется как неприемлемое, что может происходить каждые несколько минут, хотя, возможно, вы захотите обновлять имеющуюся заявку, если проблема остается после истечения определенного настраиваемого интервала. С другой стороны, если система мониторинга обнаруживает сбой, особенно критического компонента, вы, скорее всего, захотите, чтобы она постоянно сообщала об этом кому-то дежурному. Может быть, вы даже захотите, чтобы она продолжала сообщать об этом человеку каждый раз, когда она обнаруживает, что ошибка все еще присутствует, с информацией о том, сколько времени это продолжается. Вы можете захотеть, чтобы, пока проблема существует, сообщения отправлялись чаще или реже. Ваша система мониторинга должна быть гибкой в используемых формах оповещения и позволять вам пользоваться различными механизмами оповещения для разных типов проблем.

Предупреждения об ошибках, которые система отправляет, должны быть ясными и простыми для понимания. Если получатели предупреждения должны искать дополнительную информацию или обращаться к другому человеку, чтобы перевести предупреждение в понятную форму, сообщение не является достаточно понятным. Например, сообщение об ошибке «`SNMP запрос на 10.10.10.1 для 1.2.3.4.5.6.7.8.9.10 не прошел`» не так понятно, как «`Интерфейс Hssi4/0/0 на маршрутизаторе wan-router-1 не работает`». Аналогично, «`Соединение с портом 80 на 10.10.20.20 не установлено`» не так понятно, как «`Веб-сервер на www-20 не отвечает`».

Однако сообщение не должно сообщать о предположениях, которые могут оказаться неверными. Например, если в сообщении сказано «`Веб-сервер на www-20 не работает`», а не «не отвечает», системный администратор может проверить, работает ли он, и посчитать предупреждение ложной тревогой, а не проверять, завис ли сервер или не отвечает по какой-либо другой причине.

Я вся горю! Я тону!

Однажды очень рано утром в одной семье позвонил домашний телефон. Жена проснулась, взяла трубку и услышала страстный женский голос, который говорил: «Я вся горю. Я тону». Она подумала, что это розыгрыш, и положила трубку. Через полчаса тот же звонок повторился. После четвертого звонка муж наконец проснулся, взял трубку и выпрыгнул из кровати.

Это была система аварийного предупреждения в его серверной. Система вентиляции и кондиционирования вышла из строя, вода из нее вылилась на пол. Система звонила ему. Разработчик не сказал ему, как звучит сигнал предупреждения, а просто попросил прописать свой номер телефона в определенном файле конфигурации. Проверьте свою систему оповещения и сообщите о ней тем, кто может столкнуться с нею вместо вас.

22.1.2.3. Передача на более высокий уровень

Другой элемент политики и процедур, который должна реализовывать ваша система мониторинга и оповещения, – это политика передачи на более высокий

уровень, предписывающая, какое время может существовать проблема до ее передачи другому человеку, обычно руководителю. Политика передачи на более высокий уровень обеспечивает, что, даже если человек, получающий предупреждение, находится в отпуске или не отвечает, проблема будет передана кому-нибудь еще. В политике передачи на более высокий уровень нужно описывать различные пути передачи для разных категорий предупреждений.

Пример: процедура передачи

В одной системе собственной разработки имелась особенно сложная процедура передачи. Система могла быть сконфигурирована при помощи таблицы ответственности, которая распределяла службы по ответственным лицам. Они могли быть физическими лицами или группами людей. Конфигурация системы могла быть настроена при помощи графиков отпусков, поэтому система знала, кого предупреждать не надо. Если проблема оставалась, система могла пойти вверх по цепи ответственности к сотрудникам, стоящим все выше и выше на служебной лестнице. У каждого типа службы – электронной почты, Веб, DNS и т. д. – была собственная конфигурация, а определенные системы – прокси-сервер генерального директора, веб-сайт электронной коммерции и т. д. – могли быть отмечены как критические, и в этом случае передача шла быстрее. У каждой службы было ответственное лицо по умолчанию, но можно было сделать исключение для систем с особыми требованиями. Все это обеспечивало очень эффективное оповещение.

Вы также можете захотеть иметь возможность подтвердить получение экстренного сообщения, чтобы сообщения перестали отправляться на определенное время, до подтверждения вручную, до исправления проблемы или при какой-либо комбинации этих условий в зависимости от политики. Это аналогично кнопке повторения сигнала на будильнике. Подтверждение является признаком того, что вы активно работаете над проблемой, и избавляет вас от раздражающих постоянных сообщений, когда вы пытаетесь исправить неполадку. Без этой функции очень заманчиво отключить предупреждение, однако это приводит к тому, что забывают устранить проблему или, что еще хуже, вновь включить предупреждение.

22.1.2.4. Системы активного мониторинга

Система активного мониторинга обрабатывает проблемы, которые обнаруживает, и активно устраняет те из них, которые может устранить. Например, система активного мониторинга может сбросить порт модема, если обнаружит его странное состояние, или отключить модем от модемного пула, если неполадку не удалось исправить при помощи сброса.

Системы активного мониторинга могут быть полезны до определенного момента. Несмотря на то что они реагируют быстрее человека, у них есть ограничения. Обычно система активного мониторинга может реализовать только временные меры. Система не способна обнаружить корень проблемы и принять постоянные меры, которые на самом деле необходимы (см. главу 16). Кроме того, нужно убедиться, что система активного мониторинга сообщает о том, что она делает,

и открывает заявку на принятие постоянных мер. Однако системным администраторам может быть сложнее обнаружить реальный источник проблемы, когда были приняты постоянные меры. Системные администраторы также должны не идти на поводу у лени и не забывать принимать постоянные меры для устранения проблем, которые выявила система активного мониторинга. Если системные администраторы просто автоматизируют временные меры при помощи системы активного мониторинга, рано или поздно все придет в беспорядок и система в целом станет менее надежной.

Пример: активный мониторинг и неправильные «меры»

В одной компании система активного мониторинга отслеживала директорию /var и обновляла файлы логов, когда диск заполнялся. Она удаляла самый старый файл лога и таким образом освобождала пространство. В какой-то момент файлы логов стали обновляться каждый раз, когда система мониторинга проверяла диск, и было невозможно посмотреть файлы логов в разделе /var, потому что к тому времени они все имели нулевую длину.

Оказалось, что разработчик включил отладку одного из своих процессов, который каждую минуту запускался при помощи хрона[1]. Таким образом, задание хрона каждую минуту отправляло сообщение электронной почты. Почтовый ящик (расположенный в /var/mail) заполнил диск.

Также системы активного мониторинга имеют ограничение в плане проблем, которые они могут решать, даже временно. Некоторые проблемы, которые система может обнаружить, но не может устранить, связаны с физическими неисправностями, например отсутствием в принтере чернил или бумаги либо его выключением или отключением от сети. Если система не определяет источник неполадки точно и пытается исправить ее при помощи программных команд, то она рискует создать больше проблем, чем решить. Другие проблемы могут требовать сложной отладки, и нереально ожидать от автоматизированной системы возможности точно определить все такие проблемы. В частности, проблемы, которые требуют отладки на нескольких узлах и элементах сетевого оборудования, например медленную передачу файлов между двумя узлами в устойчивой сети, не способна решить ни одна из известных нам автоматизированных систем.

В любом случае хорошая идея – ограничить то, что может делать автоматизированная система. С точки зрения безопасности автоматизированная система, имеющая привилегированный доступ ко всем машинам или к их большинству, очень уязвима для злонамеренного использования. Основное внимание при создании таких систем всегда уделяется функциональности, а не безопасности, и системы активного мониторинга являются большими, сложными программами, имеющими привилегированный доступ к некоторым машинам, поэтому неизбежны уязвимости безопасности. Кроме того, такие системы являются

[1] Хрон – демон ОС UNIX, исполняющий предписанные команды в строго определенные дни и часы, указанные в специальном файле с именем crontab. – *Примеч. науч. ред.*

привлекательными целями в силу своего уровня привилегированного доступа во всей сети. Система активного мониторинга – это не то, что нужно вам в незащищенной сети. С точки зрения надежности чем больше этой программе разрешено делать в вашей сети, тем выше ущерб, который она может нанести, если выйдет из-под контроля.

22.2. Тонкости

Когда у вас будет базовый мониторинг и он начнет расширяться для наблюдения за бóльшим количеством устройств, вы захотите сделать систему мониторинга более доступной для других системных администраторов, чтобы все системные администраторы компании могли обслуживать свои списки устройств. Вы также начнете замечать проблемы, которые она упускает, и захотите наблюдать транзакции целиком, от начала и до конца. Другими словами, вместо того чтобы просто проверять, что почтовая машина работает и принимает SMTP-подключения, вы можете захотеть проверить, способна ли она доставить сообщение электронной почты. Кроме того, вы можете захотеть оценить, сколько времени занимает выполнение транзакций.

В конце концов вы, ваша группа и ваше руководство захотят наблюдать за все большим количеством объектом, пока вы не будете наблюдать за всем. Мы рассмотрим способы упростить расширение. Другое усовершенствование, которое может потребоваться вам в будущем, – это обнаружение устройств, чтобы вы знали, когда к сети подключаются новые устройства.

22.2.1. Доступность

Обычно система мониторинга устанавливается одним или двумя системными администраторами, которые разбираются с каждой ее деталью. Они – единственные люди, которые знают, как добавлять объекты для наблюдения, поэтому они также становятся теми, кто отвечает за все изменения и дополнения. Первоначально это может не требовать большого объема работы, но со временем система мониторинга станет более развитой и ее нагрузка возрастет.

Когда система мониторинга будет становиться все более устойчивой и стабильной, важно сделать ее доступной для группы в целом. Любой системный администратор должен сам уметь добавить что-то в список наблюдаемых объектов, а не подавать запрос конкретному системному администратору, который может быть занят другими задачами.

Обеспечение доступности системы мониторинга требует хорошей документации. Некоторые формы мониторинга могут потребовать поиска информации, которая обычно не используется при ежедневном администрировании, например SNMP MIB для компонента системы. Документация должна сообщать системному администратору, какая информация ему потребуется и как ее найти, а также как внести требуемые изменения в конфигурацию мониторинга. Если есть варианты выбора, например как часто объект должен опрашиваться, какие значения соответствуют какому уровню тревоги, какие приоритеты имеют проблемы, какие графики строить или как определять путь передачи на более высокий уровень, эти возможности также должны быть четко документированы. В данной ситуации ключом является документирование предпочтительных значений по умолчанию.

Если все запросы на дополнительный мониторинг должны направляться к одному или двум людям, это неудобно как системным администраторам, которые устанавливали систему, так и остальным системным администраторам в группе. Система, которая не доступна всей группе, не будет использоваться достаточно широко, и группа не получит от нее максимум пользы.

22.2.2. Тотальный мониторинг

В идеале хорошо иметь возможность наблюдать за всем или, по крайней мере, за всем вне рабочих станций. Это особенно важно для компаний, которые требуют очень высокой доступности, например для сайтов электронной коммерции. Если внесение систем и служб в список для наблюдения является задачей, выполняемой вручную, то периодически о ней будут забывать и пропускать ее. Чтобы мониторинг вашей службы был тотальным, он должен быть введен в процесс установки.

Например, если для предоставления обслуживания вы устанавливаете много одинаковых машин, вам следует пользоваться процессом автоматизированной установки, описанным в главе 3. Если вы устанавливаете машины таким образом, вы можете обеспечить внесение машины в число объектов системы мониторинга как часть этого процесса установки. В качестве альтернативы вы можете установить на машину какое-нибудь средство, которое активизируется, когда машина займет свое окончательное место назначения, – если вы размещаете машины в защищенной сети, – и обеспечить ему способ сообщить системе мониторинга о том, что машина работает и что за ней нужно наблюдать. Обеспечение тотального мониторинга требует некоторой степени автоматизации. Если такие задачи нельзя автоматизировать, процесс установки может, по крайней мере, автоматически создавать заявку в службу поддержки, которая будет требовать внесения машины в число объектов системы мониторинга.

22.2.3. Обнаружение устройств

Также может быть полезна система мониторинга, которая обнаруживает подключение новых устройств к сети. Такая система полезна там, где нужен тотальный мониторинг, потому что она должна обнаруживать любые устройства, которые остались незамеченными и не были внесены в число объектов системы мониторинга какими-либо другими способами. Также может быть полезно просто знать, что устройство было добавлено и когда это произошло. Например, если устройство вызывает проблему в сети, это знание может сэкономить несколько часов отладки.

22.2.4. Сквозное тестирование

Сквозное тестирование означает тестирование транзакций целиком, когда система мониторинга действует как пользователь службы и проверяет, что вся транзакция успешно завершена. Сквозное тестирование может быть относительно простым, например отправка сообщения электронной почты через почтовый сервер или запрос конкретных веб-страниц, который вызывает обращение к базам данных, и проверка отображенного содержимого. Оно может представлять собой более сложную проверку, имитирующую все шаги, которые делает пользователь, чтобы купить что-нибудь на вашем сайте электронной коммерции.

Пример: проверка почты

В AT&T, а затем в Lucent Джон Бэгли (John Bagley) и Джим Уиттхофф (Jim Witthoff) разработали систему проверки электронной почты. Она отправляет сообщения электронной почты (mailping) на почтовые серверы и измеряет время, которое прошло до его прихода обратно на исходную машину. В определенный момент она наблюдала 80 серверов электронной почты, в том числе SMTP-шлюзы как под UNIX, так и под MS-Exchange. Она предоставляет ряд веб-средств для отображения данных о времени доставки за определенный день либо для определенного сервера за указанный период. Помимо сбора исторических данных, в ней есть механизм создания предупреждений, если конкретное сообщение не было доставлено после истечения определенного порогового значения времени. Возможность сквозного мониторинга передачи электронной почты в компании позволила не только быстрее реагировать на проблемы, но и создать метрику, которая позволила совершенствовать службу со временем. Теперь некоторые коммерческие системы мониторинга предоставляют эту функцию.

Как только вы начнете осуществлять более широкий мониторинг, вы увидите проблемы, которые упускает ваша система мониторинга. Например, если вы предоставляете услуги электронной коммерции через Интернет, необходимо успешное выполнение последовательности действий, чтобы ваш пользователь смог завершить транзакцию. Ваша система мониторинга может показывать, что все работает, но конечный пользователь сталкивается с проблемой в осуществлении полной транзакции.

Транзакция может полагаться на то, за чем вы и не думали наблюдать или за чем наблюдать очень трудно. Например, если транзакция полагается на отправку электронной почты, что-то может быть не так с конфигурацией вашего почтового сервера, из-за чего будет невозможно правильно доставить сообщение, хотя сервер принимает электронную почту для доставки. Ошибка в приложении может привести к его зависанию, сбою или созданию «мусора» в определенный момент процесса. В базе данных могут отсутствовать некоторые таблицы. Многое может пойти не так и не быть обнаруженным вашей системой мониторинга.

Лучший способ убедиться, что служба, которую хотят использовать ваши пользователи, активна и работает правильно, – имитировать пользователя и проверить, что транзакция завершена успешно. В примере с сайтом электронной коммерции создайте тестовую ситуацию, запрашивая страницы в порядке, в котором их запрашивал бы пользователь, и проверяя содержимое отображаемых страниц на каждом этапе, чтобы убедиться, что там есть необходимые данные и ссылки. Проверьте базу данных, чтобы убедиться, что транзакция была записана в нужном месте. Проведите проверку авторизации кредитной карты и убедитесь, что она проходит успешно. Отправьте сообщение электронной почты и убедитесь, что оно доходит. Пройдите через каждый этап процесса, как это сделал бы пользователь, и убедитесь, что на каждом этапе все работает, как предполагалось.

Такое сквозное тестирование может выявить проблемы, которые в другом случае остались бы незамеченными до обращения пользователя с жалобой. Если в среде электронной коммерции проблема какое-то время не будет замечена, это может привести к серьезному ущербу. Существует крупный и растущий рынок

коммерческих систем мониторинга, многие из которых ориентированы на особые нужды электронной коммерции.

22.2.5. Мониторинг времени ответа приложений

Другой тип расширенного мониторинга, который может быть очень полезен как в корпоративной среде, так и в сфере электронной коммерции, – это мониторинг времени ответа приложений. Каждый компонент системы может работать, но, если система будет слишком медленной, вашим пользователям это не понравится. В среде электронной коммерции это означает, что вы будете терять бизнес. В корпоративной среде это приведет к потере производительности и многочисленным жалобам на медленную работу сети, системы или приложения. В любом случае, если вы не отслеживаете время реакции приложений, выяснение того, почему ваши клиенты недовольны, может занять определенное время, за которое ваша репутация рискует потерпеть серьезный ущерб.

Гораздо лучше найти способ отслеживать время ответа приложений, которое будет ждать конечный пользователь приложения. Затем полезно создать как временной график, так и какую-либо форму предупреждения о том, что время ответа превысило порог. Мониторинг времени ответа приложения обычно является расширением ранее рассмотренного сквозного тестирования. Если это возможно, такая информация может отправляться разработчикам приложения, чтобы помочь им в масштабировании и оптимизации своего продукта.

22.2.6. Расширение

Когда вы начнете наблюдать за некоторыми объектами и увидите, насколько полезен мониторинг, вы захотите наблюдать за бóльшим количеством аспектов работы своей компании. Повышение количества наблюдаемых объектов создает проблемы расширения. У всех систем мониторинга возникают проблемы при расширении. Простой сбор всех данных, которые нужно проверять каждые 5 мин, требует больших затрат времени. Он может дойти до момента, когда система мониторинга все еще пытается собрать и обработать данные из одного сеанса, а в это время уже начинается следующий.

Системам, выполняющим исторический мониторинг, обычно требуется дополнительная обработка для сокращения данных, которые они хранят. Некоторые устройства могут выдать запрашиваемую информацию только через некоторое время, а система обычно способна одновременно поддерживать ограниченное количество открытых запросов. Все это может привести к проблемам с расширением по мере того, как система будет наблюдать за бóльшим количеством объектов.

Пример: проблемы расширения

В WebTV Networks пользовались MRTG (Oetiker 1998a) для наблюдения за сетевым оборудованием и составления исторических графиков. По мере роста сети появились проблемы производительности: каждый сеанс мониторинга требовал такого большого объема обработки, что данные еще обрабатывались, когда начинался следующий сеанс. Эксплуатационный персонал сети в конце концов написал новое приложение, названное Cricket (Allen 1999), которое было более эффективным.

При расширении системы мониторинга на тысячи объектов в крупной сети сетевые каналы могут быть перегружены просто трафиком мониторинга. Чтобы решить эту проблему, в некоторых системах мониторинга есть удаленные зонды, которые собирают данные и отправляют главной станции только выводы. Если эти зонды стратегически размещены в сети, они могут существенно снизить объемы генерируемого сетевого трафика. Главная станция хранит данные и обеспечивает их доступность системным администраторам. Кроме того, главная станция содержит основную конфигурацию и распространяет ее на удаленные станции мониторинга. Следует заметить, что эта модель обладает лучшей масштабируемостью, чем одна станция мониторинга или несколько несвязанных станций.

Системы мониторинга в реальном времени также имеют проблемы с расширением. Когда такая система отслеживает много характеристик большого количества устройств, всегда будут объекты в «красном» состоянии, подверженные какому-либо сбою и требующие внимания. Чтобы правильно расширять систему, системные администраторы должны иметь возможность сразу сказать, какая из «красных» проблем «самая красная» и имеет наибольшее значение. В принципе, проблема заключается в том, что система мониторинга обычно имеет только несколько значений для индикации состояния наблюдаемого объекта. Часто их всего три: «зеленый», «желтый» и «красный». Мониторинг большого количества объектов требует более точной градации. Например, можно встроить очень подробную систему приоритетов и система оповещения сможет отображать проблемы в порядке их приоритета.

Другая распространенная проблема заключается в том, что сбой элемента сети без резервирования между системой мониторинга и наблюдаемыми объектами может вызвать огромный поток сообщений об ошибках в системе мониторинга, хотя на самом деле сбой будет один. Поток предупреждений может скрыть реальную причину проблемы и вызвать панику у людей, которые их получают. В идеальном случае в системе мониторинга должен поддерживаться принцип цепочек взаимосвязей. Цепочка взаимосвязей объекта, за которым наблюдает система, содержит другие сбои, которые могут вызвать появление информации о сбое данного объекта. Затем система мониторинга должна использовать цепочку взаимосвязей для изменения своих предупреждений. Например, вместо того чтобы отправлять 50 сообщений на пейджер, она может отправить одно, в котором говорится: «Множественные сбои: основная причина...», и указать только самый первый сбой в цепочке, а не следующие за ним. В графическом формате она может показать сбои вместе с цепочками взаимосвязей в виде соответствующей древовидной структуры, чтобы основная причина была четко видна. Это нетривиальная в реализации и обслуживании функция, и она вряд ли будет доступна в каждой системе мониторинга. Если в вашей системе мониторинга нет такой функции составления сводок об ошибках, у вас может быть возможность реализовать что-то подобное за счет наличия нескольких удаленных станций мониторинга, особенно в глобальной сети. Центральная система мониторинга будет предупреждать системных администраторов, когда она не сможет получить сообщение от удаленных систем мониторинга, иначе будут поступать сообщения о проблемах, обнаруженных удаленными системами. В качестве альтернативы вы можете обучить свой персонал, как действовать в таких ситуациях, и поддерживать актуальные схемы взаимосвязей, к которым они смогут обратиться в случае потока предупреждений.

Другая проблема с расширением системы мониторинга в реальном времени связана с тем, как обрабатываются проблемы. Если несколько человек одновре-

менно пытаются без координации решить одну и ту же проблему, не зная, что другие люди над ней работают, они могут ухудшить положение. В самом лучшем случае будет зря потрачено много времени. Кроме того, они будут мешать друг другу и делать неверные предположения о том, что происходит в системе. В системе мониторинга должен быть какой-то способ, позволяющий системному администратору «заявить» о проблеме, чтобы остальные системные администраторы знали, что кто-то над ней работает и к кому обращаться, если они хотят помочь. Это может быть реализовано через систему заявок на устранение неполадок и процедуры, связанные с выдачей задания по проблеме перед началом работы над ней системного администратора.

22.2.7. Метамониторинг

Метамониторинг – это мониторинг вашей системы мониторинга, то есть средство, позволяющее убедиться, что ваша система мониторинга не отказала. Если вы не получали предупреждений в течение трех дней, означает ли это, что все хорошо, или кто-то отключил машину, которая обрабатывает предупреждения? Компании часто забывают следить за своими системами мониторинга, а когда происходит сбой, о нем просто не предупреждают.

Самая простая форма метамониторинга – обеспечить, чтобы система мониторинга наблюдала несколько простых собственных показателей, например заполнение своего собственного диска. Предупреждения об этом должны появляться задолго до состояния, которое не позволит системе мониторинга работать.

При мониторинге большего количества устройств или если работоспособность очень важна, имеет смысл использование второй системы мониторинга, которая наблюдает только за основной системой мониторинга.

Метамониторинг должен быть основан на SLA, как и любая другая система мониторинга. Например, если вы предполагаете, что основная система мониторинга сможет выполнять все свои запросы каждые 10 мин, метамониторинг должен предупреждать, если запрос не выполняется более 10 мин.

Если система в соответствии с SLA могла в течение нескольких недель выполнять полный цикл запросов, а теперь это вдруг не получается, в ситуации нужно разобраться. Если такое состояние сохраняется, то, возможно, причина заключается в сбое жесткого диска, неправильной конфигурации сети или выходе процесса из-под контроля. Кроме того, это может показывать, что кто-то случайно нарушил конфигурацию.

Исторический метамониторинг может фиксировать, как система отвечает на растущее число запросов. По мере роста количества наблюдаемых служб системе понадобится больше времени, чтобы опросить их все. Сбор исторических данных может помочь спрогнозировать момент, в который система мониторинга больше не сможет удовлетворять требованиям SLA. Чтобы предотвратить перегрузку системы мониторинга, можно воспользоваться методами расширения.

22.3. Заключение

В данной главе мы рассмотрели мониторинг в двух аспектах: сбор исторических данных и мониторинг и оповещение в реальном времени. Эти две формы довольно сильно отличаются в плане состава и предназначения, но вам нужно учитывать некоторые проблемы, общие для обоих типов.

Исторический мониторинг доступности и сбор данных означают отслеживание доступности и использования систем для дальнейшего отражения данных на графике и анализа. Он включает сбор, хранение и сокращение больших объемов данных. Сбор исторических данных требует больших объемов дискового пространства, баз данных и обработки. Он полезен для планирования ресурсов сети, обоснования бюджета, тарификации пользователей, предоставления обзора происходящего в системе при обнаружении проблем и аномалий.

Мониторинг в реальном времени предполагает опрос систем для проверки их состояния и ожидание сообщений о проблемах от собственных средств мониторинга систем. Мониторинг в реальном времени обычно объединен с системой оповещения. Эта комбинация используется для обнаружения проблем и предупреждения о них системных администраторов (почти) сразу же после того, как они происходят. Это средство предоставления лучшего обслуживания и обнаружения первопричины проблемы. Оно предоставляет более точную информацию, чем сообщения от пользователей о проблемах типа «Я не могу загрузить свою почту».

Оба типа мониторинга необходимы сайтам электронной коммерции, потому что их пользователи более удаленные и менее терпеливые – им все равно, знаете ли вы о проблеме или исправляете ли ее, потому что они могут просто уйти на другой сайт. Мониторинг в обеих своих формах – прекрасное средство для любого хорошо организованного сайта.

У обеих форм мониторинга возникают проблемы, когда дело касается расширения, и разделение системы мониторинга на несколько пунктов сбора данных и один центр в обоих случаях является наилучшим методом. Мониторинг в реальном времени имеет проблемы расширения, связанные с назначением приоритетов и приемлемой, своевременной и скоординированной реакцией на предупреждения.

По мере развития вашей системы мониторинга вы захотите реализовать сквозное тестирование и тестирование времени ответа приложений, чтобы точно знать, через что проходит конечный пользователь и приемлемо ли это. Кроме того, вам могут потребоваться методы проверки того, что все отслеживается правильно, особенно если вы занимаетесь предоставлением услуг. Для этого вы можете обратиться к способам добавления системы в список мониторинга после его создания. Кроме того, вы можете обратиться к способам обнаружения подключения устройств к сети, а не системе мониторинга.

Мониторинг – очень полезное средство. Кроме того, он является проектом, охват которого будет расширяться после реализации. Знание направлений, по которым системе потребуется развиваться, поможет в выборе подходящих систем мониторинга в начале проекта, их расширении и добавлении функциональности по необходимости в течение их жизненного цикла.

Задания

1. Как вы осуществляете мониторинг систем, за которые отвечаете? Если у вас нет формальной системы мониторинга, автоматизированы ли какие-либо аспекты вашего несистематического мониторинга?
2. Выполняете ли вы активный мониторинг чего-либо в вашей среде? Если да, насколько хорошо он работает? Мешает ли он вам находить первопричины проблем? Объясните, почему.

3. Какие системы вы добавили бы в систему мониторинга, если бы она у вас была, и почему? Какие аспекты этих систем вы хотели бы отслеживать?
4. Если у вас уже есть система мониторинга, как вы могли бы ее улучшить?
5. Какие возможности, рассмотренные в данной главе, являются для вас наиболее важными при выборе системы мониторинга для своей компании и почему?
6. Какие не рассмотренные возможности (если они есть) важны для вас и почему?
7. Рассмотрите бесплатные системы мониторинга исторических данных. Какая из них, по вашему мнению, лучше всего подойдет для вашей среды и почему?
8. Рассмотрите коммерческие системы мониторинга исторических данных. Какая из них, по вашему мнению, лучше всего подойдет для вашей среды и почему?
9. Если бы вам пришлось выбирать между бесплатной и коммерческой системами мониторинга исторических данных, которые вы выбрали в предыдущих вопросах, какую из них вы предпочли бы приобрести для своей компании и почему? Каких функций, по вашему мнению, ей не хватает, если такие есть?
10. Рассмотрите бесплатные системы мониторинга в реальном времени. Какая из них, по вашему мнению, лучше всего подойдет для вашей среды и почему?
11. Рассмотрите коммерческие системы мониторинга в реальном времени. Какая из них, по вашему мнению, лучше всего подойдет для вашей среды и почему?
12. Если бы вам пришлось выбирать между бесплатной и коммерческой системами мониторинга в реальном времени, которые вы выбрали в предыдущих вопросах, какую из них вы предпочли бы приобрести для своей компании и почему? Каких функций, по вашему мнению, ей не хватает, если такие есть?
13. Как вы думаете, на какое количество объектов – машин, сетевых устройств, приложений и т. д. – потребуется расширить вашу систему в следующие три года? Что вам понадобится, чтобы выполнить это требование?
14. Есть ли какие-либо преимущества и недостатки в использовании одной программы для обоих типов мониторинга, если это возможно?

Глава 23

Служба электронной почты

Электронная почта – это служба, от которой зависит бизнес любой компании. Все ожидают, что электронная почта просто будет всегда работать, сбои здесь недопустимы. Часто она является единственным приложением, которым пользуется генеральный директор. Впечатление вашего генерального директора о надежности электронной почты может иметь долгосрочное влияние на другие аспекты деятельности группы системных администраторов, такие как бюджет и репутация.

Около 45% информации, важной для бизнеса, находится в сообщениях электронной почты (Osterman 2000). Для многих компаний это один из основных способов существования, а для потенциальных клиентов – способ связи с персоналом продаж и поддержки. Основное внимание в электронной почте должно уделяться надежности, следом за ней идет расширяемость.

Если вам требуется построить успешную систему электронной почты, у вас также должны быть хорошие пространства имен (глава 8), архитектура безопасности (глава 11), мониторинг служб (глава 22) и резервные копии (глава 26).

23.1. Основы

Надежная, масштабируемая служба электронной почты должна строиться на прочной основе. Системный администратор, который проектирует и строит службу электронной почты, должен обеспечить основу в первую очередь, прежде чем пытаться добавлять функции или расширять службу для работы с бóльшими объемами трафика.

Простая, понятная, хорошо документированная архитектура системы электронной почты является основой построения надежной службы. Кроме того, важно пользоваться открытыми протоколами и стандартами во всей системе электронной почты, чтобы обеспечить возможность максимального взаимодействия с другими системами и другими приложениями в системе. В частности, один из ключевых элементов инфраструктуры, с которым требуется взаимодействовать системе электронной почты, – это система управления пространством имен, которая реализует организационную структуру корпоративных пространств имен, связанных с электронной почтой. Вспомните из главы 5: сервис не может называться сервисом, пока не выполняется мониторинг.

Электронная почта – это способ связи с остальным миром, поэтому некоторые элементы этой службы всегда будут целями для потенциальных злоумышлен-

ников. Следовательно, во время проектирования и реализации системы электронной почты должна учитываться безопасность.

Наконец, в силу того что электронная почта содержит так много жизненно важной информации, вопросы неприкосновенности электронной почты и ее хранения должны быть изучены и приведены в соответствие с политикой компании и любыми нормативно-правовыми требованиями.

23.1.1. Политика неприкосновенности

В каждой компании должна быть политика неприкосновенности электронной почты, доведенная до каждого сотрудника. Политика неприкосновенности должна описывать, кто и при каких обстоятельствах может читать электронную почту пользователя. Политика также должна разъяснять, что электронную почту может непреднамеренно просмотреть персонал администрирования при выполнении своей работы, обычно при проведении диагностики. Кроме того, политика должна указывать, что электронная почта, которая проходит через другие сети, например Интернет, не может считаться частной и незашифрованная конфиденциальная информация компании не должна отправляться через сети других лиц или на адреса в таких сетях.

Во многих компаниях электронная почта, приходящая на корпоративные серверы или проходящая через них, не считается частной. В других компаниях указывают, что корпоративные машины не должны использоваться для личного общения, что обычно сводится к тому же самому. Некоторые компании автоматически просматривают входящую и исходящую электронную почту на наличие определенных ключевых слов, некоторые доходят до проверки прикрепленных файлов на наличие потенциально конфиденциальной информации. Другие компании указывают, что люди, использующие корпоративную электронную почту, могут считать ее неприкосновенной, но перечисляют обстоятельства, при которых правила неприкосновенности могут больше не выполняться.

Вне зависимости от того, какая политика установлена высшим руководством компании, системные администраторы должны ее реализовывать. Группа системных администраторов должна обеспечить, чтобы каждый, кто пользуется службой корпоративной электронной почты, был в курсе политики и подтвердил это.

23.1.2. Пространства имен

Пространства имен рассмотрены в главе 8, здесь мы сосредоточимся на пространстве имен электронной почты. Пространство имен для адресов электронной почты компании является наиболее заметным как извне, клиентам и деловым партнерам компании, так и изнутри, сотрудникам, которые ежедневно ею пользуются. Очень важно сделать его правильным.

Наиболее важным элементом правильного построения пространства имен электронной почты является использование одного адреса для внешней и внутренней электронной почты. Если для внутренней почты используется один адрес, а для почты, приходящей извне компании, – другой, люди неизбежно будут давать неправильный адрес электронной почты клиентам и деловым партнерам, что может привести к потере клиентуры. Не ждите, что люди будут помнить, что

у них два адреса электронной почты и кому какой нужно давать. Для всех заинтересованных лиц, в том числе для системных администраторов, устраняющих проблемы, гораздо проще, если у каждого есть один адрес для внутренней и внешней электронной почты.

Стандартизация адресов электронной почты за счет использования адресов вида имя.фамилия, например John.Smith@foo.com, является популярной, особенно у руководства. Однако обычно мы не приветствуем адреса электронной почты вида имя.фамилия. Слишком велика вероятность, что в вашей компании будет два человека с одинаковым именем или даже с одними и теми же именем и фамилией. Когда вы наймете второго Джона Смита, John.Smith становится John.A.Smith, чтобы его не путали с новым сотрудником John.Z.Smith. В этот момент визитки первого человека становятся непригодными. Визитки трудно обновить после выдачи.

В некоторых системах электронной почты вопрос противоречивых адресов вида имя.фамилия решается при помощи создания автоматического ответа, который пытается помочь отправителю разобраться, какому «Джону Смиту» он пишет, например, показывая первые десять совпадений в корпоративной директории. Несмотря на то что это кажется удобным, это не является совершенным решением. Такие ответы имеют смысл, только если письма получает человек. Если адресат был подписан на какие-либо рассылки, эти сообщения станут перенаправляться.

Эрик Олмэн, который в 1985 году разработал Sendmail, в файле cf/README программы объясняет, почему такой тип форматирования является проблемным (Shapiro and Allman 1999):

> Как правило, я категорически против использования полных имен в качестве адресов электронной почты, потому что они совершенно не являются уникальными. Например, в сообществе разработчиков UNIX-программ есть два Энди Танненбаума (Andy Tannenbaum), по крайней мере два известных Питера Дойча (Peter Deatsche), а в Bell Labs когда-то было два Стивена Р. Борна (Stephen R. Bourne) с офисами в одном коридоре. Кто из них будет вынужден страдать от унижения, будучи Stephen.R.Bourne.2? Менее известный или тот, кто позже пришел?

Вместо этого мы предпочитаем создавать пространство имен, которые уникальны в пределах корпорации, используя именные маркеры, например `chogan`, `tal`, `jsmith` и т. д. Чтобы помочь людям найти адрес электронной почты человека, с которым они хотят связаться, можно предоставить службу директорий. У пользователей должна быть возможность выбирать свой собственный маркер, хотя предварительно должно быть выбрано значение по умолчанию, основанное на алгоритме, который комбинирует инициалы с именами и фамилиями. Маркер должно быть достаточно трудно изменить после установки, чтобы препятствовать неоправданным изменениям. Маркеры не должны повторно использоваться пару месяцев, чтобы не позволить кому-либо захватить маркер недавно уволенного сотрудника для просмотра его остаточной электронной почты.

23.1.3. Надежность

Электронная почта – это жизненно необходимая служба. Люди ожидают, что электронную почту можно отправлять и получать всегда, точно так же, как ожидают гудка после поднятия телефонной трубки и включения света после нажатия выключателя. Как и в случае с другими важными службами, люди не осознают, как сильно они от нее зависят, пока она не откажет.

Сбой системы электронной почты – это очень серьезное происшествие, которое приводит к огромному количеству звонков в службу поддержки в течение короткого периода. Он обычно происходит именно тогда, когда кому-то нужно срочно отправить важные документы и рядом нет системных администраторов. Так как система электронной почты настолько важна, ее сбои будут эмоционально тяжелыми как для системных администраторов, так и для пользователей. Служба электронной почты – это не та служба, с которой системные администраторы могут экспериментировать. Новые системы и архитектуры в службе электронной почты должны устанавливаться только после тщательного тестирования.

Что более важно, с отказом системы электронной почты связаны издержки. Неполученная электронная почта может вызвать в бизнесе панику. Не выполняются контрактные обязательства, клиенты переходят к другим поставщикам, и из-за перехода людей на более старые и медленные способы связи теряется время.

Пример: бета-тест службы электронной почты

Крупная технологическая компания продвигала принцип использования централизованно размещенных серверных пулов для деловых приложений, например электронной почты. В поддержку этого принципа компания быстро перевела все 100 тыс. сотрудников с локальных серверов подразделений на единый глобальный пул серверов. Сетевые соединения с пулом серверов были настолько перегружены, что пользоваться ими было невозможно. В результате во всей компании не было связи примерно месяц, пока не была повышена пропускная способность сети. Не пытаясь учиться на ошибках, компания решила использовать пул серверов для демонстрации новой версии своего программного обеспечения электронной почты. Это обещало стать крупнейшим из когда-либо проводимых бета-тестов. Но также стало катастрофой. В конце концов компания научилась не рисковать так сильно с таким критическим приложением. Однако было слишком поздно. К этому моменту многие организации создали для своих сотрудников подпольные серверы электронной почты, ухудшив ситуацию. Ваша корпоративная система слишком важна, чтобы использовать ее как игровую площадку или опытную лабораторию.

Национальные энергетические системы и телефонные сети всех развитых стран являются системами со значительной избыточностью, спроектированными и построенными с учетом требований надежности. Проектирование системы электронной почты точно так же должно быть ориентировано на надежность, разве что в меньших масштабах.

Начните с понятного, простого проекта. Выберите оборудование и программное обеспечение по критериям надежности и возможности взаимодействия. Данные для снижения количества сбоев должны храниться в RAID-системах.

В идеале следует иметь резерв для быстрой замены машин электронной почты. Однако многие компании не могут позволить себе такие расходы. Если вы не можете позволить себе быструю замену, создайте план, который вы сможете незамедлительно выполнить, чтобы восстановить службу, если что-то откажет.

23.1.4. Простота

Система электронной почты должна быть простой. Сложность снижает надежность и усложняет поддержку системы.

Ограничьте количество машин, обеспечивающих службу электронной почты. Это ограничивает количество машин, которые должны быть надежными, и количество мест, которые системные администраторы должны проверить для поиска проблем. Прежде всего, не включайте рабочие станции в процесс доставки электронной почты. Несмотря на то что рабочие станции под UNIX можно настроить как серверы электронной почты, этого делать не надо. Обычно у них нет надежных средств резервирования, питания и других функций, необходимых серверу.

Служба электронной почты имеет пять основных аспектов: транспортировка электронной почты, доставка электронной почты, доступ, обработка списков и фильтрация. Агент пересылки электронной почты (Mail Transport Agent – MTA) передает электронную почту из точки в точку, обычно с сервера на сервер; *агенты доставки электронной почты* (Mail Delivery Agent – MDA) получают сообщения электронной почты и хранят их на сервере получателя; *серверы доступа к электронной почте* предоставляют протоколы доступа (POP3, IMAP4), которые позволяют пользовательскому почтовому агенту (Mail User Agent – MUA) на рабочей станции пользователя осуществлять доступ к отдельным сообщениям; *обработка списков* – это доставка одного сообщения группе людей в списке; *фильтрация* означает фильтрацию спама и вирусов.

Для небольших компаний простая архитектура обычно означает наличие всех этих функций на одной машине, возможно, с дополнительной системой передачи почты, подключенной к Интернету, в качестве интерфейса между компанией и остальным миром. Для более крупных компаний простота часто предполагает разделение транспортировки почты, доставки почты и обработки списков на различные системы или группы систем. Несколько выделенных систем передачи электронной почты будут доставлять электронную почту машинам либо обработки списков, либо доставки. Машины обработки списков также используют системы передачи электронной почты для доставки сообщений отдельным получателям в каждом списке.

В крупной компании службу электронной почты может обеспечивать несколько машин, но в идеале все системы должны быть одного типа. Избегайте доставки электронной почты на рабочие станции людей и убедитесь, что их клиенты электронной почты настроены для отправки электронной почты при помощи связи с системой передачи, а не самостоятельной маршрутизации почты. Отключите протокол SMTP на машинах, которые не являются официальным элементом службы электронной почты. Если требуется, например, возможность отправить электронное сообщение разработчику о том, что компиляция его программы завершена, создайте конфигурацию SMTP, привязанную к системе передачи, чтобы отправлять сообщения через службу электронной почты. Благодаря этому системные администраторы всегда будут знать, куда доставляется вся почта для конкретной учетной записи. Конфигурация, которая может привести к доставке электронной почты одной учетной записи в несколько возможных мест, приводит к путанице и «потере» сообщений[1].

[1] Почта теряется в том смысле, что предполагаемый получатель о ней не знает и не видит ее, потому что она пришла в другое место. Такая почта не возвращается отправителю, потому что она была успешно доставлена, хотя и не тому получателю.

Что касается путаницы, серверы, которые настроены для отправки всей электронной почты в централизованную службу электронной почты, также должны быть настроены отмечать отправителя как принадлежащего конкретно этому серверу, и центральная система электронной почты не должна переписывать адрес отправителя, если это не учетная запись пользователя. Если у вас есть кластер веб-приложений из 500 серверов и вы периодически получаете сообщения от dbadmin об ошибках доступа к базе данных, хорошо бы сразу узнать, на каком сервере возникла проблема. Да, есть другие способы это выяснить[1], но для электронной почты обычно чем проще, тем лучше.

Пример: плохая схема доставки электронной почты

Схема доставки электронной почты одного производителя компьютеров разрешала отправку сообщений на любую UNIX-машину, на которой у получателя была учетная запись. Эта схема также показывала полное имя узла машины, с которой человек отправлял электронную почту. Например, сообщения, отправленные с server5.example.com имели поле От: user123@server5.example.com. Когда кто-то отвечал на одно из таких сообщений, ответ направлялся на ту машину, с которой было отправлено сообщение, поэтому он доставлялся туда, а не на главный почтовый ящик пользователя. Таким образом, когда кто-то отправлял сообщение с машины, которой он обычно не пользовался, ответ отправлялся на эту машину и «терялся». Если бы адрес попал кому-нибудь в адресную книгу, а машина выводилась из эксплуатации, сообщения стали бы возвращаться. Служба поддержки часто получала жалобы о потерянных сообщениях, но, из-за того что система электронной почты была настолько неструктурированной, персоналу было трудно выяснить, что случилось.

Системным администраторам надо было реализовать систему электронной почты, которая передавала бы все сообщения на центральный сервер, переписывающий адрес отправителя, чтобы тот не содержал имя машины, с которой отправляется сообщение, – это называется маскировкой имени узла. Таким образом, все ответы автоматически пойдут через центральный почтовый сервер, который направит сообщения прямо в основной ящик пользователя.

Простота также предполагает отсутствие шлюзов и других устройств перевода электронной почты. Пользуйтесь одними стандартами по всей сети и для связи с другими системами. Шлюзы переводят электронную почту из одного формата в другой или несколько других, часто из собственного или нестандартного формата либо протокола в стандартный. Шлюзы повышают сложность и обычно являются источниками бесконечных проблем для компаний, которые ими пользуются. Кроме того, шлюзы часто удаляют данные об истории доставки, потому что они хранятся в другом формате, и из-за этого становится труднее отслеживать проблемы. В разделе 5.1.3 вы найдете пару поучительных историй, которые должны настроить вас против использования шлюзов.

---

[1] Например, заголовки Received-From (Получено-От) или поиск идентификатора сообщения в логах электронной почты.

Мы рекомендуем создать единый механизм для реализации списков рассылки и управления ими. Для этого есть много способов, и компании, которые существуют уже несколько лет, обычно используют больше одного из них. Такой недостаток стандартизации усложняет поддержку списков и существенно затрудняет реализацию автоматизированных механизмов поддержки и сокращения списков. Заставлять пользователей заучивать множество процедур для работы с электронной почтой недопустимо.

Крупные компании с несколькими серверами должны иметь возможность перемещать почтовые ящики пользователей между серверами для компенсации нагрузки. То есть, если сервер становится перегруженным, некоторые почтовые ящики перемещаются на менее загруженную машину. Когда это происходит, почтовый клиент каждого человека нужно перенастроить, чтобы указать новую машину. Один из способов избежать этого – указать записи DNS для каждого пользователя в виде username.pobox.example.com, что является именем нынешнего почтового сервера человека. Если его почтовый ящик перемещается на другую машину, данные DNS изменяются и клиент не нужно перенастраивать. Если вы используете для чтения электронной почты веб-интерфейс, применяйте то же самое имя DNS для перенаправления HTTP-запросов на нужный веб-сервер. Другой способ – использовать MDA, который поддерживает блокировку файлов, с вашими клиентами MUA. Эти серверы множественного доступа к электронной почте могут использоваться для доступа по одной и той же учетной записи без необходимости перемещать почтовые ящики.

23.1.5. Блокировка спама и вирусов

«Мусорная» электронная почта также известна как спам, или нежелательная коммерческая электронная почта (Unsolicited Commercial Email – UCE). Часто более 50% электронной почты, приходящей на почтовый сервер из Интернета, является спамом. С конца 1990-х годов электронная почта также является основным способом распространения компьютерных вирусов и других вредоносных программ с компьютера на компьютер.

Как спам, так и вредоносные программы можно блокировать и на клиенте электронной почты, и на сервере. Мы считаем, что лучше всего блокировать их на сервере. Проще обновить сервер, чем сотни почтовых клиентов. Кроме того, мы имели возможность убедиться, что пользователи легко разбираются в том, как отключать защитные программы на своих клиентах. Некоторые клиенты просто отключают их, думая, что система будет работать быстрее.

Совершенных программ против спама не существует. Как компьютер может знать, что вам не нужно конкретное сообщение электронной почты? Случаи, когда входящее сообщение с точностью до бита соответствует известному сообщению спама, бывают очень редко. А для спама, который не встречался раньше, этот прием не работает. То же самое справедливо и для антивирусных программ. Более того, несмотря на то что можно обнаружить сообщение, содержащее известный вирус, новый вирус засечь практически невозможно. Таким образом, блокировка вредоносной электронной почты стала аналогична гонке вооружений: спамеры и распространители вирусов находят способы обойти традиционные программы обнаружения, после чего разработчики программ обнаружения совершенствуют свои программы, а злоумышленники – свои приемы, и так продолжается до бесконечности.

Мы считаем, что централизация этой функции на конкретном наборе машин является важной. На самом деле сейчас существуют службы, которые выполняют анализ спама. Можно направить электронную почту на эту службу при помощи DNS-записи MX, она будет обрабатываться и затем доставляться на ваш сервер. Однако при использовании таких служб возможны проблемы неприкосновенности частной информации. С другой стороны, если сообщение секретное, оно не должно отправляться через Интернет в незашифрованном виде.

23.1.6. Универсальность

Одна из фундаментальных основ системы электронной почты – открытые каналы связи внутрь компании и из нее. Для успешного общения с максимальным количеством людей система электронной почты должна строиться на основе открытых протоколов, которые приняты и реализованы повсеместно.

Для транспортировки электронной почты это означает применение протокола на основе SMTP. Так как транспортировка электронной почты предполагает связь со многими другими системами, хорошо организованный интернет-стандарт будет поддерживаться еще долго. SMTP практически повсеместно распространен в Интернете. Скорее всего, новый протокол электронной почты будет расширением SMTP, таким как широко применяемый ESMTP или расширенный SMTP, а не полностью новым и несовместимым с SMTP протоколом. Все системы должны поддерживать SMTP в качестве транспортного протокола; для простоты и универсальности он должен быть единственным транспортным протоколом, используемым в системе.

Универсальность также касается связи внутри компании и почтовых агентов пользователя. Она справедлива для методов, которые люди могут использовать для чтения электронной почты. Количество протоколов в этой области чуть больше, а изменения со временем происходят проще, потому что обычно легко внести поддержку дополнительного протокола клиента/сервера электронной почты, не затрагивая существующие. Большинство систем используют один-два наиболее популярных протокола клиентов электронной почты, поддерживая таким образом практически все программы чтения электронной почты. Система легко может поддерживать большое количество почтовых клиентов на различных ОС, если системы доставки и передачи электронной почты используют стандартные протоколы Интернета. Поддержка максимального количества клиентов за счет использования небольшого количества стандартных протоколов означает, что люди, которые предпочитают один клиент другому, смогут им пользоваться. Обычно клиенты электронной почты также поддерживают различные протоколы и легко найти протокол, который будет общим для клиента и сервера доставки почты. С другой стороны, система, в которой используется собственный протокол, ограничивает пользователей одним или двумя клиентами разработчика, где могут отсутствовать функции, необходимые или желательные для пользователей.

Нестандартные протоколы дорого стоят

Небольшая успешная начинающая интернет-компания из Силиконовой долины была куплена крупной, хорошо организованной компанией из Вашингтона. Начинающая интернет-компания пользовалась для своей

службы электронной почты стандартными протоколами. Клиентами, главным образом, были UNIX-машины, но имелось также значительное количество машин Macintosh и немного компьютеров с ОС Windows. Система электронной почты работала хорошо и была доступна каждому в компании. Когда компания была куплена и интегрирована в головную компанию, сотрудникам начинающей компании пришлось перейти на службу электронной почты головной компании, основанной на собственных стандартах Майкрософт, а не Интернета[1]. Клиентов для машин под UNIX и Macintosh не существовало. Компании пришлось купить компьютеры под Windows для каждого пользователя UNIX или Macintosh – практически для всех, – чтобы они смогли продолжать отправлять и получать электронную почту. Это было невероятно дорогим решением!

В разделе 5.1.3 можно найти больше философских рассуждений и историй на эту тему.

23.1.7. Автоматизация

Как и во всех других аспектах системного администрирования, автоматизация может упростить часто выполняемые задачи и обеспечить их надежное и точное выполнение. Многие области администрирования электронной почты должны быть автоматизированы уже при создании службы или в рамках существующих служб электронной почты.

В частности, создание учетной записи электронной почты должно быть автоматизировано как часть процесса создания учетной записи сотрудника. Автоматизация должна включать внесение человека во все актуальные списки рассылки компании и подразделения. Аналогично, удаление учетной записи электронной почты должно быть автоматизированным элементом процесса удаления учетной записи сотрудника.

Ранее мы рассматривали необходимость периодического перемещения учетных записей электронной почты между машинами для перераспределения нагрузки. Автоматизация этого процесса важна и часто является сложной задачей.

Мы выяснили, что лучше не включать автоматическое перенаправление электронной почты для людей, ушедших из компании, потому что важная информация может быть непреднамеренно отправлена кем-то, кто не знает, что человек уволился. Предпочтительна автоматическая отправка сообщения о перенаправлении с новым адресом электронной почты и о том, что человек ушел из компании.

Другой удобной формой автоматизации службы электронной почты является автоматизация администрирования списка рассылок, чтобы списки могли создаваться, удаляться и управляться напрямую пользователями, которыми они необходимы, а не системными администраторами. Это предоставляет владельцам списков лучшее, более тонкое обслуживание, а также освобождает системных администраторов от постоянной рутинной работы.

---

[1] Даже несмотря на то, что Microsoft Exchange теперь поддерживает открытые протоколы, например POP3 и IMAP4, теряется много функций, связанных с календарем и адресными книгами. В Lotus Notes есть похожие проблемы.

Уволенный сотрудник должен быть удален из всех внутренних списков рассылки. Также нужно периодически проводить автоматические проверки активных учетных записей электронной почты на соответствие базе данных персонала и проверки, позволяющие убедиться, что электронная почта для локальных учетных записей не перенаправляется за пределы компании и что отключенные учетные записи не входят в какие-либо списки рассылки. Кроме того, можно автоматизировать проверку важных внутренних списков рассылки на наличие неавторизованных адресатов.

23.1.8. Базовый мониторинг

В главе 5 было сделано замечание о том, что служба не реализована правильно, пока не осуществляется ее мониторинг. Электронная почта не является исключением из этого правила. В службе электронной почты должен осуществляться мониторинг базового уровня: каждая машина, используемая для службы, должна быть включена и подключена к сети (отвечать на `ping`), а также отвечать на запросы на соответствующие TCP-порты (SMTP на порте 25, POP3 на порте 110, IMAP4 на порте 143 и т. д.).

Для всех серверов электронной почты также должен осуществляться мониторинг дискового пространства, использования диска и загрузки процессора. Мониторинг дискового пространства помогает в планировании ресурсов при повышении требований и предупреждает системных администраторов, когда на диске остается мало свободного места. Служба электронной почты требует немало ресурсов диска и центрального процессора. Мониторинг этих элементов позволяет обнаруживать изменения уровня обслуживания, связанные с увеличением объемов электронных сообщений, петлями электронной почты и другими проблемами. В этих ситуациях наличие базового уровня нормы – прошлого состояния – помогает обнаруживать текущие проблемы.

Электронная почта для postmaster также должна отслеживаться. Адрес postmaster в каждой системе получает сообщения электронной почты об ошибках доставки сообщений или возвращении их отправителю. Благодаря мониторингу электронной почты, отправленной на этот адрес, ответственный за службу электронной почты будет знать, когда происходят сбои, и получит возможность разобраться с ними. Возвращенные сообщения, отправленные на postmaster, содержат все заголовки неправильного сообщения, а также сообщение об ошибке, информирующее о причине невозможности доставки. Эта информация очень важна для отладки электронной почты, и ее часто не хватает, когда о проблемах сообщают сами пользователи. Наконец, нужно просматривать логи на машинах электронной почты, чтобы отслеживать интенсивность потока сообщений (что может помочь с прогнозами на основе исторических данных), замечать, когда доставка электронной почте по какой-то причине остановилась, и устранять проблемы, которые могут возникнуть, когда интенсивность потока сообщений неожиданно возрастает.

Это основы мониторинга системы электронной почты. Более развитые приемы мониторинга рассмотрены в разделе 23.2.3. См. также главу 22.

23.1.9. Резервирование

Так как электронная почта является одной из важнейших служб для работы всех современных компаний, они должны ввести в систему электронной почты

избыточность, как только это будет реально возможно. В разделе 5.1.9 рассмотрены некоторые общие способы обеспечения надежности служб. В данной главе основное внимание уделяется вопросам, специфическим для электронной почты.

Когда для систем электронной почты нет резервного оборудования, должен существовать план восстановления, который в случае сбоя может быть быстро выполнен. Для узлов передачи электронной почты легко ввести резервирование и перечислить обрабатывающие узлы при помощи записей DNS MX (Mail eXchanger – узел обмена почтой) и нескольких серверов с одинаковой конфигурацией.

Резервирование узлов доставки почты отличается тем, что целые узлы не могут быть легко взаимозаменяемы. Вместо этого вы можете сделать сервер внутренне избыточным при помощи RAID и других методов. Вы можете продублировать узел, который осуществляет доступ к общему хранилищу, при помощи хранилища, подключаемого по сети, или технологии сети устройств хранения данных (Katcher 1999). Однако в этом случае вы должны быть особенно внимательны – нужно обеспечить соответствующую блокировку и контроль доступа.

Доступ клиентов должен быть избыточным с прозрачным восстановлением после отказа. Для этого вы должны понимать, как работает клиент. Клиенты обычно сохраняют результат изначального DNS-запроса, который посылается, когда они пытаются связаться с сервером доставки электронной почты для ее загрузки, поэтому простые приемы с DNS будут недостаточными. Избыточность для клиента должна обеспечиваться на IP-уровне. Есть несколько технологий, позволяющих узлу брать на себя ответы на запросы на определенный IP-адрес, когда сама машина по этому адресу не отвечает. Два распространенных способа – это применение балансировки нагрузки (уровень 4) (Black 1999) и протокол виртуального резервирования маршрутизаторов VRRP (Virtual Router Redundancy Protocol) (Knight et al. 1998).

При определении стратегии резервирования рассмотрите все компоненты системы и их функционирование. Продумывая возможные решения, принимайте во внимание то, как работают различные механизмы, как они влияют на вашу остальную систему и как другие машины будут с ними взаимодействовать.

23.1.10. Расширение

Все аспекты системы электронной почты должны расширяться по мере роста потребностей. Системы транспортировки и доставки почты должны быть готовы к работе с большими объемами трафика, серверы доступа к электронной почты должны работать с большим количеством пользователей, получающих свою почту, а системы обработки списков должны разбираться с пиками интенсивности трафика и численностью пользователей. Все должно расширяться по мере появления новых технологий, которые значительно влияют на увеличение размера сообщений.

Системы транспортировки электронной почты должны расширяться, чтобы соответствовать повышению интенсивности трафика. Интенсивность трафика характеризуют три независимые переменные: размер сообщений, количество сообщений на человека и число людей, пользующихся системой электронной почты. Чем больше людей пользуются службой электронной почты, тем больше сообщений ей потребуется обрабатывать. Количество сообщений на человека обычно постепенно растет со временем и имеет пики близко к праздникам.

Размер отдельных сообщений обычно скачкообразно увеличивается по мере появления новых технологий.

Кроме того, служба электронной почты должна расширяться, чтобы справляться с большими скачками трафика, которые могут быть вызваны презентационными мероприятиями или значительными неожиданными проблемами. Внезапное повышение объема трафика, проходящего через системы транспортировки электронной почты, не является чем-то из ряда вон выходящим. Система транспортировки электронной почты должна быть спроектирована таким образом, чтобы справляться с неожиданно высокими пиками трафика. Кроме того, системы транспортировки электронной почты должны быть способны хранить большие объемы электронной почты, которые могут накопиться в случае возникновения проблем с передачей сообщений адресатам.

Системы доставки электронной почты должны предсказуемо расширяться с ростом числа людей, обслуживаемых системой доставки. Сервер доставки почты вынужден будет расширяться со временем, даже если количество обслуживаемых им людей не будет расти, за счет повышения количества и размера передаваемых сообщений. Если пользователи хранят свою почту на сервере доставки в течение долгого времени после прочтения, сервер доставки также придется расширять для удовлетворения этой потребности. В системах доставки электронной почты всегда должно быть достаточно дополнительной емкости для хранения почты, обычным практическим правилом определения пиковой нагрузки является увеличение нормальной нагрузки вдвое. Возможны внезапные, неожиданные поступления больших сообщений.

Неправильный способ расширения

В подразделении университета был собственный сервер доставки электронной почты. При перегрузке он иногда отклонял запросы клиентов на соединение по протоколу POP3 (Mayers and Rose 1996). Для решения этой проблемы системный администратор рассылал по подразделению сообщение, публично обвиняя пользователей, применявших почтовые клиенты, которые проверяли новую электронную почту автоматически через предварительно определенное время, например каждые 10 мин. Впрочем, это была конфигурация почтовых клиентов по умолчанию, а не осознанный эгоистичный выбор, как утверждалось в его сообщении. Однако несколько пользователей потратили время на то, чтобы выяснить, как отключить эту функцию в своих почтовых клиентах, и проблема была решена, по крайней мере временно. Но проблема продолжала снова возникать по мере прихода новых сотрудников и увеличения объема трафика. Как мы видели в главе 16, лучше исправить неполадку раз и навсегда, чем частично и много раз. Это предоставляет пользователям лучшее обслуживание и в конечном итоге снижает объем работы системных администраторов.

Вместо того чтобы беспокоить и обвинять своих пользователей, системный администратор должен был осуществлять мониторинг почтового сервера, чтобы выяснить, какой недостаток ресурсов вызывал отклонение соединений. Затем он мог устранить проблему в корне и расширить сервер, чтобы справиться с возросшими потребностями. В качестве альтернативы некоторые серверные продукты оптимизируют проверку клиентами

новой почты за счет быстрого ответа о том, что новых сообщений нет, если клиент выполнял запрос в течение последних 10 мин. Это требует меньших ресурсов, чем проверка того, пришла ли этому пользователю новая почта.

С развитием новых технологий размеры сообщений обычно значительно растут. Раньше электронная почта была простым текстом и передавалась через медленные модемные соединения. Когда люди начали пересылать обычные изображения и большие программы, более крупные файлы преобразовывались в текст и разделялись на небольшие части, которые отправлялись в отдельных сообщениях, чтобы они могли передаваться по модемам. Первые изображения были черно-белыми и имели низкое разрешение. Появление мониторов с более высоким разрешением, а особенно цветных, привело к значительному росту размера изображений, отправляемых по электронной почте. Когда электронная почта распространилась на ПК и Macintosh, люди стали отправлять документы и презентации, которые представляли собой большие файлы, а могли быть очень большими. Большее количество форматов и документов, в том числе изображений с более высоким разрешением, привело к значительному увеличению размера сообщений. Появление стандартных форматов аудио- и видеофайлов, которые стало возможным пересылать вместе с сообщением, также привело к повышению объемов данных, отправляемых по электронной почте.

Всегда имейте достаточно пространства для хранения электронной почты. Отслеживайте развивающиеся технологии и будьте готовы к быстрому расширению при их появлении. Большинство почтовых систем позволяют системным администраторам установить ограничения на размер сообщений, что при правильном использовании может способствовать решению проблем с размером сообщений. Однако, если ограничения будут мешать людям работать, они найдут способ обойти их, например, разделяя сообщения на несколько меньших по размеру частей или пожаловавшись генеральному директору. Мы рекомендуем использовать ограничение размеров только в виде временной меры для решения проблемы перегрузки, пока вы ищете постоянное решение, или с действительно большим пределом, чтобы люди не могли случайно отправить что-то огромное.

Организациям, переходящим с POP3 на IMAP4, нужно учитывать особые вопросы расширения, потому что IMAP4 требует больше ресурсов сервера, чем POP3. POP3 обычно используется для перемещения электронной почты с сервера на чей-то клиент на рабочей станции или ноутбуке. Требования по дисковому пространству минимальны, потому что сервер главным образом используется в качестве буферной области до следующего подключения клиента. Как только передача будет завершена, сервер может удалить свою копию почтового ящика. Подключения клиентов имеют краткосрочный характер. Клиенты подключаются, загружают почтовый ящик и отключаются. Они не возвращаются, пока не наступит время проверить новую почту, а до этого может пройти несколько часов или дней. Однако IMAP4 поддерживает почтовый ящик и все папки на сервере и просто обеспечивает клиенту доступ к ним. Таким образом, требования по дисковому пространству гораздо более серьезны и серверы сталкиваются с долгим временем подключения. Наличие электронной почты на сервере имеет преимущество за счет более управляемых из центра и предсказуемых резервных копий. Из-за различных схем использования сети серверы

должны быть настроены для большого количества одновременных долгих сетевых подключений. Это может потребовать дополнительных усилий, так как многие операционные системы не настраиваются по умолчанию для правильного поддержания тысяч открытых соединений TCP/IP.

Для систем обработки списков характерны те же самые проблемы объема, что и для систем передачи и доставки, но, кроме того, они вынуждены иметь дело с увеличенным списком очень разнотипных адресатов. Когда машине обработки списков надо доставить сообщения большому количеству других машин, некоторые из них, скорее всего, по какой-то причине будут недоступны. Система обработки списков должна разобраться в этой ситуации, не задерживая доставку сообщений другим системам, которые доступны. Некоторые элементы расширения системы обработки списков связаны с конфигурацией программ (Chalup et al. 1998). Использование дискового пространства, пропускной способности сети, ресурсов процессора и памяти также должно отслеживаться и соответствующим образом расширяться.

23.1.11. Вопросы безопасности

Узлы передачи почты, которые связываются с точками за пределами компании, традиционно являются целями для злоумышленников, потому что такая связь по своей природе предполагает подверженность воздействию из Интернета или других внешних сетей. Эти привлекательные для атак цели имеют доступ как к внешнему миру, так и к внутренней корпоративной сети и часто имеют особый доступ к внутренним службам имен и аутентификации. Доставка почты – это сложный процесс, и поэтому она подвержена ошибкам, которые исторически использовались как уязвимости безопасности. Учитывайте вопросы безопасности начиная с первоначального проектирования, потом безопасность будет обеспечить труднее.

Почтовая система также является путем, по которому в компанию может попасть нежелательный контент, например вирусы. Некоторые разработчики предоставляют продукты, которые проверяют содержимое электронной почты на вирусы или другой нежелательный либо деструктивный контент, прежде чем она будет принята и доставлена получателю. Решите, нужно ли в вашей компании такое сканирование и не противоречит ли оно политике неприкосновенности частной информации. Если сканирование содержимого реализовано, попытайтесь обеспечить, чтобы приложение понимало максимальное количество форматов данных, чтобы оно могло проверить, например, все файлы вложения в архиве формата zip. Имейте в виду, что некоторые объекты все равно могут просочиться через сеть, и аналогичное сканирование также должно выполняться на настольных машинах ваших пользователей. При обработке тысяч или миллионов сообщений электронной почты в день такое сканирование на вирусы может быть серьезным узким местом. Если вы пользуетесь такими системами, приобретайте высокоскоростные диски.

Кроме того, рассмотрите, как почтовая система согласуется с архитектурой безопасности. Например, если в компании применяется модель безопасности периметра, какую защиту система брандмауэра предоставляет электронной почте? Есть ли в системе средства для предотвращения передачи сообщений с подозрительными заголовками, которые могут пытаться использовать уязвимости безопасности. Если нет, то где лучше всего можно реализовать эту функцию? Могут ли системы передачи внешней электронной почты использоваться

неавторизованными лицами для передачи электронной почты, не предназначенной для компании? Как можно предотвратить неавторизованную передачу электронной почты? Как пользователи получают доступ к своей электронной почте в пути или дома? Многие из простейших и наиболее распространенных способов предоставления людям доступа к их электронной почте в пути включают передачу паролей и потенциально конфиденциальной электронной почты по публичным, небезопасным сетям. Структура системы должна включать безопасный механизм удаленного доступа к электронной почте, например, такой, который описан в главе 27.

23.1.12. Распространение информации

Важным элементом создания любой службы является распространение информации о ней, особенно сообщение людям о ее функциях и о том, как ею пользоваться. Другой важный компонент распространения информации о службе – это документирование системы для системных администраторов.

Для пользователей службы электронной почты важно обеспечить, чтобы каждый из них понимал политики, связанные с системой: касающиеся неприкосновенности частной информации, перенаправления электронной почты за пределы компании, создания резервных копий и графика работы с электронной почтой, любой фильтрации содержимого и ее результатов и того, как компания определяет допустимое использование и применяет это определение к электронной почте (см. раздел 11.1.2). Пользователи должны быть предупреждены о рисках, связанных с электронной почтой: о потенциальном перенаправлении любых сообщений нежелательным адресатам, о вирусах и о том, что, если их просят запустить какую-либо программу, она, скорее всего, является вирусом. Пользователи должны знать о «письмах счастья», чтобы они могли определить такие письма и не распространять их.

Кроме того, пользователи должны быть в курсе доступных им полезных функций, например механизмов шифрования и средств администрирования списков рассылки.

К сожалению, выдача человеку кучи политик не особенно эффективна. Может быть проще инструктировать новых сотрудников устно или при помощи краткой презентации и сделать полные тексты политик доступными в сети. В некоторых фирмах создаются веб-формы, требующие у пользователей подтверждения согласия с каждой политикой.

Документирование системы электронной почты для других системных администраторов является важным. Процедуры восстановления после отказа и аварийного восстановления должны быть понятными и хорошо документированными, как и структура системы; документация должна включать схемы, на которых отображены потоки электронной почты и особенности ее обработки на всех системах. Системные администраторы, которые не работают непосредственно с системой электронной почты, должны иметь возможность выполнить какую-нибудь предварительную отладку, прежде чем сообщать о проблеме, и этот процесс также должен быть хорошо документирован. Особенно важно, чтобы системные администраторы, которые могут находиться в различных часовых поясах в удаленных подразделениях, понимали архитектуру почтовой системы и могли выполнять основные задачи по отладке самостоятельно.

23.2. Тонкости

Компания может кое-что сделать, чтобы усовершенствовать свою службу электронной почты после обеспечения всех основ. В интересах защиты частной информации людей и конфиденциальной информации компании можно обратить внимание на то, чтобы сделать шифрование электронной почты простым в применении, особенно для высшего руководства. Кроме того, юридические отделы многих компаний могут захотеть, чтобы системные администраторы реализовывали особую политику резервного копирования для электронной почты, в соответствии с которой резервные копии электронной почты удаляются быстрее других. Компания, служба электронной почты которой сильно заметна пользователям, захочет реализовать более развитый мониторинг. Некоторым компаниям, например интернет-провайдерам или сайтам электронной коммерции, может понадобиться расширение системы обработки списков для работы со списками большого объема, с большим количеством адресатов. Мы рассмотрим все это более подробно.

23.2.1. Шифрование

Одно из улучшений базовой системы электронной почты – это введение простого в применении механизма шифрования. Шифрование особенно полезно для высших руководителей, которые постоянно работают с особо конфиденциальной информацией. Этот процесс должен быть быстрым и простым, чтобы шифрование сообщение перед отправкой не занимало много времени. Шифрование должно быть полностью интегрировано в почтовый клиент, чтобы руководители могли просто щелкнуть по кнопке Зашифровать при отправке, настроить автоматическое шифрование для определенных получателей или включить шифрование по умолчанию для всех сообщений. А самое важное – санкционированный получатель должен иметь возможность так же просто расшифровать сообщение. Трудности при установке или настройке почтовых клиентов для расшифровки сообщений могут сорвать даже самые лучшие стратегические планы по шифрованию.

Доступные коммерческие пакеты шифрования интегрируются с почтовыми клиентами до различных уровней прозрачности. При рассмотрении различных продуктов учитывайте вопросы как пользовательского интерфейса, так и управления ключами. Системе шифрования требуется хранилище для ключей шифрования всех сотрудников и способ аннулирования этих ключей, если они будут скомпрометированы. Учитывайте также вопросы, связанные с действиями в экстренных ситуациях, когда с ответственным сотрудником что-то случается, а важные сообщения зашифрованы таким образом, что только этот человек может их прочесть. В некоторых системах есть механизмы восстановления паролей, но они обязательно должны иметь адекватные средства контроля, чтобы обеспечить невозможность компрометации ключей.

Системы шифрования и управления ключами являются сложными темами и должны быть подробно изучены перед реализацией. Хорошо реализованная система шифрования является активом любой компании. Однако многие разработчики криптографических средств продают проблемы, а не решения, и их нужно избегать. Советы по их обнаружению можно найти в книге Мэтта Кер-

тина «*Snake Oil Warning Signs: Encryption Software to Avoid*» (Curtin 1999a, b). Для более подробной информации по стандартам шифрования электронной почты см. книги Garfinkel 1994 и Oppliger 2000.

Учитывайте влияние закона Сарбейнса–Оксли на применение шифрования. Если вы разрешаете шифрование электронной почты, у компании должна быть возможность получить личный ключ, чтобы обеспечить доступность содержимого сообщения, если этого потребуют соответствующие органы.

23.2.2. Политика хранения электронной почты

Несмотря на то что резервные копии являются неотъемлемым элементом хорошего системного администрирования, они также могут неожиданно навредить компании. Во многих компаниях есть политика отсутствия резервного копирования электронной почты или удаления таких резервных копий через короткий период времени.

Проблема заключается в том, что, если компания будет вовлечена в любой судебный процесс, например по защите своего патента или прав на интеллектуальную собственность, все документы, связанные с делом, скорее всего, нужно будет представить в суд, а это означает поиск актуальных документов по всем магнитным лентам с резервными копиями. Обычно формальные документы, связанные с конкретной темой, хранятся в известных местах. Однако неформальные документы, такие как электронная почта, могут быть в любом почтовом ящике и поэтому на наличие потенциально актуальных документов нужно будет просмотреть всю электронную почту. Вне зависимости от того, находятся ли резервные копии на лентах или на диске, сообщения, которые соответствуют критерию поиска, затем нужно будет проверить по отдельности, причем это должен сделать человек, который сможет определить, является ли документ актуальным и необходимым для представления в суде. Это очень дорогостоящий и долгий процесс, которого юридический отдел, скорее всего, постарается избежать вне зависимости от того, помогут ли найденные документы компании. Процесс поиска в электронной почте за последние несколько лет, хранящейся на магнитных лентах, просто слишком дорогостоящий.

В средних и крупных компаниях обычно есть политика хранения документов, которая указывает, какое время должны храниться определенные типы документов. Эта политика существует для того, чтобы ограничить необходимое для хранения документов пространство и упростить поиск нужных документов. Политика хранения документов в определенный момент обычно расширяется, чтобы охватывать электронную почту, часто в связи с достижением соответствия закону Сарбейнса–Оксли. С этого момента юридический отдел будет требовать, чтобы системные администраторы реализовывали политику. Если электронная почта распространяется по большому количеству машин и некоторым нестандартным местам, реализация политики становится трудной. В частности, если электронная почта хранится на компьютерах и ноутбуках людей, которые пользуются POP3-серверами, политика должна охватывать резервные копии на компьютерах и ноутбуках и каким-то образом отделять резервные копии электронной почты от резервных копий системы, чтобы первые можно было удалять быстрее. При проектировании вашей службы электронной почты луч-

ше с самого начала принять во внимание, что у вас могут потребовать соблюдать эту политику, и решить, как вы будете это делать.

23.2.3. Расширенный мониторинг

Для компаний, в которых от электронной почты сильно зависят доходы, желательно реализовать некоторые более развитые методы мониторинга системы электронной почты. Так как передача и доставка электронной почты включают сложную последовательность действий, системные администраторы могут легко упустить какой-нибудь небольшой нюанс системы, если попытаются осуществлять только базовый мониторинг каждого компонента. Несмотря на то что базовый мониторинг очень полезен и необходим, в компаниях, где электронная почта действительно критична для бизнеса, должна быть реализована более сложная сквозная модель.

Сквозной мониторинг означает создание теста, который воспроизводит отправку сообщения кому-то, кто обслуживается данной системой электронной почты. Тест должен воспроизводить пользователя или транзакцию, приносящую доход, максимально реалистично, чтобы обнаружить все возможные проблемы, в том числе те, которые видны только за пределами сети. Мониторинг подробно обсуждается в главе 22. В частности, в разделе 22.2.4 рассмотрен сквозной мониторинг вообще и приведен пример непосредственно об электронной почте.

23.2.4. Обработка больших списков

В большинстве компаний есть списки рассылки, а у многих есть списки рассылки для обслуживания пользователей, которые платят деньги. Например, в компании может быть список рассылки, который объявляет ее пользователям об обновлении имеющихся или появлении новых продуктов. Может быть список рассылки, который держит пользователей в курсе событий в компании или сообщает о серьезных ошибках в ее продуктах. В других компаниях есть списки рассылки для людей, которые задействованы в бета-тестировании продукта. В некоммерческой организации может быть один или несколько списков рассылки, чтобы держать ее членов в курсе того, что происходит и какие мероприятия организуются. В университете могут быть списки рассылки для студентов в каждой группе. У провайдера почти обязательно будут списки рассылки для его пользователей, чтобы сообщать им об отключениях, которые могут их затронуть.

Списки рассылки управляются централизованно на почтовых серверах, а не в виде псевдонимов в почтовом клиенте одного человека. Каждый может отправить сообщение на тот же адрес, чтобы добраться до того же списка людей. Списки рассылки можно защитить, чтобы только несколько авторизованных лиц могли рассылать по ним сообщения, или чтобы сообщения перед отправкой подтверждались авторизованным лицом, или чтобы сообщения по списку могли рассылать только адресаты этого списка. Списки также могут быть открытыми, чтобы каждый мог разослать сообщения адресатам списка. Большинство программ по управлению списками предоставляет системным администраторам возможность передать управление членством в списке, ограничениями по отправке и подтверждением сообщений человеку, который управляет списком

с точки зрения бизнеса. В программе управления списками также должна быть возможность разрешить пользователям создавать и удалять свои собственные списки рассылки без привлечения системного администратора. Например, если компания начинает программу бета-тестирования для конкретного продукта, у ответственного за бета-тест руководителя должна быть возможность создать список рассылки для пользователей бета-версии, добавлять их в список и удалять из него, контролировать тех, кто рассылает по списку сообщения, и удалить список, когда бета-тест закончится. Однако, когда разрешено неконтролируемое создание списков рассылки, должны существовать политика и механизм мониторинга, устанавливающие правила для списков, связанных и не связанных с работой. Политика списков должна четко указывать, какие списки являются допустимыми и кто может заниматься такой деятельностью. Список по совместному использованию автомобилей для сотрудников из определенного региона? Вполне возможно. Список по совместному использованию автомобилей для сотрудников, которые ездят на бейсбол? Менее понятно. Как насчет списка фанатов конкретной команды? Что будет, если кто-то уйдет из компании? Может ли он остаться в списке по бейсболу с новым адресом электронной почты? И так далее.

Относительно небольшое количество компаний имеет объемные списки с большим количеством адресатов, которым требуется особое расширение. Часто такие компании предоставляют сторонние услуги другим. Требования к службе обработки списков среднестатистической компании могут быть выполнены при помощи простых, бесплатных программ. Однако списки больших объемов часто выходят за рамки возможностей этих систем. В таких ситуациях мы рекомендуем вкладывать средства в коммерческие программы или службы, способные справляться с такими большими объемами, либо пользоваться программным обеспечением с открытым исходным кодом и нанять консультанта, который ранее занимался проектированием таких систем. Службы списков большого объема также должны строиться на основе нескольких резервных систем, чтобы избежать цепных сбоев, вызванных перегрузкой сервера обработки списков сразу же после его восстановления. На сервере обработки списков большого объема важно отслеживать общее время, прошедшее от начала отправки сообщения первому адресату списка до окончания отправки последнему адресату, за исключением участков, на которых возникли проблемы со связью. Важно, чтобы адресаты списка рассылки не страдали от долгой временной задержки. Если люди в конце списка получают сообщения на день позже людей в его начале, им трудно разговаривать осмысленно, потому что они будут сильно отставать по информированности от других людей из списка. С другой стороны, известно, что некоторые крупные списки замедляют трафик, чтобы предотвратить «перебранки». Главное – обеспечить соответствие скорости реагирования серверов обработки списков и назначения этих списков.

Было опубликовано много полезных документов конференции USENIX LISA и IETF о серверах обработки списков (Chapman 1992, Houle 1996) и управлении списками (Bernstein 1992, Chalup et al. 1998). Технологии серверов обработки списков рассылок по электронной почты с годами значительно изменились по мере повышения требований к ним. Как и во многих других областях системного администрирования, важно быть в курсе развития технологий в данной области.

23.3. Заключение

Очень важно обеспечить правильную работу электронной почты. Люди зависят от нее даже больше, чем сами это осознают. Во многом она аналогична коммунальным услугам, таким как электропитание и водопровод. Вопросы расширения системы для удовлетворения растущих потребностей, мониторинга службы и обеспечения резервирования не должны откладываться на потом. Безопасность также должна учитываться с самого начала, потому что серверы электронной почты являются привлекательными целями для злоумышленников, а электронная почта – популярным способом распространения вирусов.

Перед созданием системы электронной почты вы должны продумать несколько политик. Компании должны внимательно определить политику пространства имен для электронной почты и обеспечить, чтобы для внутренней и внешней связи использовалось одно и то же пространство имен. Кроме того, следует определить политику неприкосновенности частной информации и довести ее до людей, которые пользуются службой.

В некоторых компаниях могут захотеть ввести в службу электронной почты шифрование для обеспечения дополнительной защиты важной информации. В более крупных компаниях могут захотеть ввести правила для снижения времени хранения резервных копий электронной почты и обезопасить себя от издержек на поиск в старой почте сообщений, актуальных для судебного разбирательства. Компании, в которых служба электронной почты связана с получением дохода, должны обеспечить ее сквозной мониторинг. Компании, имеющие серверы обработки списков большого объема, могут предъявлять особые требования, которые должны быть учтены, и для подобных целей лучше приобретать коммерческие программы.

Задания

1. Какова политика неприкосновенности частной информации в электронной почте вашей компании? Сколько людей о ней знают?
2. Сколько пространств имен электронной почты есть в вашей компании? Кто ими управляет?
3. Перечислите свои машины передачи электронной почты. Есть ли у них другие задачи?
4. Перечислите свои машины доставки электронной почты. Есть ли у них другие задачи?
5. Где в вашей компании выполняется обработка списков рассылки?
6. Когда, по вашему мнению, потребуется расширить имеющуюся у вас систему электронной почты? Какой аспект вы предполагаете расширять и почему? Когда, по вашим прогнозам, имеющихся ресурсов станет недостаточно?
7. Как вы в настоящее время осуществляете мониторинг своей системы электронной почты? Вы хотите что-нибудь изменить или добавить?
8. Насколько надежна система электронной почты в вашей компании? Как вы это определили?

9. Если в вашей компании есть несколько машин доставки, объясните, зачем нужна каждая из них. Можете ли вы уменьшить их количество?
10. Если в вашей компании есть удаленные офисы, есть ли у сотрудников в этих офисах доступ к своей электронной почте, когда соединение с основной системой отсутствует?
11. Как в вашей компании обеспечивается безопасность электронной почты?
12. Как электронная почта проходит из Интернета в вашу организацию? Как она проходит в Интернет? Какие риски в плане безопасности и подверженность внешним воздействиям связаны с этим и как ваша структура их смягчает? Какие усовершенствования можно ввести?
13. Как бы вы реализовали график хранения резервных копий электронной почты в течение 6 месяцев? Потребовалось бы вам вносить в эту политику рабочие станции? Как бы вы реализовали этот элемент?

Глава 24

Служба печати

Печать – это получение бумажной[1] копии документа, когда он вам нужен. Печать – важнейшая для бизнеса функция. Насколько мы знаем, пользователи считают ее одной из наиболее важных служб, важнее нее только электронная почта.

Странно, но многие системные администраторы относятся пренебрежительно к печати и даже ко всем тем, кто много печатает. «А чем вас не устраивает электронная версия документов?» – спрашивают противники принтеров. Многие системные администраторы гордятся тем, как мало они печатают, отказываясь работать с бумагой, когда есть электронная версия. Таким образом, многие системные администраторы, которые не понимают, насколько печать важна для их пользователей, не предоставляют для нее хорошей поддержки. Приоритеты системных администраторов должны соответствовать приоритетам пользователей[2].

Печать важна пользователям потому, что, нравится вам это или нет, но бизнес до сих пор ведется на бумаге. Контракты нужно подписывать. Схемы нужно размещать на стенах. Бумага может попасть туда, куда не могут попасть компьютеры. Когда вы за рулем, проще сверяться с маршрутом по бумажной карте, чем по электронной в ноутбуке. Люди находят разные ошибки при редактировании бумажного и электронного документа – вероятно, это зависит от среды восприятия. Даже технократы пользуются бумагой: это может удивить вас, дорогой читатель, но каждую главау этой книги корректор вычитывал на белой, плотной... бумаге для лазерных принтеров.

Если контракт необходимо подготовить к вечеру, то недопустимо потерять машину с нужным грузом из-за заклинившего принтера. Печать является бытовой потребностью, она всегда должна работать. Однако технологии печати много раз кардинально изменялись за время нашей трудовой деятельности. Поэтому мы предпочли не обсуждать достоинства и недостатки различных технологий печати – они могут стать неактуальными уже к тому моменту, как высохнет краска на этой бумаге. Вместо этого мы рассмотрим общие аспекты печати: как убедиться, что краска попадает на бумагу, как составить политики печати и спроектировать серверы печати. И наконец мы рассмотрим способы создания

---

[1] Вы можете печатать и на многих других материалах помимо бумаги, но для простоты в данной главе мы будем говорить о бумаге. Прозрачная пленка – это просто бумага, которая делается не из дерева.

[2] Однако мы все-таки не одобряем и тех, кто распечатывает каждую интересную веб-страницу, которую видит.

среды службы печати, дружественной к пользователям. Все это важно вне зависимости от развития технологий, применяемых непосредственно для печати чего бы то ни было.

24.1. Основы

Успешная система печати начинается с понимания требований к хорошей политике, подкрепленной целостным проектированием. Без необходимой политики проектирование не будет иметь верного направления. Без проектирования функции печати будут нестабильными и более сложными в использовании.

24.1.1. Уровень централизации

Какой должна быть совершенная система печати? Некоторые хотят, чтобы их собственные принтеры были подключены к их собственным компьютерам. В их совершенном мире у каждой машины был бы собственный высокоскоростной принтер с высоким качеством печати. Это очень дорого, но очень удобно для пользователей. Для других основной вопрос заключается в том, что вне зависимости от того, сколько есть принтеров, должна быть возможность печати с любого узла на любом принтере. У такого подхода есть преимущество возможности при необходимости «одолжить» чей-то принтер с высоким качеством печати (возможно, цветной), и такая конфигурация является более гибкой. Финансисты видят высокую стоимость принтеров и их обслуживания, поэтому предпочли бы централизовать печать – возможно, рекомендовать, чтобы в каждом здании был один высокоскоростной принтер, один принтер с высоким качеством печати и один цветной принтер[1]. Для других неважно, сколько имеется принтеров или у кого к ним есть доступ, так как каждая копейка расходов возмещается через систему возврата платежей. Кто-то старается придерживаться золотой середины.

Основное требование системы печати – возможность для людей печатать на всех принтерах, которыми им разрешено пользоваться, – в их число могут входить все принтеры или только их четко определенная группа. Расходы представляют собой либо постраничную, то есть сдельную оплату, либо индивидуальное финансирование каждой группы – центра, подразделения, отдела. Если вам хочется усложнить себе жизнь, попробуйте использовать совершенно разные способы оплаты расходов на оборудование, расходные материалы и обслуживание.

Типичное распределение для офиса – один принтер на участок здания, то есть коридор, крыло или этаж. Эти принтеры могут быть доступны либо любому в компании, либо любому в бюро калькуляций. У некоторых могут быть личные принтеры из-за вопросов конфиденциальности (им нужно печатать документы, содержащие конфиденциальную информацию), эгоизма (они важные и демонстрируют это наличием собственных принтеров) или каких-либо других потребностей бизнеса. Кроме того, высокоскоростные, широкоформатные плоттеры, фотопринтеры и другие специализированные печатающие устройства могут иметь особый контроль доступа из-за нестандартных расходов на эксплуатацию.

---

[1] Мы представляем себе кошмар, когда финансовый директор требует наличия одного принтера на целую транснациональную компанию и устанавливает срок распространения распечаток на следующий день. Однако существует довольно много интернет-служб, придерживающихся именно такого подхода в отношении вопросов печати.

Существует компромисс между расходами и удобством. Большее количество принтеров обычно означает большее удобство: легче получить доступ к принтеру или больше доступных типов принтеров. Однако большее количество принтеров обходится дороже.

С другой стороны, общий, централизованный принтер может быть настолько дешевле, что вы можете воспользоваться частью сэкономленных средств, чтобы купить принтер значительно более высокого качества. Предположим, что недорогой настольный принтер стоит 100 долларов. Если десять человек совместно используют один принтер, то его самоокупаемость составляет 1000 долларов. На момент написания этой книги на 1000 долларов можно купить хороший сетевой принтер и еще останется достаточно денег на несколько лет обслуживания. Если этим принтером станут пользоваться 20 человек, то у них будет лучший принтер за половину цены отдельных настольных принтеров, кроме того, они станут выполнять небольшую зарядку, когда будут ходить за своими распечатками.

Пример: отсутствие стандартов для принтеров

Когда контроль над тратами невелик или отсутствует совсем, расходы станут непредсказуемыми. В одной компании было мало ограничений на трату денег на предметы дешевле 600 долларов. Когда стоимость настольных лазерных принтеров упала ниже этого предела, многие сотрудники стали их покупать, и поддержка десятков новых моделей добавилась к нагрузке группы системных администраторов. Им часто требовалось установить принтер, поддерживать его драйверы и отлаживать его работу. Без контрактов на обслуживание люди выбрасывали принтеры, а не ремонтировали их. Руководство начало разбираться в этой проблеме, и неофициальная проверка показала, что многие закупленные принтеры подключены к домашним компьютерам сотрудников. Были введены меры по контролю расходов, и вскоре проблему удалось решить. Большинство купленных принтеров были медленными и с низким качеством печати по сравнению с централизованно закупленными принтерами, расположенными в каждом коридоре. Однако сотрудники ненавидели эту политику. Их больше волновало наличие принтера в пределах нескольких дюймов от их стола, чем его более высокое качество или рентабельность.

24.1.2. Политика архитектуры печати

В каждой компании должны иметься письменные политики, связанные с печатью. Первая из них – *политика общей архитектуры печати*, определяющая, насколько централизованной будет печать. Задача этого документа – показать, сколько людей будут совместно использовать принтер для печати вообще – то есть один принтер на компьютер, один на коридор, один на здание, один на этаж, – кому положены персональные принтеры и как принтеры будут подключаться к сети.

Для приемлемой надежности сетевым принтерам требуется центральная система буферизации печати, устройство, принимающее и хранящее задания для

печати, пока принтер не будет готов их выполнить. Часто буферизация является элементом системы контроля доступа, потому что она определяет, кто на каком принтере может печатать. Кроме того, система буферизации может перенаправлять задачи по печати со сломанных принтеров и принимать такие интеллектуальные решения, как «напечатать это на фирменном бланке на любом принтере на четвертом этаже»[1]. В современных принтерах есть встроенная система буферизации, но их память может быть ограничена, поэтому отдельный узел буферизации все-таки может потребоваться. Политика должна определять требуемый уровень резервирования. Одна система буферизации часто может обслуживать десятки или сотни принтеров, но она создает одну точку возможного отказа. В некоторых системах буферизации печати есть «горячие» замены либо можно настроить резервные узлы буферизации. В некоторых ОС нельзя использовать для буферизации машину под другой ОС, не теряя функциональности. Вы можете сделать, чтобы такие машины использовали для буферизации центральный узел с той же самой ОС, имеющий программу шлюза, которая позволяет использовать главную систему печати, напрямую связанную с принтером (Limoncelli 1998).

Кроме того, данная политика должна подробно описывать, как выполняется обслуживание: собственными силами и расходными материалами или по контракту. В политике должна быть показана точка, в которой издержки обслуживания, в том числе трудовые затраты, время работы и время недоступности службы или другое условие, становятся настолько высокими, что замена принтера будет выгоднее.

В компании также должна быть *бухгалтерская политика*, которая определяет, покупаются ли принтеры подразделениями, которые их используют, из центрального бюджета или из специального источника. Подобные решения должны быть приняты в отношении оплаты обслуживания и ремонта. Оплата расходных материалов – бумаги, тонера – может быть спорным вопросом, если принтеры не прикреплены в явном виде к конкретным финансовым единицам в организации. В копирах и лазерных принтерах используется одна и та же бумага, поэтому, если они будут входить в разные бюджеты, может наступить неразбериха. Простейший метод – оплата всего из центрального бюджета. Поскольку все больше копиров подключаются к сетям и могут работать как лазерные принтеры, это становится естественной тенденцией развития.

С другой стороны, более точная градация оплаты может исключить растрату ресурсов. Университеты часто вводят постраничную оплату, с различными графиками цен для разных типов принтеров. Студенты могут получать определенное количество «бесплатных» страниц каждый семестр. Совершенного решения не существует, но деньги нужно откуда-то брать. Задача заключается в создании наименее неудобного решения.

Вопросы, касающиеся того, кто заказывает расходные материалы и кто заправляет их в принтеры, также должны быть элементом письменной политики. В некоторых офисах расходные материалы заказывает секретарь подразделения, но иногда заказы централизованы. В некоторых компаниях предполагается, что пополнять бумагу и менять картриджи будут пользователи конкретного

[1] Конечно, у них должна быть возможность сообщить пользователю, какой принтер в конце концов был выбран.

принтера, в других операторы наблюдают за принтерами и выполняют эти задачи. Мы не рекомендуем позволять пользователям самостоятельно заменять картриджи с тонером. Иногда эта процедура является сложной и подверженной ошибкам, и ее нельзя оставлять обычным пользователям. Более того, наш опыт показывает, что пользователи меняют картридж при малейших признаках проблем с качеством, тогда как обученный оператор может предпринять другие меры, например потрясти картридж с тонером, чтобы его хватило еще на пару сотен страниц. Замена картриджей без необходимости – это бесполезная трата денег, кроме того, здесь затрагиваются вопросы экологии.

Должен быть документированный *стандарт оборудования принтеров*. В этой политике должно быть две части. Первая часть должна меняться редко, и в ней необходимо указать долговременные стандарты, например будет ли использоваться PostScript или PCL, должны ли покупаться устройства для двусторонней печати, когда они доступны, какой протокол должны использовать принтеры для связи – LPD (Line Printer Daemon Protocol) через TCP/IP (McLaughlin 1990), протокол печати SMB (Server Message Block) для NT (Epps et al. 1999), AppleTalk или кабельное соединение через параллельные порты либо USB, – как принтеры подключаются к сети и т. д. Вторая часть должна представлять из себя список рекомендуемых принтеров и конфигураций на данный момент. Например, вы можете указать одну-две одобренные конфигурации для людей, покупающих цветной принтер, цветной принтер для слайдов и пару черно-белых принтеров в двух или трех ценовых диапазонах. Эта часть должна регулярно обновляться. Эти стандарты также помогают сэкономить деньги, потому что они могут обеспечить вашей компании оптовые скидки. Проблем можно избежать за счет фильтрации всех заказов на покупку оборудования через группу системных администраторов или других компетентных людей, как упоминалось в разделе 21.2.1, для проверки полноты заказов и определения времени установки, чтобы системные администраторы не были застигнуты врасплох, когда оборудование будет доставлено. Ограничение количества используемых моделей также снижает число типов расходных материалов, которые должны быть у вас в запасе, а это экономит деньги и позволяет избежать путаницы.

Пример: рекомендуемые конфигурации экономят время системных администраторов

Рекомендуемые конфигурации должны включать все, что пользователи могут забыть, но что потребуется системным администраторам для завершения установки. В компании была централизованная система печати, и в каждой части здания имелся принтер. Эти принтеры всегда были одной и той же модели. Группы, которым требовался принтер для собственного использования, часто покупали такую же модель принтера, как у остальных в здании. Однако группы не знали о необходимости покупки дополнительного блока двусторонней печати, кабеля и программы для подключения к сети. Когда системных администраторов просили устанавливать такие принтеры, им приходилось сообщать пользователям плохие новости о том, что, пока не будут куплены необходимые дополнения, устройством нельзя будет пользоваться. Эта проблема сохранялась, пока не был написан документ о стандартах принтеров.

Политика доступа к принтерам должна определять, кто к каким принтерам имеет доступ и как это будет поддерживаться. Например, людям может быть разрешено печатать на всех принтерах, только на тех принтерах, за которые заплатило их подразделение, или что-то среднее. Эта политика также должна определять, кто может отменять задания по печати на принтерах: например, те, кто не является системным администратором, могут отменять только свои собственные задания, а администраторы имеют возможность отменять любое задание печати на системах буферизации печати, которые они контролируют. В университетах может понадобиться тщательно контролировать это, потому что студенты часто имеют склонность к «войнам отмен».

Мы будем оптимистично смотреть на офисную среду. В бизнесе, под защитой брандмауэра, целесообразно разрешить всем в компании печатать на любом принтере и отменять любое задание на любом принтере. Разрешение печатать на любом принтере в компании предоставляет людям возможность заменить печатью факсимильную связь. Дизайнер в Сан-Хосе может напечатать документ на принтере в Японии через корпоративную глобальную сеть, экономя расходы на международный телефонный звонок. Можно ли злоупотреблять этим? Определенно. Однако это бывает очень редко и будет еще реже, если на первой странице напечатано имя нарушителя. Если у сотрудников есть частный принтер и они не хотят, чтобы на нем печатали другие, они могут закрыть свои двери. Если кто-то просит распечатку, это может быть хорошей возможностью сказать человеку, что не следует печатать на частном принтере. Если люди могут печатать на любом принтере, им должно быть известно, где расположены принтеры. Вы не захотите, чтобы люди по ошибке печатали на принтерах в другой стране.

Пример: «открытая» политика отмены

Кажется, что разрешать всем отменять задания на печать других людей – это создавать всем неприятности. Однако такая политика успешно применялась, когда Том работал в Bell Labs. Давление коллектива не позволяло отменять чьи-либо задачи, кроме своих. Однако в обычных случаях выхода печати из-под контроля – чаще всего при печати по ошибке кода PostScript вместо выходных данных PostScript – предотвращалась пустая трата бумаги, потому что первый, кто замечал проблему, мог отменить задачу по печати. Это не было бы так успешно в менее дружественных коллективах, где товарищество между сотрудниками не такое сильное. Учитывая, что задание может быть отменено с передней панели большинства принтеров, в большинстве офисов такая политика стала фактическим стандартом.

Нужно создать *политику назначения имен принтерам*. Мы предпочитаем присвоение имен по географическому принципу, то есть имя показывает, где находится принтер. Нет ничего более неприятного, чем принтеры, имена которых не несут никакой информации об их расположении. Несмотря на то что может быть «круто» и креативно иметь принтеры, названные `decaf`, `latte`, `mocha` и `froth`, это затрудняет людям поиск своих распечаток. Если назвать принтер по номеру помещения, в котором или рядом с которым он расположен, то пользователям будет проще его найти.

Одна из наиболее серьезных проблем в названии принтера по его местоположению заключается в том, что в случае изменения местоположения все должны будут обновить свою конфигурацию принтера. Иначе люди будут раздражены, когда узнают, что не могут найти принтер fl2rm203, потому что теперь он стоит в комнате 206 на другой стороне коридора. Возникновение подобной ситуации менее вероятно, если этажи спланированы так, что в них есть выделенные помещения для принтеров, которые вряд ли будут перемещаться или имеют форму, которая не подходит для использования в других целях.

Если принтер, скорее всего, будет перемещаться, для него лучше подойдет более общее название, например имя, указывающее, на каком этаже он находится, возможно, объединенное со словом *«север»*, *«восток»*, *«юг»* или *«запад»*.

Принтеры, управляемые централизованно, не следует называть по имени группы, которая пользуется принтером. Если эта группа переедет в другую часть здания, она захочет забрать принтер. Люди, которые останутся, потеряют этот принтер, либо им придется изменить свою конфигурацию принтеров, а это похоже на наказание ни за что. Принтеры, принадлежащие конкретным группам, не должны называться по группам, которые ими пользуются, чтобы, когда вы решите централизовать службу, людям было проще к этому привыкнуть.

UNIX-принтеры часто имеют имя из двух частей. Первая часть – это обычное имя принтера, а вторая часть может быть кодом, указывающим тип распечатки. Например, имя 2t408-d может отправить задачу на принтер в комнате 2t408 в дуплексном (двустороннем режиме), а 2t408-s может быть псевдонимом того же принтера, но в одностороннем режиме.

24.1.3. Структура системы

Когда будут определены правила, вы можете спроектировать и реализовать архитектуру системы печати. Некоторые системы печати предоставляют очень малую гибкость, другие – слишком большую.

- *Пиринговая* архитектура является очень децентрализованной: все узлы направляют по сети задачи напрямую на нужный принтер. Она является простейшей в создании, потому что часто вам нужно знать только IP-адрес или имя принтера, чтобы отправлять на него задания печати. Однако эта конфигурация может быть самой сложной в администрировании. Любое изменение принтера, которое требует изменений на стороне узла (клиента), должно быть распространено между всеми клиентами. Например, если принтер заменяется на более новую модель, всем узлам может потребоваться новый драйвер принтера.
- *Центральный буфер* – это более централизованная архитектура, которая предоставляет более высокий уровень контроля. В простейшей версии данной архитектуры все узлы отправляют свои задания печати на центральный сервер, который затем распределяет их по различным принтерам под своим управлением. Этот сервер работает как буфер, который собирает все задания по печати и затем может принимать интеллектуальные решения. Например, сервер может конвертировать различные форматы печати – PostScript в PCL или наоборот, – собирать информацию постраничной тарификации и т. д., а также способен выполнять интеллектуальный выбор принтера. Например, пользователи могут отправлять задачи на «первый доступный принтер на четвертом этаже», или на «любой цветной принтер»,

или на «цветной принтер для печати на слайдах самого высокого качества». Только этому узлу требуются драйверы и служебные программы конкретных принтеров, которым необходимо обслуживание, поэтому он является единственным местом, куда нужно будет вносить обновления.

У этих двух архитектур есть несколько вариантов. Одна из проблем пиринговых архитектур – по мере роста они становятся более сложными и хаотичными. Эту проблему можно смягчить за счет либо более централизованного подхода, либо применения какого-нибудь автоматизированного механизма обновления клиентов. Например, вы можете воспользоваться любым механизмом автоматической установки программ для распространения патча, который обновляет драйвер принтера или изменяет настройки принтера. UNIX-системы могут распространять информацию о конфигурации принтеров через различные механизмы: NIS, `cfengine` и т. д. Несмотря на то что большинство клиентов печати под UNIX не могут читать конфигурацию напрямую из NIS, это могут сделать заменяющие средства, такие как Line Printer Remote, next generation (LPRng) (Powell and Mason 1995). В качестве альтернативы простой скрипт может переводить информацию, записанную в базе данных NIS, в локальный файл конфигурации.

Проблема с центральным буфером заключается в том, что он создает единственную точку отказа. Однако, из-за того что за счет централизации вы можете сэкономить деньги, часть сэкономленных средств можно пустить на создание резервных средств. Буфер может представлять собой две избыточных системы буферизации, которые могут автоматически или вручную восстанавливаться после отказа. Кроме того, это может облегчить обновление серверов, потому что один сервер можно отключить для обновления без прерывания обслуживания. Иногда может быть трудно обеспечить автоматическое восстановление после отказа. Учитывая, насколько редкими являются сбои оборудования, вы можете выбрать ручное восстановление после отказа, если этот процесс хорошо документирован и его выполнению можно обучить всех системных администраторов.

Другие варианты этих архитектур включают системы буферизации печати для каждой группы, несколько резервных систем, одну система буферизации печати на здание и т. д. В некоторых компаниях есть две системы буферизации, каждая из которых обслуживает половину пользователей, возможно, разделенные по зданиям, но у систем имеется возможность заменить друг друга в случае отказа. Каждая система буферизации печати в системе печати увеличивает количество работы системных администраторов по ее поддержке. Существенную часть этой работы можно облегчить при помощи автоматизации, но имейте в виду, что не все можно автоматизировать.

В последнее время пиринговая архитектура становится более распространенной, потому что современные принтеры имеют надежные встроенные программы буферизации. Такое раньше было редкостью, а если и существовало, то было подвержено частым ошибкам. Настройка современных операционных систем для связи с принтером гораздо проще и обычно может выполняться пользователями без помощи системных администраторов.

Проблема с пиринговой печатью заключается в том, что становится трудно узнать, как отменить ненужное задание, если вы не можете найти машину, которая отправила его на принтер. Однако все больше принтеров поддерживают отмену задач напрямую с панели управления принтера.

21.1.4. Документация

Само собой разумеется, что архитектура, рабочие процедуры, и программы, используемые в вашей системе печати, должны быть документированы. Документация является критическим элементом любой хорошо организованной системы. Системные администраторы должны предоставить своим пользователям три типа документации по печати:

1. *Инструкция по печати* должно включать меню и кнопки, по которым нужно щелкнуть, чтобы подключиться к выбранному принтеру, и объяснять, какие команды должны быть выполнены. Например, в UNIX-среде может объясняться, какие параметры среды должны быть установлены, следует ли применять `lpr` или `lp` и какие опции использовать для односторонней и двусторонней печати, печати на бланках и других особых вариантов печати. Этот документ не должен меняться слишком часто. Он должен быть доступен как элемент начального руководства или веб-сайта, который показывается новым пользователям.
2. *Список принтеров* должен быть каталогом всех доступных принтеров, их местоположений и особенностей, таких как цвет, качество и т. д. Этот документ должен указывать пользователям, где они могут найти инструкцию по печати. Этот каталог должен обновляться каждый раз, когда в систему добавляется новый принтер или удаляется старый. Этот документ должен размещаться на стене рядом с каждым принтером, который в него входит, а также входить в состав начального руководства или веб-сайта, который показывается новым пользователям.
3. *Метка принтера* должна быть на каждом принтере и показывать его имя или имена. Лотки для бумаги должны быть помечены, если они предназначены для пленок, бланков и т. д.[1] Принтеры легко пометить, но мы все равно видели много компаний, в которых системные администраторы забывали это сделать. Пользователи принтеров будут считать, что это самая важная документация, которую вы можете предоставить. Остальное обычно можно выяснить!

Карты принтеров

В Google можно зайти на страницу *http://print*, чтобы просмотреть веб-сайт, на котором перечислены все принтеры по местоположению и планы этажей, чтобы помочь пользователям их найти. Щелчок по имени принтера вызывает меню, которое включает ссылки на настройку вашего компьютера для печати на этом принтере – сначала определяется ваша ОС и вам даются указания, – ссылку на описание возможностей принтера, ссылку, которая вызывает очередь печати для этого принтера, и ссылку, открывающую об этом принтере заявку в службе поддержки.

[1] Мы рекомендуем использовать единую схему расположения лотков. Например, лоток для пленок – это всегда лоток 2. Это поможет предотвратить ситуацию, в которой документы будут случайно напечатаны на пленках, а пленки – на бумаге.

24.1.5. Мониторинг

Как было сказано в главе 5, ничто не заслуживает названия *«служба»*, пока не осуществляется его мониторинг. Такого внимания требуют два аспекта. Первый из них – это собственно буферизация и печать. Системные администраторы должны осуществлять мониторинг каждой системы буферизации, чтобы убедиться, что очередь не зависла, диск буферизации не заполнен, логи обновляются, процессор не перегружен, диск буферизации не отказал и т. д. Это должно быть частью нормальной системы мониторинга.

Второй аспект, за которым необходимо следить, – это состояние каждого принтера. Картриджи и лотки для бумаги нужно заправлять. Запасы бумаги в шкафах нужно пополнять. Большинство сетевых принтеров поддерживают SNMP и могут предупреждать вашу систему мониторинга о том, что у них застряла бумага, кончаются чернила или бумага. Принтеры точно отслеживают, сколько у них осталось бумаги, поэтому о том, что бумага почти кончилась, могут быть предупреждены системные администраторы, хотя мы предпочитаем разрешать пользователям самим заправлять бумагу.

Хотя существуют автоматизированные средства сообщения о том, что бумага в принтере кончилась, автоматического способа сказать, есть ли рядом с принтером хороший источник бумаги, не существует. Системные администраторы могут либо регулярно проверять принтеры, либо попросить пользователей сообщать им, когда заканчивается бумага.

Пример: тестирование печати

Новые принтеры имеют средства индикации, показывающие, когда у них кончаются чернила, но более старым принтерам требуется тестовая печать. В одной компании пользовались программой, которая создавала пробную страницу для каждого принтера утром каждый понедельник. На этой странице были время, дата, предупреждение, чтобы пользователи не выбрасывали ее, а также большая проверочная распечатка. Был назначен оператор, который забирал эти распечатки и заправлял чернила, если тестовая распечатка была нечитаемой. Оператор вез тележку с бумагой и клал ее в шкафы для расходных материалов под каждым принтером. Такая очень простая система позволяла поддерживать высокий уровень обслуживания.

24.1.6. Экологические вопросы

Будучи системными администраторами, мы должны нести ответственность за экологические аспекты печати. Чернила токсичны. Печать уничтожает деревья, а выбрасывание распечаток заполняет свалки. Конечно, напечатанные страницы можно впоследствии перерабатывать, однако с переработкой также связаны расходы и экологическое воздействие. Системы печати должны быть спроектированы в расчете на минимизацию отходов. Картриджи с чернилами должны перерабатываться. Системные администраторы должны быть внимательны к экологическому воздействию химических веществ, используемых в процессе печати. Следует избегать печати, создающей отходы, и по возможности призы-

вать к решениям без использования бумаги. Кроме того, за счет снижения количества покупаемой бумаги и картриджей можно обеспечить значительную экономию расходов. Расходы на переработку отходов обычно снижаются, если отделять бумагу, которую можно переработать.

Пользователи будут сдавать бумагу на переработку, если этот процесс будет простым и реально выполнимым. Если нет корзин для перерабатываемых отходов, люди не будут их собирать. Размещение корзины для перерабатываемых отходов рядом с каждым мусорным ведром и каждым принтером упрощает переработку отходов. Наша обязанность как системных администраторов – создать такую программу, если она не существует, но создание такой системы может быть прямой обязанностью других людей. Мы должны взять на себя все обязанности по координации с хозяйственным отделом в создании такой системы или, если она уже существует, в обеспечении того, чтобы рядом с каждым принтером были расположены мусорные корзины только для бумаги, размещены инструкции и т. д. То же самое можно сказать о переработке использованных картриджей с чернилами. Это хорошая возможность для сотрудничества с людьми, ответственными за копиры в вашей организации, потому что в этом вопросе многие аспекты вашей деятельности пересекаются.

Некоторые аспекты являются обязанностями пользователей, но системные администраторы могут облегчить их, предоставляя пользователям подходящие средства. Кроме того, системные администраторы не должны создавать препятствия, прививая своим пользователям вредные привычки. Например, обеспечение доступности средств предварительного просмотра для распространенных форматов, таких как PostScript, для всех пользователей, помогает им меньше печатать. Принтеры и дополнительные средства печати должны по умолчанию поддерживать дуплексную (двустороннюю) печать. Не печатайте разделительную страницу перед каждой распечаткой. Замена бумажных форм веб-формами и процессами без использования бумаги также позволяет сэкономить бумагу, хотя сделать их простыми в использовании довольно тяжело.

Пример: создание программы переработки

В крупной компании не перерабатывали картриджи с чернилами, даже несмотря на то что на новых картриджах были закупочные метки и указания по возврату старых картриджей. Поставщик даже предлагал вознаграждение за возврат старых картриджей. Оправданием того, что компания не пользовалась преимуществами этой системы, было в том, что никто в компании не создал для этого процедуру! Прошли годы упущенной экономии, пока кто-то наконец решил проявить инициативу в создании процесса. Как только новая система была введена в строй, компания стала экономить тысячи долларов в год.

Мораль заключается в том, что такие вещи не делаются сами собой. Проявите инициативу. Все будут поддерживать процесс, если его создаст кто-то другой.

24.2. Тонкости

Системные администраторы могут внести в свою службу печати некоторые интересные дополнения, чтобы повысить качество обслуживания до уровня компании «Роллс-Ройс».

24.2.1. Автоматическое восстановление после отказа и балансировка нагрузки

Мы рассматривали резервные серверы печати. Часто восстановление таких систем после отказа производится вручную. Системные администраторы могут создать системы автоматического восстановления после отказа, чтобы снизить время простоя, связанное с проблемами с принтерами.

Если служба печати работает с большими объемами, системные администраторы должны обеспечить использование резервных систем для балансировки нагрузки. Например, может быть две системы буферизации печати, каждая из которых обслуживает половину принтеров для балансировки нагрузки и заменяет другую в случае сбоя для минимизации времени простоя.

В автоматическом восстановлении после отказа есть два элемента: обнаружение проблемы и ее передача другой системе буферизации. Причину отказа службы иногда трудно определить правильно. Система буферизации может не быть способной печатать, даже если она отвечает на эхо-запросы, принимает новые подключения, отвечает на запросы о состоянии и разрешает отправку новых заданий. Лучше всего, если сервер может предоставить более подробную диагностику, не делая распечатки. Если в очереди нет заданий, вы можете убедиться, что сервер принимает новые задания. Если задания в очереди есть, вы можете убедиться, что текущее задание не было в процессе печати слишком долго, что может быть признаком проблемы. Вы должны быть внимательны, потому что небольшие задачи PostScript могут создавать большое количество страниц или долгое время работать, не создавая страниц.

Важно определить способ избежать ложных сообщений. Вы также должны различать неработающий сервер и неработающий принтер.

Помимо проблем с серверами, большинство проблем печати мы видели на стороне рабочих станций, особенно это касается драйверов и приложений. Вероятность многократных одновременных сбоев можно снизить за счет наличия, по крайней мере, надежных серверов печати.

Печать с привлечением сторонних исполнителей

Если что-то необычное, связанное с печатью, требуется вам лишь время от времени, например брошюрование, использование дырокола, печать в больших объемах или очень широких форматах, многие типографии принимают файлы PDF. Отнести PDF-файл в типографию один раз в какой-то период времени гораздо выгоднее, чем покупать необычный принтер, который редко используется.

Практически все типографии принимают PDF-файлы по электронной почте или на своем веб-сайте. Некоторые типографии даже создали драйверы принтеров, которые «печатают в Сети». Эти драйверы отправляют распечатку на печатные устройства напрямую из приложений. Затем вы можете зайти на веб-сайт исполнителя для предварительного просмотра результатов, изменения опций и оплаты. Большинство типографий доставляют результаты вам, то есть вам не придется выходить из своего офиса.

24.2.2. Выделенный сотрудник для обслуживания

Принтеры – это механические устройства, и часто их надежность можно повысить, исключив их обслуживание необученными людьми. Мы не хотим недооценить технические способности наших пользователей, но мы видели, как очень умные люди ломали принтеры, пытаясь сменить картридж.

Следовательно, может быть полезно иметь выделенного клерка или оператора для обслуживания принтеров. Во многих компаниях есть достаточно принтеров для того, чтобы нанять для их обслуживания отдельного работника с частичной занятностью, который просто будет смотреть каждый принтер раз в несколько дней, чтобы проверить, правильно ли он печатает, достаточно ли в нем бумаги и т. д. Кроме того, этот человек может отвечать за ремонт принтеров. Несмотря на то что у компании может быть контракт на обслуживание, «чтобы об этом позаботились», кому-то все-таки надо связываться с поставщиком, согласовывать время ремонта и принимать техника. Согласование времени обслуживания и описание проблемы может требовать очень большого количества времени, и часто выгоднее назначить для выполнения этой задачи клерка, чем системного администратора. Этим может заниматься, например, секретарь или менеджер.

Заказ расходных материалов часто может быть отдан в ответственность секретарям или клеркам, если вы предварительно получите разрешение их руководителя. Напишите документ с точными кодами заказа для картриджей, чтобы исключить догадки и предположения.

24.2.3. Уничтожение бумаги

Люди печатают страшные вещи: личную электронную почту, конфиденциальную корпоративную информацию, номера кредитных карт и т. д. Мы даже видели, как некто проверял принтеры, печатая файл UNIX /etc/passwd, не зная, что зашифрованное второе поле могло быть взломано. В некоторых компаниях уничтожают мало документов, в каких-то есть особые правила уничтожения, другие уничтожают практически все.

Мы не так много можем сказать об уничтожении бумаги, кроме того, что хорошо бы уничтожать все, что вы не хотите видеть на первой полосе New York Times, и в этом случае лучше преувеличить опасность, чем недооценить ее. Если что-то не напечатать – это будет даже безопаснее, чем уничтожение.

Другое, на что нужно обратить внимание, – это то, что уничтожение бумаги собственными силами вызовет появление в вашей компании большого шредера для уничтожения бумаги, а уничтожение силами сторонних исполнителей предполагает передачу ваших бумаг на их станцию уничтожения. Мы постоянно слышим истории о службах уничтожения бумаги, которые были замечены в том, что они не уничтожают бумагу, как обещали. Мы не знаем, правда или это или городские сплетни, но настоятельно рекомендуем регулярно проверять ваших сторонних исполнителей по уничтожению бумаги, если вы пользуетесь их услугами. Услуги по уничтожению бумаги обычно довольно дороги, поэтому вы должны убедиться, что получаете то, за что платите.

Мы предпочитаем уничтожение бумаги собственными силами с назначением человека для наблюдения за процессом, чтобы обеспечить его правильное выполнение.

24.2.4. Борьба с недопустимым использованием принтеров

Старая пословица Usenet гласит: «Нельзя решить социальные проблемы при помощи технологий». Это справедливо и для печати. Нельзя написать программу для обнаружения использования принтеров не для работы или для выявления расточительной печати. Однако правильный контроль коллектива и обеспечение соблюдения политик позволяют многого добиться. В вашей политике допустимого использования (раздел 11.1.2) должно быть указано, какое использование принтера является недопустимым.

Постраничная оплата может создать убедительную причину для экономии бумаги. Если задача заключается в контроле расходов на печать, а не в возмещении затрат группы системных администраторов на расходные материалы, вы можете предоставить каждому человеку определенное количество «бесплатных» страниц в месяц или позволить подразделениям объединить свой «бесплатный» объем. В такой схеме большое значение имеет психологический фактор. Вам вряд ли захочется создавать ситуацию, в которой люди зря тратят время на что-то другое, потому что боятся, что их начальник накажет их за превышение своей нормы.

В одной компании каждый месяц просто объявляли десять сотрудников, которые печатали больше всех, чтобы пристыдить людей и призвать их меньше печатать. Теоретически предполагалось, что люди будут печатать меньше, если узнают, что они являются крупнейшими потребителями услуг печати. Однако некоторые сотрудники восприняли это как соревнование и состязались, кто будет входить в список больше всего месяцев подряд. Этот подход был бы более эффективным, если бы список показывался только руководству или если бы системный администратор приходил к этим людям лично и вежливо сообщал бы об их статусе. Стыд может работать только в определенных ситуациях.

Мы предлагаем уравновешенный нетехнический подход. Разместите принтер в заметном, часто посещаемом месте. Это отобьет желание использовать принтер в личных целях сильнее любой политики или системы тарификации. Если кто-то печатает особенно расточительно, обратитесь к человеку. Не будьте мелочны при небольших нарушениях, это раздражает.

Распечатка в 500 страниц

Системные администраторы были возмущены, когда однажды нашли около принтера 500-страничную распечатку читов для различных компьютерных игр. Когда это показали директору, он разобрался с этим очень мудро. Вместо того чтобы всех ругать, он разослал всем сотрудникам по электронной почте сообщения о том, что нашел эту распечатку около принтера без титульной страницы, указывающей, кто ее сделал. Он напомнил людям, что небольшое количество печати в неслужебных целях было допустимо и что он бы не хотел, чтобы такой очевидно ценный документ потерялся. Поэтому он попросил владельца документа зайти к нему в офис и забрать его. Через неделю распечатка была переработана, потому что хозяин так и не нашелся. Больше ничего никому не нужно было говорить.

24.3. Заключение

Печать – это бытовая услуга. Пользователи предполагают, что она всегда работает. Основа надежной системы печати – четко определенные политики о том, где будут размещаться принтеры – на рабочих станциях, централизованно или и здесь и там, – какие типы принтеров будут использоваться, как они будут называться и какие протоколы и стандарты будут применяться для связи с ними. Архитектура системы печати может варьироваться от сильно децентрализованной – пиринговой – до очень централизованной. Важно включить в архитектуру элементы резервирования и восстановления после сбоев. Для обеспечения качества обслуживания нужно выполнять мониторинг системы.

Пользователям системы печати требуется определенное количество документации. Нужно документировать, как печатать и где находятся принтеры, к которым они имеют доступ. На самих принтерах должны быть метки.

Печать оказывает влияние на экологию, поэтому системные администраторы обязаны не только работать с другими подразделениями для создания и поддержки программы переработки бумаги, но и предоставлять подходящие средства, чтобы пользователи по возможности избегали печати.

В лучших системах печати также есть автоматическое восстановление после сбоев и балансировка нагрузки, а не восстановление вручную. Там есть клерки, которые выполняют обслуживание и пополняют расходные материалы, на это не тратится время системных администраторов, а необученные пользователи не касаются чувствительных элементов принтеров. В лучших системах печати предоставляются услуги по уничтожению важных документов. Кроме того, в них учитывается, что многие проблемы печати являются социальными и не могут быть решены исключительно технологическим путем.

Задания

1. Опишите нетехнические политики печати в вашей среде.
2. Опишите архитектуру печати в вашей среде. Является ли она централизованной, децентрализованной или комбинированной?
3. Насколько надежна ваша система печати? Как вы это оценили?
4. Что происходит в случае сбоя в вашей системе печати и кто ставится в известность?
5. Когда появляются новые пользователи, как они узнают о правилах процесса печати? Как они узнают о ваших нормах допустимого использования?
6. Как вы решаете экологические вопросы, связанные с печатью? Перечислите политики и процессы, которые у вас есть, а также меры общественного воздействия и поощрения.
7. Какие способы избежать печати предлагаются вашим пользователям?

Глава 25

Хранение данных

В системах, которыми мы управляем, хранится информация. Возможности компьютеров по хранению информации удваиваются каждую пару лет. Первые домашние компьютеры могли хранить 120 Кб на гибком диске. Сейчас обычно говорят о петабайтах – миллионах миллионов килобайтов. Каждый эволюционный скачок в емкости требовал радикального изменения методов управления данными.

Вам нужно знать два факта о хранении данных. Первый из них – хранение становится все дешевле – невероятно, но факт. Второй – оно становится все дороже – невероятно, но факт.

Этот парадокс станет вам понятен, когда вы поработаете с хранением данным хотя бы недолгое время. Цена отдельного диска постоянно снижается. *Цена за мегабайт* стала такой низкой, что теперь люди говорят о *цене за гигабайт*. Когда в системах заканчивается дисковое пространство, люди жалуются на то, что они могут пойти в местный компьютерный магазин и купить диск практически за копейки. Как кому-то вообще может не хватать пространства?

К сожалению, стоимость подключения всех этих дисков и управления ими растет практически беспредельно. Раньше диски подключались при помощи шлейфа или двух, которые стоили по доллару каждый. Теперь волоконно-оптические кабели, подключенные к контроллерам крупных массивов данных, стоят тысячи. Данные записываются несколько раз, и для доступа к данным с нескольких узлов одновременно применяются сложные протоколы. Сильный рост требует радикальных изменения в системах аварийного восстановления или *резервных копиях*. По сравнению с тем, чего стоит управление данными, сами диски практически бесплатны.

Сдвиг основных акцентов с наличия пространства на управление данными в течение их жизненного цикла является невероятным. Теперь обсуждается не цена за гигабайт, а *цена за гигабайто-месяц*. Данные, опубликованные в начале 2006 года одной из крупных фирм по IT-исследованиям, показали изменение расходов на хранение. Для простых массивов с отражением различие в стоимости предложений низкого и высокого класса составляло два порядка.

Хранение данных – это широкая тема, по которой написано много хороших книг. Поэтому мы уделим внимание основной терминологии, некоторым размышлениям об управлении хранением и ключевым методам. Каждый из них является инструментом, готовым к применению при необходимости.

25.1. Основы

Чтобы хранение данных не стало войной между поставщиками и потребителями, мы предлагаем радикальную идею о том, что хранение должно управляться как ресурс сообщества. Это задает управлению хранением такое направление, что каждый может работать для достижения общих целей по пространству, времени работы, производительности и расходам. Хранение должно управляться, как любая другая служба, и у нас есть советы в этой области. Производительность, устранение неполадок и оценка новых технологий являются обязанностью группы обслуживания систем хранения.

Но начнем мы с краткого экскурса в терминологию и технологии хранения данных.

25.1.1. Терминология

Как системному администратору вам уже может быть знакомо многое из терминологии хранения данных. Поэтому мы кратко выделим термины и ключевые принципы, которые будут в дальнейшем использоваться в данной главе.

25.1.1.1. Основные элементы отдельных дисков

Чтобы понимать вопросы производительности различных систем хранения, следует разбираться в лежащих в их основе носителях и основных операциях жесткого диска. Понимание узких мест отдельных элементов дает основу для понимания узких мест и усовершенствований, которые появляются в более сложных системах.

- *Шпиндель, пластины и головки:* диск состоит из нескольких пластин, на которых записаны данные. Пластины укреплены на одном шпинделе и вращаются вместе. Данные на пластинах записываются на дорожках. Каждая дорожка – это окружность со шпинделем в центре, и каждая дорожка имеет свой радиус. Цилиндр – это все дорожки данного радиуса на всех пластинах. Данные записываются в секторах, или блоках, на дорожки, и дорожки имеют различное количество блоков в зависимости от того, насколько далеко от центра они находятся. Дорожки, находящиеся дальше от центра, длиннее, и поэтому в них больше блоков. Головки считывают и записывают данные на диске, нависая над соответствующей дорожкой. На каждой пластине есть одна головка, но они все укреплены на одном блоке и перемещаются вместе. Обычно за раз считывается целая дорожка или целый цилиндр, и данные кэшируются, так как время, необходимое для перемещения головок в нужное место (время поиска), больше, чем время, требуемое для поворота диска на 360°.
- *Контроллер диска:* электроника на жестком диске; контроллер диска реализует протокол диска, например SCSI или ATA. Контроллер диска связывается с узлом, к которому подключен диск. Для контроллеров диска важны уровень соответствия стандартам и любые реализуемые ими улучшения производительности, например буферизация или кэширование.
- *Адаптер главной шины (HBA – Host Bus Adapter):* HBA находится в узле и управляет связью между диском (или дисками) и сервером. Для связи с контроллером диска HBA использует протокол доступа к данным. Интел-

лектуальный HBA также может быть источником улучшений производительности. Обычно он находится на материнской плате компьютера или карте расширения.

25.1.1.2. RAID: избыточный массив из независимых дисков

RAID – это общая категория для методов, использующих несколько независимых жестких дисков для создания хранилища, которое больше, надежнее или быстрее, чем можно создать при помощи одного диска. Каждый метод RAID называется уровнем (табл. 25.1).

Таблица 25.1 Распространенные уровни RAID

Уровень RAID	Методы	Характеристики
0	Распределение	Быстрее чтение и запись, плохая надежность
1	Отражение	Быстрее чтение, хорошая надежность, очень дорогой
5	Распределенный контроль четности	Быстрее чтение, медленнее запись, более экономичен
10	Распределение с отражением	Быстрее чтение, лучшая надежность, наиболее дорогой

- *RAID 0,* также известный как распределение данных, распределяет данные по нескольким дискам так, что они могут работать как один большой диск. Виртуальный диск RAID 0 быстрее, чем одиночный диск; в блоке RAID на разных дисках может параллельно выполняться несколько операций чтения и записи. RAID 0 менее надежен, чем одиночный диск, потому что при сбое одного диска весь блок становится бесполезным. С увеличением количества дисков статистически растет вероятность ошибки.
- *RAID 1,* также известный как отражение, использует два или более дисков для записи одних и тех же данных. Нужно выбирать диски с идентичными характеристиками.

  Каждая операция записи выполняется на обоих (или всех) дисках, и данные на обоих (всех) дисках записываются идентично. Операции чтения можно разделить между дисками, ускоряя доступ для чтения. Скорость записи определяется самым медленным диском. RAID 1 повышает надежность. Если один диск отказывает, система продолжает работать.

> **Запомните: RAID 0**
>
> RAID 0 и RAID 1 – две наиболее распространенные стратегии RAID. Людям часто трудно запомнить, чем они отличаются. Вот наше мнемоническое правило: «RAID 0 дает нулевую помощь, когда диск ломается».

- *RAID 2 и 3* – это редко используемые стратегии, достаточно похожие на RAID 5, поэтому мы рассмотрим общий принцип там. Однако следует отме-

тить, что RAID 3 предоставляет особенно хорошую производительность при последовательном чтении. Таким образом, большие графические данные, потоковые данные и видеоприложения часто используют RAID 3. Если ваша организация хранит такие файлы, вы можете захотеть реализовать RAID 3 для этого конкретного сервера, особенно когда файлы обычно архивируются и не меняются часто.

- *RAID 4* также похож на RAID 5, но используется редко, потому что обычно он медленнее. RAID 4 быстрее RAID 5, только когда система специально создана под него. Одним из таких примеров является файловый сервер Network Appliance с тщательно отрегулированной файловой системой WAFL.
- *RAID 5*, также известный как распределенный контроль четности, ориентирован на повышение надежности, как и отражение, но с меньшими расходами. RAID 5 аналогичен RAID 0 – распределение для получения большего объема, – но имеет один дополнительный диск для записи информации восстановления. Если один диск отказывает, RAID 5 продолжает работать. Когда сломанный диск заменяют, данные на нем перестраиваются при помощи диска восстановления. Во время перестроения снижается производительность. RAID 5 предоставляет более высокую скорость чтения, как и RAID 0. Однако запись может занимать больше времени, так как создание и запись информации восстановления требуют чтения информации на всех остальных дисках.
- *RAID 6–9* либо не существуют, либо являются маркетинговым названием вариаций предыдущих уровней. Правда.
- *RAID 10*, изначально названный RAID 1 + 0, использует распределение для повышения размера и скорости, а отражение – для надежности. RAID 10 – это группа RAID 0, отраженная на другую группу. Каждый отдельный диск в группе RAID 0 отражается. Так как отражение – это RAID 1, такой стандарт шутливо называют 1 + 0, или 10. Перестроения на системе RAID 10 не так сильно затрагивают производительность, как на системе RAID 5. Как и в случае с RAID 1, многократные отражения возможны и широко используются.

RAID-системы часто поддерживают *«горячую замену»*, дополнительный неиспользуемый диск в корпусе. Когда диск отказывает, система автоматически перестраивает данные на диске «горячей замены» (это не справедливо для RAID 0, где потерянные данные нельзя перестроить). В некоторых системах RAID может быть несколько RAID-блоков, но только один диск «горячей замены». Первый RAID-блок, которому требуется новый диск, забирает дополнительный диск, что экономит расходы на несколько запасных дисков.

25.1.1.3. Тома и файловые системы

Том – это элемент хранилища данных, видимый серверу. Первоначально том был диском и каждый диск был одним томом. Однако с появлением разделов, RAID-систем и других технологий том может быть любым типом хранилища, предоставляемым серверу в целом. Сервер видит том как один логический диск, даже если тот фактически состоит из более сложных частей.

Каждый том отформатирован файловой системой. Каждый из нескольких типов файловых систем был изобретен для своей цели или для решения той или иной проблемы производительности. Распространенные файловые системы Windows – это FAT, DOS FAT32 и NTFS. В системах UNIX/Linux есть UFS, UFS2, EXT2/EXT3, ReiserFS и множество экспериментальных файловых систем. Некоторые файловые системы выполняют *протоколирование*, то есть ведут простой список изменений, запрашиваемых у файловой системы, и применяют их разом. Это повышает скорость записи и ускоряет восстановление после сбоя системы.

25.1.1.4. DAS: хранилище прямого подключения

Хранилище прямого подключения, или DAS (Directly Attached Storage), – это обычный жесткий диск, подключенный к серверу. DAS означает любое решение по хранению, в котором хранилище подключено к серверу кабелями, но не по сети. Он включает RAID-массив, напрямую подключенный к серверу.

25.1.1.5. NAS: хранилище сетевого подключения

Хранилище сетевого подключения, NAS (Network-Attached Storage), – это новый термин для технологии, существующей довольно недолго: клиентов, осуществляющих доступ к хранилищу, подключенному к серверу. Например, для UNIX-клиентов, которые используют NFS для доступа к файлам на сервере, или систем Microsoft Windows, использующих CIFS для доступа к файлам на Windows-сервере. Многие поставщики делают сетевые файловые серверы «под ключ», которые сразу работают с несколькими протоколами общего доступа к файлам. Network Appliance и EMC производят такие системы для хранения больших объемов информации. Linksys и другие компании производят меньшие системы для потребителей и малого бизнеса.

25.1.1.6. SAN: сети хранения данных

Сеть хранения данных, SAN (Storage Area Network), – это система, в которой как дисковые подсистемы, так и серверы включаются в выделенную сеть – специальную сеть с высокой скоростью и низкой задержкой, оптимизированную под протоколы систем хранения. Любой сервер может подключиться к любой системе хранения – по крайней мере, в соответствии с правилами контроля доступа. То, к чему могут подключаться серверы, – это том системы хранения, который определяется своим номером логического блока (LUN – Logical Unit Number). LUN может быть диском, слоем группы RAID 5, целой стойкой систем хранения или чем угодно, к чему обеспечивают доступ системы хранения. Серверы осуществляют доступ к LUN на уровне блоков, а не файловой системы. Обычно только один сервер может подключаться к определенному LUN в конкретный момент времени, иначе серверы будут путаться, потому что одна система будет обновлять блоки, а другие не будут этого видеть. Некоторые системы SAN предоставляют **кластерные файловые системы**, в которых выбирается один сервер для разграничения доступа, поэтому несколько серверов могут одновременно получать доступ к одному тому. Средства резервного копирования на магнитные ленты также можно подключить к сети и сделать общедоступными с тем преимуществом, что многие серверы будут совместно использовать один дорогой привод для магнитной ленты. Другое преимущество SAN заключается в том, что они снижают объемы изолированного хранения. При исполь-

зовании DAS некоторым серверам может не хватать дискового пространства, а у других оно бывает достаточным. Свободное пространство недоступно для серверов, которым оно необходимо. С технологией SAN у каждого сервера могут быть разделы любого требуемого размера, и дисковое пространство не изолируется от применения.

25.1.2. Управление хранением

Методы управления хранением полагаются на комбинацию процессов и технологий. Самые успешные решения включают пользователей как партнеров, а не делают системных администраторов «полицией систем хранения».

Довольно часто пользователи приходят к системным администраторам со срочным запросом на большее пространство для конкретного приложения. Универсального ответа не существует, но применение рассмотренных принципов может значительно уменьшить количество так называемых экстренных запросов дискового пространства, которые вы получаете. Всегда лучше предупреждать проблему, чем реагировать на нее, и это определенно касается хранения.

25.1.2.1. Относитесь к системам хранения как к ресурсу сообщества

Распределение пространства становится менее политическим, а пользователи больше участвуют в самоуправлении, когда серверы хранения выделяются по группам. Это особенно эффективно, если расходы на службу хранения выделяются из собственного бюджета группы. Таким образом, пользователи и их цепь руководства чувствуют наличие большего контроля и ответственности.

Исследования показывают, что приблизительно 80% расходов на хранение – это накладные расходы – главным образом, на поддержку и резервные копии, – а не стоимость жестких дисков. Должна быть возможность работать с руководством, чтобы передать по крайней мере некоторые из накладных расходов каждой группе. Этот подход является наилучшим для компании, потому что руководители, чьи бюджеты затронуты растущими потребностями хранения, также являются теми, кто может попросить свои группы прекратить ставшую неактуальной работу для экономии пространства.

Однако иногда невозможно выделить сервер хранения одной группе. Когда сервер хранения должен обслуживать много групп, всегда лучше всего начать с оценки потребностей хранения вашей пользовательской базы. Когда оценка будет выполнена, вы будете знать, какое пространство требуется группе сейчас, удовлетворяет ли имеющееся пространство этим требованиям и какое пространство группа предполагает использовать в будущем.

Объединяя данные оценок потребностей различных групп, вы сможете построить общую картину потребностей организации. Во многих случаях перераспределение части имеющегося пространства может быть достаточным для удовлетворения выявленных потребностей. В других случаях нужно составить план приобретения оборудования для предоставления дополнительного пространства.

Выполнение оценки потребностей хранения подразделений и групп является началом процесса создания сообщества хранения. В качестве элемента оценки группы будут рассматривать свои потребности хранения с точки зрения бизнеса и потребностей работы, а не просто будут говорить: «Чем больше, тем лучше!»

Одно из существенных преимуществ такого изменения в отношении к вашим пользователям заключается в том, что системные администраторы больше не будут «плохими парнями», а станут людьми, которые помогают пользователям выполнять нужные задачи. Пользователи в рамках своих групп могут самостоятельно следовать своей программе действий в плане хранения, и из поля зрения персонала поддержки пропадает весь набор распространенных жалоб пользователей.

Общая и пригодная для применения емкость диска

При покупке средств хранения важно помнить, что общее пространство значительно отличается от пространства, пригодного для использования.

Компании требовался сетевой массив хранения для 4 Тб имеющихся данных с предполагаемым ростом до 8 Тб в течение 2 лет. Пользователь сказал об этом поставщику, который охотно отправил ему 8-гигабайтную систему хранения. Пользователь начал конфигурировать массив, и значительная часть пространства ушла на текущие нужды файловой системы, а также диски для избыточности RAID, образов системы и «горячей замены». Вскоре пользователь обнаружил, что текущие потребности приближались к 100% того, что осталось. Система не могла поддерживать никакой рост.

К счастью, пользователь смог в рабочем порядке решить вопрос с поставщиком и заменить диски вдвое большими. Из-за того что это было сделано до того, как пользователь принял официальную доставку, диски не считались «подержанными».

Несмотря на то что проблема с потребностями емкости в будущем была теперь решена, сложности не прекратились. Большее количество дисков требовало бóльших ресурсов процессора. Почти две недели приложение было очень медленным, пока не была назначена экстренная модернизация процессора контроллера массива. Финансовому отделу это не очень понравилось, потому что ему пришлось одобрить первоначальную систему, затем обновление дисков, а потом выделить крупную сумму на модернизацию процессора.

25.1.2.2. Проведите оценку потребностей хранения

Вы могли подумать, что первый шаг в оценке потребностей хранения – узнать, кто какими системами хранения пользуется. На самом деле это *второй* шаг. Первый шаг – поговорить с подразделениями и группами, которые вы поддерживаете, чтобы узнать их потребности. Если начинать процесс оценки, основываясь на текущем использовании, часто это пугает людей – а вдруг вы будете отбирать у них ресурсы или перераспределять ресурсы без учета их мнения.

Если вы пойдете прямо к своим пользователям и спросите у них, что работает и что не работает в нынешней среде хранения, вы создадите связь и установите доверие. Если вы сможете показать им графики роста их индивидуальных объемов хранения данных за последний год и воспользуетесь ими, чтобы обучить пользователей, а не ругать их, это может помочь разобраться в их реальных потребностях.

То, что вы узнаете, может удивить вас, как приятно, так и неприятно. Некоторые группы могут дать неправильные сведения о своих потребностях, боясь нехватки ресурсов. Другие могут бороться за выживание со слишком малым объемом ресурсов, но не жаловаться, потому что они убеждены, что все находятся в такой ситуации.

Какие вопросы вы должны задавать при оценке дискового пространства? Спросите об общем использовании дисков, как нынешнем, так и перспективном, на следующие 6–18 месяцев. Хорошая идея – пользоваться более привычными единицами измерения, чем просто «месяцы», если это возможно. Пользователям может быть проще указывать рост в процентах, а не в гигабайтах. Например, спросите о следующих 2–6 кварталах в компании или о ближайших семестрах в учебном заведении. Вам также нужно поинтересоваться тем, какие запускаются приложения и какие проблемы возникают при их повседневном использовании. Вы можете считать, что адекватно наблюдаете использование группой дискового пространства и видите тенденции развития, поэтому способны без труда предсказывать потребности группы, но некоторые элементы вашей инфраструктуры хранения уже могут быть перегружены так, что этого не видно из простых показателей. Это может стать понятным, когда пользователи предоставят сведения.

Невозможно достичь цели

Средняя фирма по разработке чипов, тесно взаимодействуя с новым партнером, заказала высококлассное оборудование для нового кластера, удовлетворяющего требованиям партнера. Производительность, доступность по цене, надежность и т. п. анализировались и горячо обсуждались. Однако, после того как появилось новое оборудование, оказалось, что одна маленькая деталь была упущена. Компания, заказавшая новое оборудование, работала с данными, которые отличались от данных партнера, и заказанное решение по хранению нельзя было расширять, используя то же самое оборудование. Чтобы сделать кластер большего размера, нужно было бы заменить больше половины более дорогих компонентов (корпус, контроллеры). Вместо того чтобы удовлетворять потребности по хранению всей инженерной группы компании в течение года, он работал в одном подразделении около полугода.

Кроме того, возможно, что ближайшие события, которые выделяются из общего потока, могут повлиять на потребности хранения. Например, подразделение, которое вы поддерживаете, может в следующем семестре планировать принять ученого, способного принести большое количество исследовательских данных. Либо инженерная группа может работать над внесением в свой график выпуска еще одного продукта или дополнительных сценариев использования в свое автоматическое тестирование – все это, конечно, потребует значительного увеличения выделяемого пространства. Часто системные администраторы узнают об этом в последнюю очередь, так как ваши пользователи могут и не думать о своих планах в смысле требований, необходимых для реализации информационных систем. Таким образом, очень полезно поддерживать хорошие связи и в явном виде спрашивать о планах пользователей.

Работайте вместе, чтобы уравновесить нагрузку системы

В одной из компаний Страты инженеров по окончательной сборке программ раздражало отслеживание проблем в автоматических сборках поздно ночью. Некоторые сборки таинственным образом давали сбои на отсутствующих файлах, но проблема была невоспроизводима вручную. Когда инженеры рассказали о своей проблеме системным администраторам, те смогли проверить логи сервера и графики нагрузки затронутых узлов. Оказалось, что изменение в графике сборки вместе с новыми тестами, реализованными в сборке, вызвали пересечение по времени процессов сборки и резервного копирования. Даже несмотря на то, что они работали на различных серверах, эта одновременная нагрузка вызывала превышение уровня нагрузки одного файлового сервера над нормальным уровнем в несколько раз, что вызывало увеличение времени ожидания запросов к некоторым файлам. Отсутствие файлов вызывало сбои разделов сборки, затрагивая, таким образом, всю сборку в самом конце, когда делалась попытка связать все вместе.

Так как эта сборка обычно требовала 12–18 ч, сбои серьезно влияли на график работы инженеров. Поскольку резервное копирование также является критически важным, оно не могло быть отключено, когда инженерам не хватало ресурсов. Был достигнут компромисс, предполагающий изменение как времени сборки, так и времени резервного копирования, чтобы минимизировать вероятность их перекрытия. Это решило сиюминутную проблему. Для решения проблемы в корне была начата реорганизация систем хранения, чтобы сборка следующих продуктов не сталкивалась с такими проблемами.

25.1.2.3. Отражайте группы в инфраструктуре хранения

Когда вы соберете необходимую информацию о нынешних и будущих потребностях ваших пользователей в системах хранения, следующим шагом является отражение групп и подгрупп в инфраструктуре хранения. На этом этапе вам, возможно, придется решить, группировать ли пользователей со сходными потребностями по применению приложений или по структуре отчетности и рабочих групп.

Если это возможно, распределяйте пользователей по подразделениям или группам, а не по использованию. Большинство проблем с ресурсами хранения являются политическими и/или финансовыми. Отделение пользователей одного сервера или тома системы хранения в одну рабочую группу создает естественный путь разрешения всех разногласий об использовании ресурсов полностью в пределах этой рабочей группы. Используйте групповые разрешения на запись, чтобы обеспечить запрет использования этого хранилища теми, кто не входит в группу.

Некоторые пользователи, распределенные по нескольким подразделениям или рабочим группам, могут иметь похожие, но необычные требования. В этом случае может быть необходимо решение с общим хранилищем, удовлетворяющим этим требованиям. Такой сервер хранения должен быть разделен на разделы,

чтобы изолировать каждую группу на своем собственном томе. Это устраняет по крайней мере один элемент возможного конфликта из-за ресурсов. Также исчезает необходимость участия системных администраторов в разрешении конфликтов из-за дискового пространства, так как каждая группа может сама управлять выделенным ей томом.

Если ваша среда поддерживает квоты, а ваши пользователи не сопротивляются их применению, можно установить внутри группы индивидуальные квоты на использование пространства. При организации такого типа распределения пространства в имеющихся системах хранения может быть полезным временно установить групповые квоты при перераспределении объемов выделенного пространства.

Многие люди будут против использования квот, имея для этого хорошую аргументацию. В критические моменты квоты могут снижать производительность. Инженер, который пытается собрать или проверить элемент нового продукта, но упирается в ограничение квоты, вынужден либо тратить время на освобождение достаточного пространства, либо связаться с системным администратором и бороться за повышение квоты. Если у инженера близок предельный срок выполнения, это может вызвать сбой графика всей работы над продуктом. Если ваши пользователи сопротивляются квотам, выслушайте их аргументы и посмотрите, возможен ли какой-либо компромисс, который будет удобен обеим сторонам, например экстренные запросы на повышение с гарантированным временем ответа. И хотя вам необходимо понимать потребности каждого человека, вам также нужно видеть картину в целом. Реализация квот на сервере таким образом, что они не будут позволять кому-то работать, – плохая идея.

25.1.2.4. Разработайте политику хранения запасных частей

В большинстве компаний в каком-то виде есть запасы часто требуемых запчастей. Мы рассмотрели запчасти вообще в разделе 4.1.4, но хранение требует немного дополнительного внимания.

Раньше типы дисков, применяемые в системах хранения и на рабочих станциях, сильно различались. Это означало, что системным администраторам было гораздо проще выделить определенный набор запасных дисков для инфраструктурного использования. Сейчас многие массивы хранения и серверы рабочих групп строятся из серийных частей, и такие диски могут использоваться как на настольной рабочей станции, так и в массиве хранения рабочей группы. Обычно считается, что общие запчасти – это хорошо. Однако, если пользователю откажутся дать новый диск, но он увидит неиспользуемый диск на полке на случай сбоя сервера, это может показаться ему произволом. Как системные администраторы могут обеспечить достаточное резервирование дисков в качестве запчастей для важной системы хранения, не скрывая дисков, которые также нужны для новых настольных систем или нужд отдельных пользователей? Здесь следует найти баланс, который является важным элементом политики, указывающей, как распределяются запчасти. Немногие системные администраторы могут собрать столько запчастей, сколько они хотели бы, поэтому наличие системы для их распределения очень важно.

Лучше всего отделять запасные диски общего назначения от запасных дисков для инфраструктуры хранения. Вы можете прогнозировать количество необходимых дисков для обеих задач на основе сбоев похожего оборудования, происходивших в прошлом. Если вы отслеживаете использование общего простран-

ства – и вы должны это делать, чтобы избежать сюрпризов, – то можете сделать некоторые оценки о том, как часто диски отказывают, чтобы количество запасных дисков было адекватным.

При росте объемов хранилищ планируйте не только количество дисков, необходимых для расширения существующих хранилищ, но и возможную модернизацию сервера, например процессора и памяти. Если вы планировали расширение за счет приобретения новых систем целиком, например автономных сетевых массивов хранения, обеспечьте закупку запчастей для этих систем до конца финансового года, в котором они будут приобретаться.

25.1.2.5. Планируйте будущее хранение

Особенно сложный аспект запасных частей для систем хранения заключается в том, что, когда пользователь просит диск, ему почти всегда нужно больше, чем просто диск. Пользователю, чей системный диск отказал, действительно нужен новый диск, а также стандартизированная установка ОС. Пользователю, у которого заканчивается общее дисковое пространство и который хочет установить свой диск, действительно нужно больше общего пространства или еще один диск, а также дополнительное резервное копирование. И так далее.

Мы не призываем системных администраторов к образу мыслей «докажите, что вам это нужно». Системные администраторы должны стараться помогать людям, а не быть церберами. Поэтому вы должны понимать, что каждый раз, когда диск покидает ваш шкаф для хранения, скорее всего, потребуется что-то еще. Другой возможный образ мыслей заключается в том, что сейчас существует проблема, решение которой вам известно, а при отсутствии ее устранения в будущем возникнет проблема, которую вам потребуется выявить. С какой из них вы предпочли бы иметь дело?

К счастью, как мы показали во многих разделах этой книги, можно структурировать среду, чтобы такие проблемы проще решались по умолчанию. Если в вашей компании имеются резервные копии на отдельных рабочих станциях, некоторые программы резервного копирования позволят вам настроить их так, чтобы они автоматически обнаруживали новый локальный раздел и начали создавать его резервные копии, если это не было специально отменено. Сделайте доступными для пользователей сетевые загрузочные диски, а также инструкции, как ими воспользоваться для установки ОС по умолчанию на новый диск. Этот подход позволяет пользователям заменять свои диски и получать стандартизированный образ ОС. Запланируйте ежеквартальный технологический перерыв, чтобы у вас была возможность обновлять общую систему хранения для выполнения перспективных требований, прежде чем пользователей затронет недостаток пространства. Думать о службах хранения – хороший способ быть в курсе особенностей вашей среды и мест, где вы можете улучшить обслуживание своих пользователей.

25.1.2.6. Создайте стандарты хранения

Стандарты помогают вам сказать «нет», когда появляется кто-то с непонятным оборудованием и говорит: «Пожалуйста, установите это мне». Если вы установите стандарты хранения, люди с меньшей вероятностью смогут провести заказ нестандартного оборудования через бухгалтерию и затем будут ожидать, что вы станете поддерживать все, что у них есть.

Широкий диапазон различных решений по хранению означает, что найти то, которое подходит вам, является гораздо лучшей стратегией, чем поддержка всего и вся. Наличие стандарта помогает держаться в стороне от оборудования, которое ему не соответствует.

Стандарт может простым, например запиской от руководителя, в которой говорится: «Мы покупаем только IBM», или сложным, например длинным документом с подробными требованиями, которым должен соответствовать поставщик и его решения, чтобы их можно было покупать. Задача стандартов – обеспечить целостность за счет определения процесса, набора характеристик или и того и другого.

У стандартизации есть много преимуществ, от содержания общего набора запчастей до минимизации количества различных систем, с которыми системный администратор должен справляться при интеграции систем. Как только вы дойдете до наличия плана хранения, который учитывает как нынешние, так и будущие потребности хранения, важно создать стандартизацию. В некоторых организациях может быть очень трудно реализовать контроль соблюдения стандартов, но это всегда стоит приложенных усилий. Так как жизненный цикл многих систем является относительно коротким, неоднородная среда, полная различных систем, может стать унифицированной средой в течение относительно короткого промежутка времени благодаря установке стандарта и приобретению только того оборудования, которое ему соответствует.

Если в вашей организации уже есть стандарты для определенных типов запросов или покупок, начните с изучения этой системы и добавления в нее стандартов. В ней могут быть наборы процедур, которые нужно соблюдать, например встречи с потенциально заинтересованными лицами, создание письменных спецификаций и т. д.

Если в вашей организации нет стандартов, вы можете проявить инициативу для своего подразделения. Часто вы сможете найти союзников в закупочных или финансовых отделах, так как стандарты обычно облегчают их работу. Наличие стандарта предоставляет им возможность обратиться за справкой, когда в заказе появляется что-то необычное. Оно также предоставляет им возможность разобраться с людьми, которые начинают с ними спорить о закупке оборудования, а именно либо попросить их ознакомиться со стандартом, либо направить к людям, которые его создали.

В общем случае начинайте с обсуждения необходимости стандартов и унифицированной базы запасных частей со своим руководителем и/или людьми из финансового отдела. Попросите, чтобы они передавали все заказы на новые типы оборудования в IT-подразделение перед их подачей поставщику. Заблаговременно работайте с заинтересованными лицами в подразделениях для установки стандартов систем хранения и файловых серверов. Предоставьте свою помощь для рекомендации систем и работы с пользователями, чтобы определить потенциальные кандидатуры для стандартизации.

Эта стратегия может предотвратить раздражение от работы с одиночным массивом хранения, несовместимым с коммутатором вашей сети хранения, или какой-нибудь новой интерфейсной картой, которая, как оказалось, не поддерживается версией Linux, используемой вашими разработчиками. Наихудший способ справиться с попытками установки неподдерживаемых систем – игнорировать пользователей и их запросы. Ваши пользователи станут раздражаться

и думать, что им нужно обойти вас, чтобы попытаться напрямую заявить о своих потребностях хранения.

Модернизация с переходом на более крупный принтер часто вызывает прекращение использования старых дисков или подсистем хранения. Если они достаточно старые, чтобы от них можно было избавиться, мы настоятельно рекомендуем полностью стирать их содержимое. Мы часто слышим истории о подержанных дисках, купленных на eBay, которые оказывались полными номеров кредитных карт или частной информации компании.

Люди, принимающие финансовые решения, обычно предпочитают, чтобы оборудование повторно использовалось внутри компании. Вот несколько возможных способов использования:

- Использовать оборудование в качестве запасных частей для нового массива хранения или для построения нового сервера.
- Настроить старые диски как локальные временные диски для приложений с интенсивной записью, например компиляции программ.
- Повысить надежность ключевых серверов, установив дублирующую ОС для перезагрузки под ней при сбое системного диска.
- Перевести определенную часть в пространство подкачки, если в вашей ОС оно используется.
- Создать самодельный RAID-массив для непринципиальных приложений или временного хранения данных.
- Создать глобальное временное пространство, доступное каждому, под названием /home/not backed up. Люди найдут множество повышающих производительность применений для такой службы. Название важно: людям нужно постоянно напоминать о том, что в данном случае они пользуются дисковым пространством без гарантий надежности.

25.1.3. Хранение как служба

Вместо того чтобы рассматривать систему хранения как объект, подумайте о ней как об одной из многих служб. Затем вы можете применить все стандартные базовые знания о службах. Что-то может считаться службой, если у него есть SLA и выполняется мониторинг, позволяющий следить за тем, соответствует ли доступность SLA.

25.1.3.1. SLA хранения

Что должно входить в SLA хранения? Инженерной группе могут понадобиться определенные объемы пространства, чтобы обеспечить автоматическим сборкам релизов достаточно пространства для ежедневной работы. У финансового отдела могут быть минимальные ежедневные потребности в пространстве, но ему может требоваться определенный объем пространства раз в квартал для создания отчетов. Группа обеспечения качества или группа, администрирующая ограниченные по времени экзамены студентов, может выразить свои потребности во времени ответа, а также в общем дисковом пространстве.

SLA обычно отражаются в доступности и времени ответа. Доступность для системы хранения может рассматриваться и как достижимость, и как количество пригодного для использования пространства. Время ответа обычно оценивается как задержка – время, необходимое для завершения ответа, – при заданной

загрузке. Кроме того, в SLA должны быть указаны ожидания по среднему времени исправления неполадок (MTTR – Mean Time Trouble Repair).

Используйте стандартные средства тестирования для измерения этих показателей. У них есть преимущества возможности использования независимо от платформ. Система должна тестироваться в вашей собственной среде с вашими собственными приложениями, чтобы убедиться, что система будет вести себя как объявлено, но, по крайней мере, вы можете настоять на конкретном минимальном результате тестирования, чтобы взять систему для собственной оценки, которая будет включать больше работы и участия как с вашей стороны, так и со стороны поставщика.

25.1.3.2. Надежность

Все рано или поздно ломается. Вы не можете предотвратить сбой жесткого диска. Вы можете обеспечить совершенное, рекомендованное поставщиком охлаждение и питание, и все равно в конце концов он сломается. Вы не можете предотвратить сбой HBA. Время от времени бит, передаваемый по кабелю, попадает под гамма-луч и инвертируется. Если у вас восемь жестких дисков, вероятность того, что один завтра сломается, в восемь раз выше, чем если бы у вас был только один. Чем больше у вас оборудования, тем выше вероятность сбоя. Звучит удручающе, но есть и хорошая новость. Существуют методы, чтобы справиться со сбоями и достичь практически любого необходимого уровня надежности.

Главное – отделить поломку компонента от прекращения работы. Если у вас есть один жесткий диск, его сбой приводит к прекращению работы: соотношение поломок и прекращений работы составляет 1:1. Однако, если у вас есть восемь жестких дисков в конфигурации RAID 5, одна поломка не вызовет прекращения работы. Чтобы вызвать прекращение работы, требуется два сбоя, один из которых происходит быстрее, чем может быть выполнена «горячая замена». Мы успешно отделили поломку компонента от нарушений обслуживания. Подобная стратегия может применяться к сетям, расчетам и другим аспектам системного администрирования.

Конфигурация службы хранения может повысить ее надежность. В частности, определенные уровни RAID повышают надежность, NAS также можно настроить так, чтобы повысить общую надежность.

Преимущество централизованного хранения (NAS или SAN) заключается в том, что дополнительные затраты на надежность распределяются между всеми пользователями службы.

- *RAID и надежность*: все уровни RAID, кроме RAID 0, увеличивают надежность. Данные на избыточном блоке RAID продолжают быть доступными, даже если диск ломается. Вместе с доступной «горячей заменой» избыточная конфигурация RAID может существенно повысить надежность.

  Однако важно осуществлять мониторинг системы RAID на предмет сбоя дисков и хранить несколько запасных дисков для замены сломанных. Каждый опытный системный администратор может рассказать страшную историю о системе RAID, за которой не наблюдали, а сломанный диск не менялся несколько дней. В конце концов ломается второй диск и теряются все данные системы. Многие системы RAID можно настроить так, чтобы они отключались через 24 ч работы в аварийном режиме. Остановка работы системы может быть безопаснее, чем отсутствие ее мониторинга в течение нескольких дней.

- *NAS и надежность:* NAS-серверы обычно поддерживают какую-то форму RAID для защиты данных, но надежность NAS также зависит от надежности сети. В большинстве систем NAS есть несколько сетевых интерфейсов. Для еще большей надежности подключайте все интерфейсы к разным сетевым коммутаторам.
- *Определите, какую надежность вы можете себе позволить:* большинство пользователей просят 100-процентную надежность. Однако на самом деле немногие руководители хотят тратить средства, необходимые для достижения уровня надежности, которого желают их сотрудники. Дополнительная надежность экспоненциально дороже. Небольшое повышение надежности стоит недорого, а совершенная надежность – дороже, чем большинство людей могут себе представить. В результате они оказываются потрясенными ценами, когда разбираются с различными требованиями к времени безотказной работы систем хранения.

Компании, предоставляющие крупномасштабные решения по обеспечению надежности, уделяют основное внимание времени безотказной работы и простоте восстановления при использовании их систем и призывают вас подсчитывать стоимость каждой минуты времени простоя, которое их системы могут потенциально предотвратить. И хотя их утверждения в общем правильны, эту экономию нужно сравнить с уровнем дублирующих ресурсов и расходов на их обслуживание. Решение по защите одного важного диска или раздела будет требовать наличия нескольких наборов дисков. В приложениях отраслей, где есть динамически изменяющиеся базы данных, например в финансовой, медицинской сферах или в электронной коммерции, обычно имеется две копии: одна локальная – в информационном центре, а другая – в удаленном информационном центре. Непрерывная защита данных (CDP – Continuous Data Protection) является наиболее дорогим методом защиты данных и поэтому используется только в крайнем случае.

Обеспечение высокой доступности данных стоит дорого. Задача системных администраторов – ставить руководство в известность о расходах, связанных с требованиями по времени безотказной работы систем хранения, включать эти расходы в подсчеты рентабельности инвестиций и оставлять деловое решение руководству. Требования могут быть изменены или перенаправлены для достижения наилучшего компромисса между расходами и надежностью.

25.1.3.3. Резервное копирование

Один из важнейших элементов службы хранения – это стратегия резервного копирования. Резервному копированию посвящена глава 26, здесь мы просто рассмотрим ряд важных вопросов, связанных с системами RAID, NAS и SAN.

- *RAID не является стратегией резервного копирования:* RAID можно использовать для повышения надежности, но важно понимать, что RAID не является заменой стратегии резервного копирования. В большинстве конфигураций RAID все данные теряются при поломке двух дисков. Пожары, землетрясения, наводнения и другие стихийные бедствия приведут к потере всех данных. Падение напряжения может повредить несколько дисков и даже RAID-контроллер. Ошибки поставщика в реализации и проблемы с оборудованием также вызовут полную потерю данных.

  Ваши пользователи могут и будут удалять важные файлы. Когда они будут это делать, их ошибка будет скопирована на зеркальный диск или диск про-

верки четности. В некоторых системах RAID есть возможность хранения образов файловой системы, то есть возможность просмотреть, какой была файловая система несколько дней назад. Она также не является решением по резервному копированию. Это просто усовершенствование процесса поддержки пользователей, которым требуется восстановление отдельных файлов, когда они случайно их удаляют. Если эти образы хранятся в той же системе RAID, что и остальные данные, пожар или поломка двух дисков уничтожит всю информацию.

Резервные копии на каких-нибудь других носителях, будь то магнитная лента или даже другой диск, все-таки требуются, когда у вас есть система RAID, даже если у нее имеется возможность хранения образов. Образ не поможет восстановить блок RAID после пожара в вашем информационном центре.

Считать, что приобретение системы RAID означает отсутствие необходимости соблюдать основные принципы защиты данных, – это очень распространенная ошибка. Не совершайте ее!

Зачем нужны резервные копии

Однажды Страта заказывала для клиента RAID-систему без явного указания о том, как будут выполняться резервные копии. Когда она узнала, что поставщик считал, что резервные копии были не нужны, она ужаснулась и была шокирована. Поставщик планировал в конце концов предоставить в системе поддержку устройства записи на магнитную ленту, но этого не происходило в течение года. Добавление в систему карты высокоскоростного интерфейса, чтобы хранить резервные копии отдельно от основной вычислительной сети, было приемлемым для клиента способом обойти проблему. При покупке системы хранения спрашивайте о возможностях резервного копирования и восстановления.

- *Использование зеркальных томов RAID в качестве резервных копий:* вместо того чтобы использовать зеркальные тома для постоянной защиты данных, некоторые системы **разрывают**, или отключают, зеркальные диски, получая статичную, неизменную копию данных, с которой выполняется резервное копирование. Это выполняется в координации с системами баз данных и ОС, чтобы обеспечить целостное отражение данных с точки зрения приложения. После завершения резервного копирования зеркальный том **заново подключается** и перестраивается для обеспечения защиты до начала следующего процесса резервного копирования. Преимущество заключается в том, что резервное копирование не замедляет нормальную работу с данными, так как оно затрагивает только диски, которые не используются в других целях. Недостаток состоит в том, что во время операции резервного копирования данные не защищаются, а при перестроении зеркального тома рабочая система функционирует гораздо медленнее.

  Многие системные администраторы иногда используют такие возможности отражения для создания резервной копии важного диска, например загрузочного диска сервера, в случае поломки диска, повреждения ОС, нарушения

безопасности или возникновения других проблем. Так как ошибка или нарушение будут честно отражены на другом диске, система не запускается в настоящем зеркальном режиме RAID 1. Отражение создается и затем отключается, поэтому его обновления не происходят. После того как будут выполнены и проверены изменения конфигурации, например обновления операционной системы, зеркальный том можно обновить и опять отключить, чтобы сохранить новую копию. Это лучше, чем восстанавливать данные с магнитной ленты, потому что быстрее. Кроме того, это более точно, поскольку некоторые системы резервного копирования на магнитные ленты не могут правильно восстановить загрузочные блоки и другие метаданные.

- *Использование зеркальных томов RAID для ускорения резервного копирования:* чтобы ускорить резервное копирование, можно воспользоваться блоком RAID с двумя зеркальными томами. Изначально в системе есть идентичные данные на трех наборах диска, что называется конфигурацией **тройного отражения**. Когда пора делать резервные копии, один отраженный блок отключается, снова в координации с системами баз данных и ОС, чтобы данные на нем были целостными. Теперь можно выполнять резервное копирование с отделенного зеркального блока. После завершения резервного копирования зеркальный блок снова подключается, происходит перестроение и вскоре система возвращается к своему нормальному состоянию. Перестроение не так сильно влияет на производительность рабочей системы, потому что запросы на чтение можно распределить между двумя основными зеркальными блоками.
- *NAS и резервное копирование:* в конфигурации NAS на клиентских машинах обычно не хранятся уникальные данные. Если данные хранятся там, то все сотрудники хорошо информируются, что их резервное копирование не выполняется. Это вносит простоту и прозрачность, особенно в плане резервного копирования. Понятно, где находятся все общие данные пользователей, и поэтому процесс резервного копирования упрощается.

  Кроме того, за счет размещения общих данных пользователей на сервере NAS нагрузка по резервному копированию этих данных разделяется, главным образом, между самим сервером NAS и сервером, отвечающим за резервное копирование, и поэтому изолируется от серверов приложений и серверов подразделений. При такой конфигурации клиенты становятся взаимозаменяемыми. Если ломается чей-то настольный компьютер, человек может воспользоваться любым другим.
- *SAN и резервное копирование:* как было упомянуто выше, SAN упрощает резервное копирование двумя способами. Во-первых, устройство для записи на магнитную ленту может поддерживать подключение к SAN. Таким образом, все серверы могут совместно использовать одно дорогое решение для библиотеки магнитных лент. Во-вторых, за счет наличия выделенной сети для трафика файлов резервное копирование не пересекается с нормальным трафиком сети.

  В системах SAN часто есть средства, которые создают образы LUN. За счет координации создания этих образов с базами данных и другими приложениями резервные копии можно делать автономно в течение дня, не затрагивая нормальную работу.

25.1.3.4. Мониторинг

Если за чем-то не наблюдают, это не служба. Несмотря на то что мы широко рассмотрели мониторинг в главе 22, здесь стоит рассказать о некоторых особых требованиях к мониторингу службы хранения.

Важным элементом стратегии соответствия потребностям ваших пользователей является построение точной модели ваших систем хранения. Для каждого сервера хранения вам нужно знать, сколько пространства используется, сколько доступно и сколько пользователь предполагает использовать в следующий временной период планирования. Обеспечьте мониторинг исторических данных, чтобы вы могли видеть уровень изменения использования пространства со временем, и проверяйте его регулярно. Отслеживайте трафик доступа к системам хранения, например локальные операции чтения/записи или пакеты доступа к файлам по сети, чтобы построить модель, которая позволит вам оценивать производительность. Вы можете пользоваться этой информацией для заблаговременного предотвращения проблем и планирования будущей модернизации и изменений.

Просмотр данных мониторинга по томам является наиболее распространенным и чаще всего поддерживается многими средствами мониторинга. Просмотр тех же данных по группам пользователей позволяет системным администраторам более дифференцировано подходить к каждой группе, а сотрудникам – следить за собственным использованием.

> **Сравнение пользователей**
>
> Может быть полезно позволить пользователям просматривать статистику своей группы в сравнении с другими группами. Однако в напряженной политической обстановке это может быть воспринято как попытка унизить одну группу перед другой. Никогда не пользуйтесь групповой статистикой, чтобы намеренно унизить или обвинить людей с целью изменения их поведения.

Помимо уведомлений об отключениях и сбоях системы/службы, вас нужно предупреждать о таких событиях, как заполнение хранимой информацией определенной доли доступного пространства либо пики или провалы в передаче данных или времени ответа сети. Очень полезным может быть отслеживание интенсивности использования процессора на выделенном файловом сервере, так как одним из признаков проблем со службами файлов или неуправляемости клиентов является резкий рост интенсивности использования процессора. В случае статистики по группам уведомления можно отправлять прямо затрагиваемым пользователям, которые затем смогут лучше сами разобраться со своим использованием ресурсов. Некоторые люди предпочитают, чтобы им напоминали, а не жестко удерживали квоты пространства.

За счет реализации скриптов уведомлений с различными получателями вы можете эмулировать наличие жестких и мягких квот. Например, когда том заполняется на 70%, скрипт может отправить сообщение на адрес массовой рассылки группы или подразделения для пользователей этого тома. Если том

продолжает заполняться и заполнение достигает 80%, следующее уведомление можно отправить руководителю группы для обеспечения запроса на очистку диска. Его копия может быть также отправлена в службу поддержки, чтобы администраторы компании знали, что в ближайшем будущем возможен запрос на увеличение дискового пространства.

Подводя итог, мы рекомендуем вам отслеживать следующие связанные с хранением аспекты:

- *Поломки дисков.* С избыточными системами RAID поломка одного диска не вызовет остановку работы службы, но сломанный диск должен быть быстро заменен или следующий сбой может привести к потере обслуживания.
- *Другие сбои.* Наблюдайте, например, за доступом к каждому сетевому интерфейсу NAS.
- *Используемое/свободное пространство.* Это наиболее часто задаваемый пользователями вопрос. Предоставляя эту информацию пользователям по запросу на внутреннем веб-сервере, вы освободите множество заявок в службе поддержки.
- *Темпы изменений.* Эти данные особенно полезны в прогнозировании будущих потребностей. Подсчитывая темпы изменений использования пространства в типичный период интенсивной нагрузки, например во время квартального выпуска продукции или первого семестра нового учебного года, вы можете постепенно прийти к показателям, которые позволят вам прогнозировать потребности в пространстве с определенным уровнем достоверности.
- *Локальное использование ввода/вывода.* Мониторинг этого значения позволит вам увидеть, когда конкретное устройство хранения или массив начинает полностью заполняться. Если происходят сбои, сопоставление времени со статистикой ввода/вывода может быть бесценным в отслеживании проблемы.
- *Локальный сетевой интерфейс.* Если решение по хранению начинает медленно отвечать, сопоставление его локальных показателей ввода/вывода с показателями сетевого интерфейса и используемой пропускной способности сети предоставляет признаки того, где может быть сбой.
- *Использование пропускной способности сети.* Сопоставление общей сетевой статистики с показателями локального интерфейса, например фрагментацией и обратной сборкой, может предоставить полезные указания для оптимизации производительности. Обычно полезно отслеживать именно сети между серверами и системами хранения и обобщать данные таким образом, чтобы их можно было легко просмотреть вне области основной сетевой статистики.
- *Операции с файлами.* Работа службы хранения через такие протоколы, как NFS или CIFS, также требует отслеживание статистики уровня службы, например операций NFS *badcall*.
- *Недостаточное использование.* Если популярная файловая система в последнее время не выполняет никаких операций с файлами, это часто является признаком какой-либо другой проблемы, например сбоя между файловым сервером и клиентами.
- *Использование отдельных ресурсов.* Этот аспект может быть очень полезным или очень опасным, в зависимости от культуры вашей организации.

Если группы пользователей сами управляют своими ресурсами, он является практически обязательным. Во-первых, они уделяют очень большое внимание данным, поэтому в какой-то мере это проявление уважения к их приоритетам. Во-вторых, они в любом случае будут пытаться независимо генерировать данные, что загружает машины. В-третьих, будет одной причиной меньше предоставлять привилегии `root` не системным администраторам. Использование `root` для получения информации об использовании диска – это распространенное оправдание, почему инженерам и руководителям групп «нужен» `root`-доступ к общим серверам.

25.1.3.5. Предостережения о SAN

Так как технологии SAN постоянно меняются, может быть трудно заставить компоненты различных производителей работать вместе. Мы рекомендуем ограничиться одним-двумя производителями и тщательно тестировать свои решения. Когда производители предлагают вам посмотреть свои новейшие и лучшие продукты, отказывайтесь. Говорите таким производителям, что вы хотите видеть только продукцию, которая уже реально работала какое-то время. Пусть другие люди справляются с ошибками в новых продуктах[1]. Это ваши данные, наиболее ценный актив вашей компании, а не игрушки.

Ограничившись небольшим количеством производителей, вы сможете лучше наладить связи. У сотрудников по продажам и инженеров будет бóльшая мотивация поддерживать вас как постоянного клиента.

С другой стороны, лучше всего подвергать новые модели тщательному тестированию, прежде чем интегрировать их в свою инфраструктуру, даже если они от того же производителя. Производители приобретают сторонние технологии, изменяют подсистемы реализации и делают то же самое, что и любые другие производители. Обычно задача производителя – усовершенствовать возможности своих продуктов, но иногда новые возможности не считаются улучшением такими людьми, как мы.

Создайте набор тестов, которые вы считаете важными для вашей среды. Типичный набор тестов может включать стандартные для отрасли тесты, тесты конкретных приложений, полученные от их разработчиков, и попытки выполнить особо специфичные для компании операции, а также подобные операции при гораздо более высокой нагрузке.

25.1.4. Быстродействие

Под быстродействием понимается время, которое требуется вашим пользователям для чтения и записи данных. Если служба хранения, которую вы предоставляете, слишком медленная, ваши пользователи найдут способ обойти ее, например, подключая дополнительные диски к своим компьютерам или жалуясь руководству.

Самое важное правило оптимизации – сначала измерить, потом оптимизировать на основе полученных данных, а затем измерить снова. Часто мы видим, как системные администраторы выполняют оптимизацию на основе догадок о том,

[1] Этот ценный совет появился в программной презентации на LISA 2003 Пола Килмартина (Paul Kilmartin), директора по доступности и управлению производительностью в eBay.

что замедляет систему. Измерение означает применение средств операционной системы для сбора данных, например, о том, какие диски используются наиболее интенсивно или какова сравнительная доля обращений для чтения и для записи. Некоторые системные администраторы ничего не измеряют, а просто применяют различные подходы, пока не находят тот, который решит проблему с быстродействием. Эти системные администраторы зря тратят много времени на решения, которые не приносят результатов. Мы называем этот подход **слепым гаданием** и не рекомендуем им пользоваться. Смотреть на световые индикаторы обращения к дискам во время пиковых периодов нагрузки – это лучше, чем не измерять вообще ничего.

Основные средства, которые есть у системного администратора для оптимизации производительности, – это оперативная память и шпиндели. Оперативная память быстрее, чем диск. С большим количеством оперативной памяти можно больше кэшировать и меньше обращаться к диску. С большим количеством шпинделей (независимых дисков) нагрузку можно распределить по большему числу параллельно работающих дисков.

Общие правила быстродействия

1. Никогда не обращайтесь к сети, если вы можете оставаться на диске.
2. Никогда не обращайтесь к диску, если вы можете оставаться в памяти.
3. Никогда не обращайтесь к памяти, если вы можете оставаться на чипе.
4. Имейте достаточно денег и не бойтесь их тратить.

25.1.4.1. RAID и быстродействие

RAID 0 предоставляет большее быстродействие как чтения, так и записи, потому что чтение и запись распределяются по нескольким дискам, которые могут выполнять несколько операций одновременно. Однако, как мы видели, это повышение быстродействия достигается ценой надежности. Так как поломка любого диска выводит из строя весь блок RAID 0, большее количество дисков означает большую вероятность сбоя.

RAID 1 может предоставить большее быстродействие чтения, если операции чтения распределяются по обоим или по всем дискам. Скорость записи определяется быстродействием самого медленного диска в зеркальном блоке RAID.

RAID 3, как мы говорили, предоставляет особенно хорошее быстродействие при последовательном чтении. RAID 3 рекомендуется для хранения больших графических файлов, потоковых данных и видеоприложений, особенно если файлы обычно архивируются и не изменяются часто.

RAID 4 – с настроенной файловой системой – и RAID 5 обеспечивают высокую скорость чтения, но скорость записи хуже. Скорость чтения повышается за счет того, что диски могут параллельно выполнять чтение. Однако при крупной записи на блок RAID скорость чтения снижается, потому что все диски вовлечены в операцию записи. На диск контроля четности всегда осуществляется запись, помимо диска, на котором размещаются данные, а прежде чем будет выполнена запись на диск контроля четности, нужно прочитать данные со всех

остальных дисков. Запись не завершается, пока не будет также выполнена запись на диск контроля четности.

RAID 10 обеспечивает высокую скорость чтения и записи, как и RAID 0, но без недостатка надежности, от которого страдает последний. На самом деле скорость записи повышается еще сильнее, потому что зеркальные диски также могут удовлетворять запросы на чтение. Скорость записи будет определяться самым медленным зеркальным диском, на который нужно будет записать данные, так как системе не сообщается о завершении записи, пока обе или все зеркальные копии не будут успешно записаны.

25.1.4.2. NAS и быстродействие

Системы хранения, основанные на NAS, позволяют системным администраторам изолировать нагрузку по передаче файлов от остальных серверов, и системным администраторам становится проще объединить все пользовательские данные на небольшом количестве крупных серверов, чем распространять их по всей сети. Кроме того, упрощается последовательное применение к файловым серверам политик резервного копирования, использования и безопасности.

Многие компании развивают свои инфраструктуры в какой-то мере органически, со временем. Очень часто можно увидеть серверы, совместно используемые подразделением или конкретной группой пользователей, на которых как выполняются расчеты, так и хранятся файлы. Перемещение размещения файлов в блок NAS может значительно снизить загрузку сервера, повышая для пользователей быстродействие. Затраты по передаче файлов не будут устранены полностью, потому что теперь серверу для доступа к системе хранения NAS нужно будет запустить клиентский протокол. Однако в большинстве случаев есть явные преимущества.

25.1.4.3. SAN и быстродействие

SAN выигрывают от возможности убрать трафик файлов из основной сети. Сеть может быть настроена для особых нужд передачи файлов: низкой задержки и высокой скорости. SAN изолируется от других сетей, что предоставляет ей преимущество в безопасности.

Компании создавали свои версии SAN задолго до того, как кто-то решил так их называть, используя по нескольку волоконно-оптических интерфейсов на ключевых файловых серверах и направляя весь трафик через высокоскоростные интерфейсы, выделенные для систем хранения. Кристина и Страта вместе работали в компании, которая одной из первых начала применять эту концепцию. Конфигурацию серверов нужно было выполнять вручную, требовалось немного искусства в картах автоматического монтирования и записях локального узла и DNS, но быстродействие того стоило.

SAN были так удобны, что люди начали рассматривать другие способы, при помощи которых можно объединить в сеть устройства хранения. Один из таких способов – относиться к другим сетям, как если бы они были подключены напрямую. Каждая SCSI-команда инкапсулируется в пакет и отправляется по сети. Стандарт fibre channel (FC) позволяет делать это при помощи медных или волоконно-оптических сетей. Оптоволоконный канал становится расширенной SCSI-шиной, и устройства, подключенные к нему, должны соблюдать обычные правила протокола SCSI. Успех fibre channel и доступность дешевого и быстро-

го сетевого оборудования TCP/IP привели к созданию **iSCSI**, отправляющего практически такой же пакет по IP-сети. Это позволяет устройствам SCSI, например библиотекам магнитных лент, напрямую становиться элементом SAN. ATA через Ethernet (AoE) предоставляет нечто подобное для ATA-дисков.

С развитием высокоскоростных сетей и расширением доступности оборудования инкапсуляция протоколов, требующая сети с небольшим временем реакции, теперь во многом стала реальной. Мы предполагаем, что использование многоуровневых протоколов доступа к сетевым системам хранения вместе со многими другими типами протоколов в будущем увеличится.

Так как SAN – это просто сеть устройств хранения, они не ограничены одним объектом или информационным центром. При помощи высокоскоростных сетевых технологий, таких как ATM и SONET, SAN может быть «локальной» для нескольких информационных центрах в различных местах.

25.1.4.4. Оптимизация конвейерной обработки данных

Важный элемент понимания быстродействия развитых массивов хранения – разобраться, как они работают с **конвейерной обработкой данных**. Термин означает предварительную загрузку в память объектов, которые могут понадобиться в дальнейшем, при этом время доступа минимизируется. В процессорах, в которых есть **кэш второго уровня**, имеется дополнительная память для предварительной загрузки данных и команд, вот почему в некоторых задачах с большой нагрузкой на процессор Pentium III с большим кэшем второго уровня может превзойти Pentium IV при прочих равных условиях.

Алгоритмы конвейерной обработки широко используются во многих компонентах современных устройств хранения, особенно в HBA, а также в контроллерах дисков. Эти алгоритмы могут быть «*глупыми*» или «*умными*». При так называемом «глупом» алгоритме контроллер просто считывает блоки, расположенные физически рядом с требуемыми блоками, предполагая, что они будут следующим набором блоков, требуемым по этому запросу. Обычно это хорошее предположение, если диск не сильно фрагментирован. «Умный» алгоритм конвейерной обработки может осуществлять доступ к информации файловой системы и предварительно считывать блоки, которые составляют следующую часть файла, вне зависимости от того, находятся они рядом или нет. Имейте в виду, что для некоторых систем хранения «рядом» может означать не *физически рядом* с другими блоками на диске, а *логически рядом* с ними. Например, блоки в одном и том же цилиндре находятся рядом не физически, но логически.

Хотя комбинация кэширования на уровне операционной системы и конвейерной обработки очень полезна при чтении данных, запись данных является более сложным процессом. Операционные системы обычно создаются так, чтобы обеспечить **атомарную** запись или, по крайней мере, приблизиться к ней, насколько это позволяют ограничения оборудования. В данном случае «атомарный» означает «одним блоком». Атомы получили свое название до того, как люди узнали, что есть такие объекты, как субатомная физика, с протонами, электронами, нейтронами и т. п. Люди считали атом наименьшим элементом материи, который нельзя было разделить.

Эта аналогия может показаться странной, но на самом деле она довольно справедлива. Как атомы состоят из протонов, нейтронов и электронов, так и одна операция записи может включать множество этапов. Важно, что операционная

система не считает операцию записи завершенной, пока не будут выполнены все этапы. Это означает ожидание от физического оборудования подтверждения (ACK – acknowledgement), что запись была выполнена.

Один из способов оптимизации – подтверждать запись немедленно, даже если данные не были надежно записаны на диск. Это рискованно, но есть несколько способов повысить безопасность. Один из них – выполнять это только для блоков данных, а не для информации о директории и других блоков, которые могут нарушить файловую систему (мы не рекомендуем так поступать, но в некоторых системах есть такая возможность). Другой способ – хранить данные в оперативной памяти, которая при помощи батарейки может сохраняться при перезагрузке. Тогда подтверждение может быть отправлено сразу после того, как данные будут надежно записаны в этой оперативной памяти. В данном случае важно, чтобы ожидающие блоки записывались прежде, чем будет убрана оперативная память. Том перенес такое устройство в другой компьютер, не зная, что в нем было много данных, ожидающих записи. Как только новый компьютер загрузился, эти данные записались на ничего не подозревающий диск новой системы, который был серьезно поврежден. Другой тип сбоя может затронуть само оборудование. Необнаруженная севшая батарея при следующей перезагрузке может привести к катастрофе.

Трижды выполняйте sync перед halt

Самые первые версии UNIX не синхронизировали буферы записи с дисками автоматически перед остановкой системы. Операторы были обучены отключать от системы всех пользователей для исключения любых действий по записи, затем трижды вручную вводили команду `sync` перед вводом команды `shutdown`. Команда `sync` гарантирует только установку времени записи незаписанных блоков, возможна небольшая задержка, прежде чем все блоки наконец будут записаны на диск. Вторая и третья команды `sync` не требовались, но выполнялись, чтобы перед завершением работы системы прошло время. Если вы быстро печатаете, вы можете просто специально подождать.

25.1.5. Оценка новых решений по хранению

Будет ли конкретное решение по хранению иметь смысл для вашей организации – зависит от того, как вы планируете им пользоваться. Изучите свою модель использования, чтобы принять разумное, информированное решение. Рассмотрите пропускную способность и конфигурацию различных подсистем или компонентов предлагаемого решения.

Особенно внимательно ищите скрытые «подводные камни». Некоторые решения, кажущиеся доступными по цене, становятся такими благодаря использованию ресурсов памяти и процессора вашего сервера для выполнения значительной части работы. Если сервер вашего небольшого офиса или рабочей группы используется как для приложений, так и для подключения систем хранения, очевидно, что решение такого типа, скорее всего, будет неудовлетворительным.

Тестируйте все элементы новой системы

Ранние решения по хранению данных на основе SATA приобрели плохую репутацию, потому что они неосторожно использовались и устанавливались. Был прецедент с профессиональной рассылкой, когда популярный контроллер, используемый в массивах SATA, отправлял искаженные предупреждения по электронной почте, которые тихо удалялись системой электронной почты. Если бы администратор компании не проверил систему уведомления, проблема не была бы обнаружена, пока массив не дошел бы до момента потери данных.

Другая распространенная проблема – когда вы обнаруживаете, что в системе с привлекательной ценой используются очень медленные диски, а производитель не гарантирует определенной скорости дисков. Довольно часто небольшие компании собирают свои продукты из того, что у них есть, а затем предоставляют вам неожиданную скидку за счет менее желательного оборудования. По меньшей цене вы получаете менее полезную систему.

Хотя производитель может утверждать, что большинству пользователей все равно, это не ваша проблема. Настаивайте на определенных стандартах компонентов и проверяйте систему, прежде чем принять ее доставку. Вероятность совершения ошибок возрастает при использовании нестандартных частей, затрудняющих производителям процесс сборки на своей территории. Будьте вежливы, но настойчивы в получении того, что вы заказали.

25.1.6. Распространенные проблемы

В современных системах хранения применяется комбинация многоуровневых подсистем и оптимизации на каждом уровне для предоставления быстрого, эффективного хранения, обычно не требующего большой работы по обслуживанию. Здесь мы рассмотрим распространенные варианты того, как решения по хранению могут превратиться в проблемы хранения.

Многие уровни в цепочке от пластины диска до операционной системы и клиента реализованы с предположением о том, что следующий вызываемый уровень поступит правильно и каким-то образом восстановится после ошибки, снова запросив данные.

Наиболее распространенный общий тип проблем заключается в том, что некоторые граничные условия были упущены. Цепная реакция сбоев обычно начинается в нормальном взаимодействии между уровнями, но иногда, как в случае с проблемами питания или температуры, на аппаратном уровне.

25.1.6.1. Физическая инфраструктура

В современных системах хранения значительное количество оборудования часто размещается в сравнительно небольшом пространстве. Многие серверные и информационные центры были спроектированы в расчете на более старые компьютерные системы, которые занимали больше физического пространства. Когда то же самое пространство заполняется несколькими стойками систем хранения, требования по электропитанию и охлаждению будут

гораздо выше, чем по проекту серверной. Мы сталкивались с несколькими таинственными ошибками, полностью обусловленными проблемами с питанием и температурой.

Если вы сталкиваетесь с непонятными ошибками, связанными с повреждением массивов или нарушением структуры данных, может иметь смысл проверить стабильность инфраструктуры питания соответствующей машины. Мы рекомендуем включить контроль питания в мониторинг ваших систем хранения хотя бы по этой причине. Однажды мы обнаружили, что нестабильный блок NAS стал надежным, когда его переместили в стойку, где он мог получать достаточное питание (фактически большее, чем для него было указано), – и это стало для нас одновременно раздражением и облегчением.

Для оценки требований систем хранения может быть полезен индикатор потребляемой мощности, отображающий реальное потребление питания. При запуске диски часто потребляют больше мощности, чем при работе. Десяток дисков, запускаемых одновременно, может забрать достаточную мощность с общего распределительного устройства, чтобы вызвать непонятные сбои другого оборудования.

25.1.6.2. Превышение времени ожидания

Превышение времени ожидания может быть характерной проблемой, особенно в сильно оптимизированных системах, которые реализованы главным образом для скорости, а не для надежности. Решения NAS и SAN могут быть особенно чувствительны к изменениям в конфигурации сетей, от которых они зависят.

При реализации и тестировании может показаться, что изменение в конфигурации сети, например изменение топологии сети, которое теперь вводит дополнительный переход между маршрутизаторами по пути к системе хранения, ни на что не повлияло. Однако при сильной нагрузке эта небольшая задержка может быть достаточной, чтобы вызвать превышение времени ожидания TCP в сетевом соединении устройства NAS.

Иногда превышение времени ожидания возможно на стороне клиента. Когда файловая система с протоколированием работала по сети с сильно загруженного общего сервера, Страта видела, как консервативному NFS-клиенту не удавалось выполнить запись, потому что в сетевом соединении было превышено время ожидания, пока файловая система внесет эту запись в журнал. Когда приложение на стороне клиента снова запрашивало файл, полученный файл не соответствовал запросу и в клиентском приложении происходил сбой.

25.1.6.3. Поведение при перегрузке

Перегрузка пути передачи данных в любой точке цепи часто является виновником таинственных задержек, которые исчезают сами собой, и периодических медленных ответов, даже вызывающих рассмотренное выше превышение времени ожидания. При планировании пропускной способности постарайтесь не перепутать теоретический потенциал системы хранения с возможной скоростью использования.

Распространенная проблема, особенно с дешевыми и/или плохо установленными устройствами хранения, заключается в том, что скорость самого быстрого компонента путают со скоростью устройства. Некоторые производители могут случайно или намеренно содействовать этой путанице.

Можно назвать следующие примеры таких показателей, но они являются лишь частью более крупной картины:

- Кратковременная скорость ввода/вывода дисков или длительно поддерживаемые скорости ввода/вывода – большинство приложений редко осуществляют кратковременный доступ.
- Скорость шины основного блока.
- Скорость общей системной платы.
- Скорость контроллера и/или HBA.
- Скорость кэширования в памяти или конвейерной обработки.
- Скорость сети.

В ваших планах по расширению должны учитываться все эти элементы. Единственно надежные значения, на которых можно основывать ожидания по быстродействию, – это те, которые получены при тестировании устройства хранения при реалистичной нагрузке.

В системе хранения, которая работает в режиме, близком к насыщению, больше вероятность столкнуться с незапланированным взаимодействием между задержанными подтверждениями, реализованными на различных уровнях аппаратного и программного обеспечения. Так как на нескольких уровнях внутри уровня может выполняться кэширование, буферизация и конвейерная обработка, перегрузка повышает вероятность возникновения граничных условий, в том числе переполнения буферов и обновления кэша до того, как их содержимое будет записано. Как было рассмотрено ранее, разработчики обычно полагаются на то, что таких граничных условий не возникнет, обработка таких событий обычно зависит от конкретной реализации управляющего программного обеспечения производителя.

25.2. Тонкости

Теперь, когда мы рассмотрели хранение как управляемую службу и все требования, которые возникают в связи с этим, давайте поговорим о способах взять вашу надежную, высокопроизводительную и снабженную резервными копиями службу хранения и сделать ее лучше.

25.2.1. Оптимизация использования RAID по приложениям

Так как различные уровни RAID предоставляют разное быстродействие и надежность, системы RAID могут быть настроены для конкретных приложений. В этом разделе мы рассмотрим примеры для различных приложений.

Так как распределение данных в большинстве современных систем RAID осуществляется на уровне блоков, есть значительные преимущества в быстродействии при выравнивании размера блока распределяемых данных с размером блока данных, используемым в вашем приложении. Хранение баз данных – это наиболее распространенная область применения упомянутого принципа, но он также может использоваться для серверов приложений, например веб-серверов, которые проводят по сети данные с четко определенным максимальным размером пакета.

25.2.1.1. Настройка распределения данных

Для базы данных, которой требуется выделенный раздел, например Oracle, изменение размера блока, используемого базой данных, до размера блока распределения данных при хранении или наоборот может обеспечить очень заметное повышение быстродействия. Принимайте во внимание операции контроля четности уровня блока, а также размер массива. Приложению, использующему блоки размером 32 Кб, обслуживаемому массивом из пяти дисков RAID 5, будет хорошо соответствовать размер блока распределения в 8 Кб: четыре диска с данными плюс один диск контроля четности (4×8 Кб $= 32$ Кб). При использовании большего количества независимых дисков можно достичь повышенного быстродействия, например при массиве из девяти дисков по 4 Кб. Не всем приложениям потребуется такой уровень настройки, но полезно знать, что такие приемы существуют.

Такой тип настройки – подходящая причина не разделять системы хранения между различающимися приложениями, когда быстродействие является критически важным. В приложениях часто есть шаблоны доступа и предпочтительные размеры блоков, которые заметно различаются. Чтобы этот прием был эффективен, размер блока должен поддерживаться всем путем ввода/вывода. Если в вашей операционной системе используются, например, блоки по 4 Кб для создания страниц, установка размера блока распределения в RAID в 8 Кб может вызвать сбой страницы на каждой операции ввода/вывода, и быстродействие будет ужасным.

25.2.1.2. Упорядочение записи

Некоторые приложения используют для своих стандартных операций несколько операций записи в независимые потоки данных, взаимодействие двух потоков вызывает проблемы быстродействия. Мы видели много приложений, у которых были проблемы с быстродействием, вызванные тем, что другой процесс записывал большое количество информации в файл лога. Оба процесса сильно загружали один и тот же диск. После перемещения файла лога на другой диск система заработала гораздо быстрее. Похожие проблемы с подобными решениями происходят с базами данных, ведущими лог транзакций, процессами по сборке больших программ, которые пишут большие выходные файлы, и файловыми системами с протоколированием, которые ведут свой лог транзакций. Во всех этих случаях перемещение интенсивно записываемого участка на другой диск повышает быстродействие.

Иногда потоки записи могут производиться на диски различного качества. В примере с компиляцией выходной файл можно легко воспроизвести, поэтому выходным диском может быть RAM- или быстрый локальный диск.

В случае базы данных индексы, или виды, отдельных таблиц обычно обновляются часто, но не могут быть легко воспроизведены. Они требуют большого объема пространства, так как являются просто зафиксированными копиями информации в таблицах базы данных. Имеет смысл разместить данные таблиц на надежный, но более медленный RAID-массив, а данные об индексах и видах – на быстрый, но необязательно надежный зеркальный массив. Если быстрый массив далее разделяется на отдельные разделы видов или индексов, а в физический массив включаются запасные диски, даже потеря диска может привести к минимальному времени простоя с быстрым восстановлением, так как воссоздать и перезаписать потребуется только часть динамических данных.

25.2.2. Пределы хранения: отставание плотности доступа к диску

Плотность современных дисков поразительна. В месте, которое когда-то занимал диск MicroVAX на 500 Мб, теперь можно разместить несколько терабайтов. Однако быстродействие не растет так быстро.

Развитие технологии изготовления поверхности ежегодно увеличивает размер жестких дисков на 40–60%. Однако быстродействие дисков растет только на 10–20%. Разрыв между тем, сколько информации может вмещать диск, и тем, насколько быстро вы можете получать данные с диска и записывать их на него, растет. Это отставание называется **плотностью доступа к диску** (DAD – Disk Access Density) и измеряется в операциях ввода/вывода в секунду на гигабайт емкости (операций/с/Гб).

На рынке, где важно соотношение цены и производительности, многие покупатели дисков ошибочно принимают чистую емкость за производительность, совершенно игнорируя DAD. DAD важна при выборе систем хранения для конкретного приложения. Диски очень высокой емкости прекрасно подходят для ресурсов с относительно низкими потребностями. Приложениям с высокой интенсивностью ввода/вывода, особенно в плане записи, требуется лучшее соотношение DAD.

Когда вы будете планировать свою инфраструктуру хранения, вы обнаружите, что вам потребуется выделять серверы хранения конкретным приложениям, чтобы обеспечить оптимальную производительность. Может быть заманчиво купить самый большой жесткий диск на рынке, но два диска меньшего размера обеспечат лучшее быстродействие. Это особенно разочаровывает, если принять во внимание, какие потребуются дополнительное питание, место в корпусе и охлаждение.

Часто обновляемая база данных может быть структурирована таким образом, чтобы самые активно используемые таблицы размещались в разделе системы хранения, состоящем из нескольких меньших по размеру, но более производительных дисков. Файловые системы инженерных подразделений, которые работают главным образом с компиляцией, но имеют также большие модели данных, например, в фирме по разработке чипов, могут потребовать продуманной интеграции с другими элементами инфраструктуры.

При поддержке пользователей, которым нужны как интенсивный ввод/вывод, так и хранение больших объемов данных, вам придется тщательно изучить производительность своей файловой системы и разумно выполнять требования.

25.2.2.1. Фрагментация

Перемещение головки диска на новое место происходит очень медленно по сравнению с чтением данных с дорожки, на которой находится головка. Таким образом, операционные системы прилагают значительные усилия к записи всех блоков данного файла на одной дорожке диска. Так как большинство файлов читается последовательно, это может обеспечить быструю передачу данных с диска.

Однако по мере заполнения диска становится трудно найти группы смежных блоков для записи файлов. Файловые системы становятся фрагментированными. Раньше системные администраторы тратили много времени на дефрагмен-

тацию дисков, запуская программы, которые перемещали файлы, открывая промежутки свободного пространства и перенося большие фрагментированные файлы во вновь созданное смежное пространство.

Это нецелесообразно в современных операционных системах. Современным системам гораздо лучше удается не создавать фрагментированные файлы с самого начала. Быстродействие жестких дисков гораздо слабее затрагивается случайными фрагментами. Дефрагментация диска подвергает его значительному риску из-за потенциальных ошибок в программах и проблем, которые могут быть вызваны отключением питания при перезаписи важных данных.

Мы сомневаемся в справедливости утверждений разработчиков о сильном росте быстродействия за счет использования их программ дефрагментации. Риск уничтожения данных слишком велик. Как было сказано ранее, это важные данные, а не игрушки.

Фрагментация является спорным вопросом в многопользовательских системах. Представьте себе сервер NFS или CIFS. Если один пользователь последовательно запрашивает блок за блоком одного и того же файла, фрагментация может немного влиять на получаемое быстродействие, но сетевые задержки и другие факторы будут влиять гораздо больше. Более типичной нагрузкой будут десятки или сотни одновременно работающих клиентов. Так как каждый клиент запрашивает свои блоки, поток запросов перемещает головку диска над всем диском, чтобы собрать требуемые блоки. Если диск сильно фрагментирован или совсем не фрагментирован, количество движений будет примерно одинаковым. Операционные системы оптимизируют эту ситуацию, выполняя запросы по номеру дорожки, а не по порядку их получения. Так как операционные системы уже оптимизированы для этого случая, дополнительный риск, связанный с передачей данных для дефрагментации, не является необходимым.

25.2.3. Непрерывная защита данных

Непрерывная защита данных (CDP – Continuous Data Protection) – это процесс копирования изменения данных в определенный временной промежуток в одно или более вторичных средств хранения. То есть, записывая все изменения, внесенные в том, можно перемещаться вперед и назад во времени, повторяя и отменяя изменения. В случае потери данных можно восстановить последнюю резервную копию, а затем воспроизвести лог CDP до желаемого момента. Лог CDP может быть записан на другой машине, возможно, даже в другом здании.

Все чаще CDP используется в контексте не защиты данных, а защиты обслуживания. Защита данных – ключевой элемент CDP, но многие реализации также включают несколько серверов, на которых работают приложения, привязанные к защищаемым данным.

Любое решение CDP – это как процесс, так и продукт. Предложения разработчиков обычно состоят из программы управления, часто устанавливаемой с помощью их профессионального отдела обслуживания для автоматизации процесса. Несколько крупных производителей оборудования предоставляют решения CDP, которые включают их собственное оборудование и программное обеспечение с модулями от других производителей для обеспечения решений CDP конкретного производителя, поддерживающих приложения третьих сторон, например обработку транзакций баз данных.

CDP часто используется для минимизации времени восстановления и снижения вероятности потери данных. Обычно CDP довольно дорога при надежной реализации, поэтому компании обычно требуют весомых аргументов в ее пользу. Есть две основные причины, по которым компании реализуют CDP. Одна из них – обеспечить соблюдение норм отрасли. Другая – предотвратить потерю прибыли и/или выполнение обязательств, вызванное сбоями.

CDP – новое и дорогое средство и поэтому обычно используется только для решения проблем, которые нельзя решить по-другому. Одна из сфер применения CDP – это системы, где данные являются особенно важными, например финансовая информация. Другая – где изменения данных происходят очень часто. Если потеря некоторого количества данных за несколько часов означает триллионы обновлений, применение CDP может быть вполне оправданным.

25.3. Заключение

В данной главе мы рассмотрели самые распространенные типы систем хранения, а также преимущества и подходящие приложения, связанные с ними. Основные принципы управления хранением остаются неизменными: реализуйте свое решение по хранению в соответствии с нуждами приложений или пользователей и постройте несколько уровней избыточности, на каждом уровне жертвуя минимально возможным быстродействием.

Несмотря на то что диски дешевеют, управление ими становится дороже. Отношение к хранению как к службе позволяет вам установить точку отсчета при определении расходов на создание системы хранения данных и согласовать с вашими пользователями стандарты. Чтобы это сделать, у вас должны быть группы пользователей, с которыми вы будете обсуждать упомянутые стандарты, и, как с любой службой, выполняйте мониторинг для обеспечения высокого уровня качества обслуживания.

Возможности по предоставлению пользователям услуг по хранению данных значительно выросли – вы можете выбирать уровень надежности и быстродействия, необходимый для конкретных приложений. Понимание основных принципов связи устройств хранения с операционной системой и файловой системой поможет вам при выборе способов, позволяющих построить крупные решения по хранению из меньших по размеру подсистем.

Для построения решений по хранению, которые для сервера выглядят как простой, напрямую подключенный диск, но свойства которых можно сильно изменять для оптимизации под потребности приложений пользователей, можно использовать такие концепции, как RAID.

Мы также рассмотрели серьезную нерешенную проблему неравномерности роста плотности диска и пропускной способности ввода/вывода диска, которая в ближайшие годы будет становиться все более важной.

Задания

1. Какие типы систем хранения вы встречали в своей жизни. Сколько из них казались многообещающими при представлении? Сохранились ли у вас до сих пор какие-нибудь системы дома?

2. Рассмотрите текущие цены на системы хранения. Каковы возможности самой дешевой системы хранения по сравнению с самой дорогой? Какие ценовые категории вы видите для различных возможностей?
3. Как бы вы охарактеризовали основные системы хранения своей организации на основе классификации, введенной нами в данной главе? Считаете ли вы, что нынешняя система хранения хорошо удовлетворяет ваши потребности, или другой тип был бы удобнее?
4. Есть ли у вас список распространенных типов потоков данных в системах хранения вашей организации? Каково соотношение чтения и записи?
5. В RAID 1 и выше применяется несколько дисков для повышения надежности. Восемь дисков – это восьмикратное повышение вероятности возникновения одного сбоя в заданный период времени. Если в блоке RAID 5 есть восемь дисков, компенсируют ли эти два фактора друг друга? Почему?
6. Жесткий диск в десять раз быстрее оперативной памяти. Представьте, что у вас есть большая база данных, которой требуется доступ со скоростью оперативной памяти. Сколько независимых дисков потребуется, чтобы 1000 запросов в секунду выполнялись так же быстро, как при хранении всей базы данных в оперативной памяти? (Предположим, что оперативная память будет на нескольких компьютерах, каждый из которых может параллельно обрабатывать некоторое количество запросов.) Рассмотрите текущие цены на диски и оперативную память и подсчитайте, что было бы дешевле, если бы размер базы данных составлял 10 Гб, 1 Тб и 100 Тб.
7. Какие из правил быстродействия в одноименной врезке затрагиваются при применении в системах хранения HBA? Аргументируйте свой ответ.
8. Отслеживаете ли вы показатели быстродействия диска? Если бы вам нужно было улучшить производительность вашего локального решения по хранению, где бы вы могли внести изменения, не разрушая все и не начиная с самого начала?
9. Какие характеристики RAID потребовались бы вам для массива, поддерживающего сбор данных в реальном времени с датчиков показателей окружающей среды или мониторинга на заводе, и почему?
10. Обеспечено ли оптимальное использование служб хранения в вашей организации? Какие изменения вы бы внесли для усовершенствования среды хранения?

Глава 26

Резервное копирование и восстановление

Все ненавидят резервные копии. Они неудобные. Они дорогие. Службы работают медленнее – или не работают совсем, – когда выполняется резервное копирование серверов. С другой стороны, пользователи *любят* восстановления. Восстановление данных является причиной, по которой системные администраторы выполняют резервное копирование.

Возможность восстановить потерянные данные – критический элемент любой системы. Данные теряются. Оборудование ломается. Люди удаляют файлы по ошибке и умышленно. Судьи конфискуют все связанные с делом документы, которые хранились на вашем компьютере. Акционеры требуют спокойствия, обусловленного уверенностью в том, что природная или другая катастрофа не сделает их вложения бесполезными. Кроме того, данные повреждаются по ошибке, умышленно или гамма-лучами из космоса. Резервное копирование аналогично страховке: вы платите за него, хотя и надеетесь, что оно никогда вам не понадобится. На самом деле оно вам нужно.

Несмотря на то что задача заключается в возможности оперативно восстановить потерянные данные, легко погрузиться в ежедневную работу по резервному копированию и забыть, что основной целью является восстановление. Этот факт подтверждается даже общим названием, которое используется для всего оборудования и программного обеспечения, связанного с этим процессом, – «система резервного копирования». На самом деле его нужно назвать «системы резервного копирования и восстановления» или, что является более подходящим, просто «система восстановления данных».

В этой книге представлен другой подход к резервному копированию и восстановлению. Читатели этой книги уже должны знать, какие команды используются в их ОС для резервного копирования и восстановления данных. Мы не будем обсуждать данные вопросы. Вместо этого мы рассмотрим теорию планирования резервного копирования и восстановления так, чтобы это было удобно вне зависимости от имеющихся в наличии продуктов по резервному копированию.

После рассмотрения теории планирования резервного копирования и восстановления мы обратим внимание на три ключевых компонента современных систем резервного копирования: автоматизацию, централизацию и управление запасами. Эти три аспекта должны помочь в принятии вами решения о покупке. После обсуждения основных принципов мы рассмотрим, как в дальнейшем эффективно поддерживать систему, которую вы создали.

Тема резервного копирования и восстановления такая широкая, что мы не можем подробно рассмотреть ее целиком. Мы предпочли охватить ключевые

компоненты. В таких книгах, как *«UNIX Backup and Recovery»* Престона (Preston 1999) и *«Windows NT Backup and Restore»* Либера (Leber 1999), очень подробно рассмотрены детали для систем UNIX и Майкрософт.

Служба резервного копирования и восстановления является элементом любой системы хранения данных. Одно исследование обнаружило, что цена покупки диска составляет примерно 20% от общих затрат, причем практически все остальные расходы идут на резервное копирование. Легко купить чистый диск и включить его в систему. Трудно обеспечить хранение данных как полноценную службу. Цены на диски падают, но общие затраты выросли, главным образом, из-за увеличения стоимости резервного копирования. Следовательно, эффективная система резервного копирования и восстановления – ваш ключ к экономически выгодному хранению данных.

Что касается терминологии, то мы используем термин **полное резервное копирование** для обозначения полного копирования всех файлов раздела; пользователи UNIX называют это «резервным копированием уровня 0». Термин **инкрементальное резервное копирование** означает копирование всех файлов, которые изменились с предыдущего резервного копирования; пользователи UNIX называют это «резервным копированием уровня 1». Инкрементальные резервные копии со временем растут. То есть, если полное резервное копирование выполняется в воскресенье, а инкрементальное – в каждый следующий день недели, количество данных, для которых выполняется резервное копирование, должно расти каждый день, потому что инкрементальное резервное копирование во вторник включает все файлы из резервной копии понедельника, а также те, которые изменились с понедельника. Резервная копия в пятницу будет включать все файлы, которые входили в резервные копии понедельника, вторника, среды и четверга, а также то, что изменилось с резервного копирования в четверг. Некоторые системы выполняют инкрементальное резервное копирование, собирающее все файлы, которые изменились со времени определенного инкрементального резервного копирования, а не последнего полного резервного копирования. Мы заимствуем терминологию UNIX и называем это *«инкрементальными резервными копиями уровня 2»*, если они содержат файлы, измененные со времени последнего уровня 1, или *уровня 3*, если они содержат файлы, измененные с последнего уровня 2, и т. д.

26.1. Основы

Создание вашей системы резервного копирования и восстановления должно начинаться с определения желаемого конечного результата и соответствующих действий для достижения этого результата. Конечный результат – это желаемые возможности системы по восстановлению. Восстановление требуется по разным причинам, и причины, актуальные для вашей среды, влияют на дельнейшие решения, например создание политики и графика.

Мы начнем с составления корпоративных инструкций, определяющих SLA касательно восстановлений на основе потребностей вашей компании, которые становятся политикой резервного копирования, определяющей график резервного копирования.

- *Корпоративные инструкции* определяют терминологию и минимальные и рекомендуемые требования к системам восстановления данных.

- *SLA* определяет требования к конкретному месту или приложению, которое руководствуется корпоративными инструкциями.
- *Политика* документирует реализацию SLA в общих терминах, понятных всем пользователям.
- *Процедура* показывает, как политика должна реализовываться.
- Подробный *график* показывает, когда для какого диска будет выполняться резервное копирование. Он может быть статическим или динамическим. Обычно он представляет собой политику, переведенную с человеческого языка на язык конфигурации программы резервного копирования.

За политикой и графиком идут рабочие вопросы. Расходные материалы могут быть дорогими и должны быть включены в бюджет. Чтобы обеспечить выполнение нашего SLA во время как резервного копирования, так и восстановления, требуется планирование времени и емкости системы. Политика и процедуры резервного копирования и восстановления должны быть документированы как для пользователей, так и для системных администраторов.

Только после определения всего этого мы можем строить систему. В современных системах резервного копирования есть три ключевых компонента: автоматизация, централизация и управление запасами. Мы рассмотрим каждый из них по очереди.

26.1.1. Причины для восстановления данных

Восстановление данных требуется по трем причинам. Если вы не понимаете их, система резервного копирования и восстановления может не выполнить эту задачу. Каждая причина имеет свои требования. Эти причины следующие:

1. *Случайное удаление файлов.* Пользователь случайно стер один или более файлов, и ему требуется их восстановить.
2. *Сбой диска.* Жесткий диск сломался, и все данные нужно восстановить.
3. *Просмотр архивных данных.* В силу деловых причин нужно регулярно сохранять цельную картину для аварийного восстановления, правовых или долговых целей.

26.1.1.1. Случайное удаление файлов

В первом случае пользователи предпочли бы быстрое восстановление любого файла в том виде, в котором он существовал в тот или иной момент. Однако обычно это невозможно. В офисной среде обычно можно ожидать возможности восстановить файл таким, каким он был один день назад, а для выполнения восстановления потребуется 3–5 ч. Очевидно, в особых случаях, которые встречаются, например, в финансовой сфере и сфере электронной коммерции, требования гораздо выше. Сейчас проще сделать восстановление удобным, потому что современное программное обеспечение (Moran and Lyon 1993) разрешает пользователям мгновенно восстанавливать свои данные – если лента[1] еще в приводе – или после вмешательства оператора – если пользователи должны ждать загрузки ленты.

[1] В данной главе мы будем говорить о носителе для резервного копирования как о ленте, хотя мы понимаем, что этому есть альтернативы.

Самостоятельное восстановление не является новой возможностью. Такая возможность предоставлялась системами начиная с 1980-х годов.

- В начале 1980-х годов операционная система VAX/VMS от DEC (сейчас HP через посредство Compaq) сохраняла предыдущие версии файлов, к которым можно было выполнять доступ, указав номер версии как часть имени файла.
- В 1988 году (Hume 1988) в Bell Labs изобрели File Motel, систему, которая навсегда записывала на оптические пластины инкрементальные резервные копии. Подразделение CommVault[1] компании AT&T предоставляло такую систему вечного резервного копирования в качестве одного из своих продуктов.
- В 1990-х годах NetApp представила свою линию дополнений для файловых серверов Filer, у которых была встроенная функция сохранения образов. Почасовые, ежедневные и еженедельные образы файловой системы рациональным образом записывались на диск. Блоки данных, которые не изменялись, записывались только один раз. Продукты Filer работали в своих файловых системах на узлах UNIX через протокол NFS, а также с другими операционными системами через протокол Microsoft CIFS, что обеспечило им популярность среди системных администраторов в компаниях, использовавших несколько ОС. Пользователям нравилось, как образы позволяли им «вернуть директорию в прошлое». Возможности создания образов или их подобий с различными уровнями эффективности хранения были добавлены другими производителями.

Такие системы становятся все более распространенными по мере того, как технологии дешевеют, а ценность информации растет.

Для системного администратора ценность образов заключается в том, что они снижают нагрузку, потому что наиболее распространенный тип запроса теперь переводится на самообслуживание. Для пользователей ценность образов в том, что они предоставляют новые возможности лучшего управления своей работой. Отношение пользователей к своей работе изменяется, когда они узнают, что могут положиться на образы. Если образы сохраняются навсегда, как в случае CommVault, люди по-другому управляют своим использованием диска, зная, что они всегда могут получить обратно то, что удалили. Даже если образы доступны только в течение фиксированного срока, пользователи создают творческие, новые и более эффективные рабочие процессы.

Кроме того, образы повышают производительность пользователей, снижая объемы потерянных данных, восстанавливаемых вручную. При случайном удалении данных пользователи могут перестроить их, а не ждать восстановления, которое может потребовать нескольких часов или даже дней. Каждый из нас вносил в файл изменения, о которых потом жалел. Ручная переделка файла – это процесс, подверженный ошибкам, но было бы глупо несколько часов ждать выполнения запроса на восстановления. При наличии образов снижается вероятность, что пользователи будут пытаться воссоздать данные вручную.

Наиболее распространенная причина запроса на восстановление – необходимость восстановить случайно удаленный файл. Современное программное обеспечение вместе с приводами для ленты может сделать этот тип восстановления функци-

[1] Теперь CommVault – отдельная компания.

ей самообслуживания. Что еще лучше, замысловатые системы, которые обеспечивают создание образов, не только решают эту проблему без необходимости вмешательства системного администратора в каждое восстановление, но и положительно влияют на рабочую обстановку в компании.

26.1.1.2. Сбои дисков

Второй тип восстановления связан со сбоями дисков – или любого оборудования либо программного обеспечения, – вызывающими полную потерю файловой системы. Сбой диска вызывает две проблемы: потерю обслуживания и потерю данных. В критических системах, например в сферах электронной коммерции и финансовой, нужно использовать RAID, чтобы поломки дисков не влияли на обслуживание, по возможности с исключением потери производительности. Однако в некритических системах пользователи обычно[1] могут ожидать выполнения восстановления в течения дня, и, несмотря на то что им не нравится утрата данных, они обычно считают потерю одного рабочего дня приемлемым риском. Иногда сбой находится между двумя крайностями: критическая система еще может работать, но данные на конкретном диске недоступны. В таком случае проблема может быть менее срочной.

Выполнение этого типа восстановления обычно требует много времени. Скорость восстановления является медленной, потому что восстанавливаются гигабайты данных, а весь объем данных будет недоступен до записи последнего байта. Что еще хуже, выполняется процесс из двух этапов: сначала нужно прочитать последнюю полную резервную копию, а затем – самую последнюю инкрементальную (или несколько).

26.1.1.3. Просмотр архивных данных

Третий тип запросов на восстановление – просмотр архивных данных. Корпоративные политики могут потребовать от вас воспроизвести всю среду в том виде, в котором она была квартал, полгода или год назад, в случае аварий или судебных процессов. Работа, необходимая для создания архива, аналогична полному резервному копированию для других целей, но есть пять отличий.

1. Архивы – это полные резервные копии. В среде, где обычно полные и инкрементальные резервные копии перемешаны на одних и тех же лентах, архивные ленты не должны быть в таком же беспорядке.
2. В некоторых компаниях требуется отделение архивных лент от других резервных копий. Это может означать, что архивные копии создаются за счет создания второго, избыточного набора полных резервных копий. В качестве альтернативы архивные копии могут создаваться за счет копирования полных резервных копий с ранее созданных резервных лент. Несмотря на то что альтернатива является более сложной, она в случае автоматизации может выполняться без вмешательства человека, когда привод для ленты не используется для других целей.
3. Архивы обычно хранятся вне офиса.
4. Архивные ленты хранятся дольше других. Они могут быть записаны на носители, которые устареют и в конце концов станут недоступны. Вам может понадобиться хранить вместе с архивами одно-два совместимых устройства для чтения лент, а также соответствующее программное обеспечение.

[1] Слово «обычно» опять касается обстановки стандартного офиса.

5. Если архивы являются частью плана аварийного восстановления, для них могут работать особые правила или законы.

При создании архивных копий не забывайте включать в них средства, которые используются для работы с данными. Средства часто обновляются, и если архивные копии используются для резервного копирования всей среды, то инструменты, вместе со своим особым набором ошибок и возможностей, должны быть в них включены. Убедитесь, что средства, необходимые для восстановления архива, и сопроводительная документация хранятся вместе с архивом.

Существует несколько специализированных ситуаций резервного копирования и восстановления, но большинство из них подходит под одну из трех категорий.

26.1.2. Типы восстановления

Интересно заметить, что три типа запросов на восстановления обычно соответствуют трем различным типам пользователей. Восстановление отдельных файлов требуется пользователям, которые случайно удалили данные, то есть непосредственным пользователям данных. Архивные копии предназначены для потребностей юридических и финансовых отделов, которые их запрашивают, то есть людей, не работающих напрямую с самими данными[1]. Полное восстановление после поломки диска – работа системных администраторов, которые обязаны выполнять конкретное SLA. Таким образом, резервные копии для полного восстановления – это часть корпоративной инфраструктуры.

В среде, где обслуживание тарифицируется с высокой точностью, эти типы резервного копирования могут тарифицироваться по-разному. Если это возможно, упомянутые группы пользователей должны индивидуально оплачивать эти специальные требования, как они оплачивали бы любую другую услугу. Может потребоваться различное программное обеспечение, и возможны разные требования к физическому хранению и к тем, кто «владеет» лентами.

Передача расходов правильному пользователю

Во время слияния корпораций Министерство юстиции США потребовало от компаний сохранять все ленты с резервными копиями, пока сделка не была подтверждена. Это означало, что старые ленты нельзя было уничтожить. Расходы на покупку новых лент были переданы юридическому отделу компании. Особое обслуживание было нужно ему, поэтому ему пришлось платить.

26.1.3. Корпоративные инструкции

Организациям требуется общий для корпорации документ, который определяет требования к системам восстановления данных. Создатели глобальных корпоративных политик должны прилагать усилия к тому, чтобы установить минимум, основанный на правовых требованиях, а не перечислять каждую конкретную деталь реализации объектов, которые рассмотрены ниже в этой главе.

[1] Все чаще юридические отделы не сохраняют резервные копии данных или стирают ленты через все более короткие сроки. Судьи не могут использовать в ходе разбирательства документы, которые не сохранились.

Инструкция должна начинаться с определения того, почему необходимы резервные копии, что составляет резервную копию и для каких данных должно выполняться резервное копирование. Некоторые указания по сохранению данных должны быть изложены в явном виде. Должны быть определены различные SLA для каждого типа данных: финансовых, важных для выполнения задачи, проектных, общих данных домашней директории, данных электронной почты, экспериментальных данных и т. д.

В инструкции должен быть указан ряд вопросов, которые нужно учесть в каждой системе, чтобы они не были упущены. Например, инструкции должны требовать тщательного планирования времени резервного копирования, а не просто выполнять его во временной интервал по умолчанию «с полуночи и до завершения». Неприемлемо указывать один и тот же временной промежуток для всех систем. Резервное копирование обычно влияет на быстродействие и поэтому должно выполняться вне периодов пиковой нагрузки. У компаний электронной коммерции с глобальной базой клиентов будет совершенно другой перерыв для резервного копирования, чем у офисов с нормальным рабочим графиком.

Резервное копирование замедляет службы

В 1999 году телекоммуникационная компания получила несколько негативных отзывов в прессе за неправильное время выполнения резервного копирования. Компания передала планирование резервного копирования третьей стороне, которая выполняла его в часы пиковой нагрузки. Это негативно влияло на быстродействие веб-сервера, раздражая ведущего технологической рубрики, который написал длинную статью о том, что у крупных компаний, предоставляющих каналы связи, фактически «их нет». Он полагал, что низкое быстродействие было связано с недостаточной пропускной способностью. И хотя ваши проблемы с производительностью, связанные с резервным копированием, могут не попасть в новости, они все-таки принесут неудобства.

Люди помнят плохие отзывы в СМИ, а не успешное устранение последствий (Dodge 1999).

Если вы пишете документ с глобальными корпоративными требованиями, вам нужно начать с опроса различных групп, чтобы узнать их требования: поговорите со своим юридическим отделом, высшим руководством, системными администраторами и вашими пользователями. Теперь ваша задача – достичь консенсуса между ними. Используйте три основных типа восстановления, чтобы очертить рамки темы.

Например, юридическому отделу могут потребоваться архивные копии для подтверждения владения авторским правом или интеллектуальной собственностью. В страховании могут потребоваться общие резервные копии, которые хранятся как минимум полгода. Бухгалтерии может потребоваться хранение данных, связанных с налогами, в течение 7 лет, но записанных только поквартально. Все чаще юридические отделы требуют короткого времени хранения электронной почты, особенно в свете того, что основная улика в судебном иске против корпорации Майкрософт была найдена при просмотре ее архивов элек-

тронной почты. В большинстве компаний настаивают на том, чтобы архивы электронной почты уничтожались через полгода.

Важно найти баланс всех этих потребностей. Вам может потребоваться провести несколько этапов опросов, пересматривать требования, пока они не будут приняты всеми заинтересованными сторонами.

Некоторые компании, особенно начинающие, могут быть слишком маленькими, чтобы им требовались какие-то другие инструкции, кроме фразы «Нужно создавать резервные копии». С ростом компании обеспечьте создание корпоративных инструкций на основе требований ваших инвесторов и юридических консультантов.

26.1.4. SLA и политика восстановления данных

Следующий этап – определить уровень обслуживания, который подходит конкретно для вашей компании. SLA – это письменный документ, который указывает, какое обслуживание и с каким быстродействием обязуется предоставить поставщик услуг. Эта политика должна создаваться в диалоге с вашими пользователями. После определения SLA его можно перевести в политику, определяющую, как оно будет выполняться.

Для создания SLA перечислите три типа восстановления, а также желаемое время восстановления, степень подробности и время хранения таких резервных копий – как часто должно выполняться резервное копирование и сколько времени должны храниться ленты, – а также промежуток времени, в который может выполняться резервное копирование – например, с полуночи до 8 ч утра.

Для большинства системных администраторов корпоративный стандарт уже существует и содержит неопределенные, высокоуровневые параметры, которые они должны соблюдать. Убедитесь, что ваши пользователи в курсе этих инструкций. С этого момента создание политики обычно является очень простым.

Пример SLA, которым мы пользуемся в остальной части данной главы, следующий. Пользователи должны иметь возможность получить любой файл с детализацией в один рабочий день за последние полгода или с детализацией в один месяц за последние три года. Восстановление после сбоя диска должно занимать 4 ч, с потерей данных не более чем за два рабочих дня. Архивы должны быть полными резервными копиями на отдельных лентах, которые создаются каждый квартал и хранятся вечно. Критические данные будут храниться в системе, содержащей доступные пользователям образы, которые делаются каждый час в период с 7 до 19 ч, а образы, сделанные в полночь, хранятся неделю. У баз данных и финансовых систем должны быть более высокие требования, которые определяются требованиями приложений и поэтому не входят в этот пример политики.

Политика, основанная на этом SLA, предполагает выполнение ежедневного резервного копирования и хранение лент в течение указанных сроков. Политика может определить, с какой частотой будет выполняться полное резервное копирование по сравнению с инкрементальным.

26.1.5. График резервного копирования

Теперь, когда у нас есть SLA и политика, мы можем установить конкретный график, в котором указано, когда выполняется резервное копирование каких

разделов с каких узлов. Несмотря на то что SLA должно меняться редко, график корректируется часто в соответствии с изменениями обстановки. Многие системные администраторы предпочитают указывать график в конфигурации программ резервного копирования.

В соответствии с нашим примером резервное копирование должно выполняться каждый рабочий день. Даже если компания сталкивается с поломкой нерезервированного диска, мы не потеряем данные больше чем за два дня. Так как полное резервное копирование требует значительно больше времени, чем инкрементальное, мы назначим его на вечер пятницы и позволим ему выполняться все выходные. С воскресенья по четверг вечером выполняется инкрементальное резервное копирование.

Вам может понадобиться решить, с какой периодичностью запускать полное резервное копирование. В нашем примере требуется ежемесячное создание полных резервных копий. Теоретически мы могли бы выполнять четверть нашего полного резервного копирования каждые выходные. Такой неторопливый темп соответствовал бы требованиям нашей политики, но был бы неразумным. Как мы отметили ранее, инкрементальные резервные копии растут со временем до завершения очередного полного резервного копирования. Более частое выполнение полного резервного копирования экономит ленту.

Однако программы резервного копирования со временем становятся все более автоматизированными. Часто можно просто перечислить все разделы, для которых нужно создать резервные копии, чтобы программа на основе этих требований сама создала график. Резервные копии выполняются автоматически, при необходимости заменить ленту по электронной почте отправляется предупреждение.

Давайте рассмотрим пример. Предположим, что для раздела с 4 Гб данных назначено полное резервное копирование каждые 4 недели (28 дней) и инкрементальное – во все остальные дни. Также предположим, что размер наших инкрементальных резервных копий каждый день растет на 5%. В первый день месяца 4 Гб емкости ленты используется для выполнения полного резервного копирования. На второй день используется 200 Мб, на третий – 400 Мб, на четвертый – 600 Мб и т. д. Емкость ленты, используемая на одиннадцатый и двенадцатый дни – 2 Гб и 2,2 Гб соответственно, что в сумме больше, чем полная резервная копия. Это означает, что на одиннадцатый день было бы разумнее сделать полное резервное копирование.

В табл. 26.1 данная гипотетическая ситуация представлена подробно с ежедневными, 7-дневными, 14-дневными, 28-дневными и 35-дневными циклами. Мы предполагаем нулевой рост после 20-го дня (80%) в более длинных циклах, потому что рост инкрементальных копий не является бесконечным.

Наихудшим случаем было бы выполнение ежедневного полного резервного копирования, или запись на ленту 168 Гб данных. Это было бы пустой тратой ленты и времени. В большинстве систем имеется больше данных, чем может быть полностью сохранено каждый день. В сравнении с лучшим способом при ежедневном полном резервном копировании используется 341% ленты. Этот график показывает, что чем длиннее цикл, тем ближе мы подходим к этому наихудшему случаю.

Наилучший в данном примере – 7-дневный цикл, или запись на ленту 49,2 Гб данных. Переход на 14-дневный цикл увеличивает использование ленты при-

Таблица 26.1. Использование ленты для 4 Гб данных, ежедневный прирост составляет 5%

Порядковый номер дня	Цикл					
	Ежедневный	7 дней	14 дней	21 день	28 дней	35 дней
1	4,0	4,0	4,0	4,0	4,0	4,0
2	4,0	0,2	0,2	0,2	0,2	0,2
3	4,0	0,4	0,4	0,4	0,4	0,4
4	4,0	0,6	0,6	0,6	0,6	0,6
5	4,0	0,8	0,8	0,8	0,8	0,8
6	4,0	1,0	1,0	1,0	1,0	1,0
7	4,0	1,2	1,2	1,2	1,2	1,2
8	4,0	4,0	1,4	1,4	1,4	1,4
9	4,0	0,2	1,6	1,6	1,6	1,6
10	4,0	0,4	1,8	1,8	1,8	1,8
11	4,0	0,6	2,0	2,0	2,0	2,0
12	4,0	0,8	2,2	2,2	2,2	2,2
13	4,0	1,0	2,4	2,4	2,4	2,4
14	4,0	1,2	2,6	2,6	2,6	2,6
15	4,0	4,0	4,0	2,8	2,8	2,8
16	4,0	0,2	0,2	3,0	3,0	3,0
17	4,0	0,4	0,4	3,2	3,2	3,2
18	4,0	0,6	0,6	3,4	3,4	3,4
19	4,0	0,8	0,8	3,6	3,6	3,6
20	4,0	1,0	1,0	3,8	3,8	3,8
21	4,0	1,2	1,2	3,8	3,8	3,8
	...	...	...	...	...	...
Всего за 42 дня	168	49,2	66,6	91,6	94,6	107,2
Процент от наихудшего случая, %	100	29	40	55	56	64
Процент от наилучшего случая, %	341	100	135	186	192	218

мерно на треть, как и дальнейший переход на 21-дневный цикл. У более длинных циклов прирост незначительный из-за нашего предположения о том, что инкрементальные резервные копии никогда не вырастут выше 80% от полной. Если бы наша реальная система была такой, как в данном примере, было бы относительно эффективно использовать 7-дневный или 14-дневный цикл либо что-то между ними.

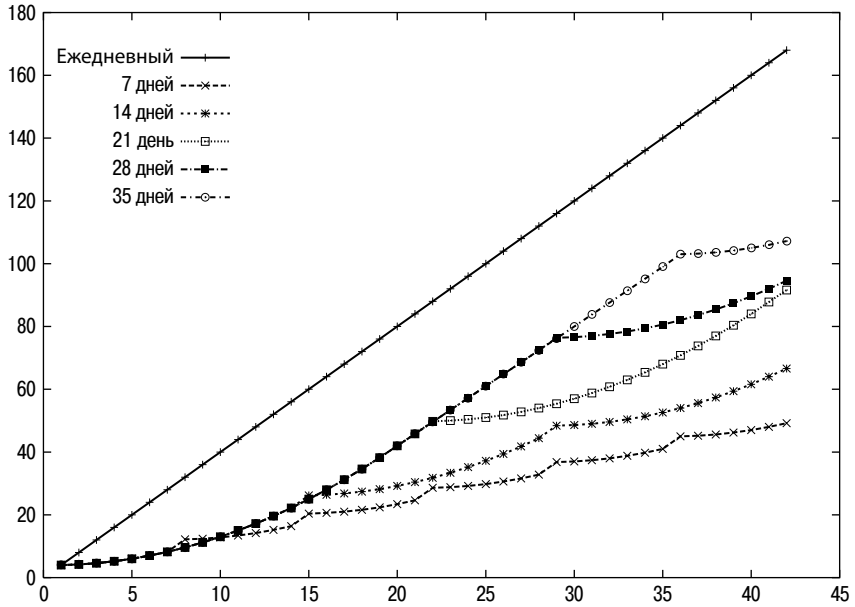

Рис. 26.1. *Рост использования ленты при циклах из табл. 26.1*

На рис. 26.1 отображен график общего использования ленты при этих циклах в течение 41 дня, с нарастающим итогом для каждой стратегии. «Ежедневная» линия показывает линейный рост использования ленты. Другие циклы начинаются с того же значения, но отклоняются от него по-своему.

Первый пример показывает основные принципы в простой ситуации. В более сложной и реалистичной модели учитывается тот факт, что доступ чаще всего осуществляется к небольшому количеству данных относительно общего объема данных на диске. Наше практическое правило заключается в том, что 80% доступа обычно осуществляется к одним и тем же 20% данных и пользователи обычно изменяют половину данных, доступ к которым они осуществляют. И хотя мы все-таки не можем заранее сказать, какие данные изменятся, мы способны дать прогноз, что первая инкрементальная резервная копия будет составлять 10% от размера данных, а каждая последующая – расти на 1%, пока очередное полное резервное копирование не сбросит цикл (табл. 26.2).

В данном случае 14-дневный цикл является наилучшим, а 21-дневный немного уступает ему и является вторым. 7-дневный цикл, который был наиболее эффективным в предыдущем примере, занимает третье место, потому что делает слишком много дорогих полных резервных копий. И снова наихудшим случаем является ежедневное выполнение полного резервного копирования. По сравнению с наилучшим случаем ежедневное полное резервное копирование требует 455% ленты. Мы также можем видеть, что циклы с 7-дневного по 28-дневный ближе друг к другу (между 106% и 115% от наилучшего случая, тогда как в предыдущем примере они сильно отличались).

Когда мы снова построим график роста использования ленты, мы увидим, как похожи циклы. График на рис. 26.2 показывает это. *Примечание*: на этом гра-

Таблица 26.2. Использование ленты для 4 Гб данных,10% прирост в день 1, 1% прирост в последующие дни

Порядковый номер дня	Цикл					
	Ежедневный	7 дней	14 дней	21 день	28 дней	35 дней
1	4,00	4,00	4,00	4,00	4,00	4,00
2	4,00	0,40	0,40	0,40	0,40	0,40
3	4,00	0,44	0,44	0,44	0,44	0,44
4	4,00	0,48	0,48	0,48	0,48	0,48
5	4,00	0,52	0,52	0,52	0,52	0,52
6	4,00	0,56	0,56	0,56	0,56	0,56
7	4,00	0,60	0,60	0,60	0,60	0,60
8	4,00	4,0	0,64	0,64	0,64	0,64
9	4,00	0,40	0,68	0,68	0,68	0,68
10	4,00	0,44	0,72	0,72	0,72	0,72
11	4,00	0,48	0,76	0,76	0,76	0,76
12	4,00	0,52	0,80	0,80	0,80	0,80
13	4,00	0,56	0,84	0,84	0,84	0,84
14	4,00	0,60	0,88	0,88	0,88	0,88
15	4,00	4,0	4,0	0,92	0,92	0,92
16	4,00	0,40	0,40	0,96	0,96	0,96
17	4,00	0,44	0,44	1,00	1,00	1,00
18	4,00	0,48	0,48	1,04	1,04	1,04
19	4,00	0,52	0,52	1,08	1,08	1,08
20	4,00	0,56	0,56	1,12	1,12	1,12
21	4,00	0,60	0,60	1,16	1,16	1,16
	...	...	...	...	...	...
Всего за 42 дня	168	42	36,96	39,2	41,16	47,04
Процент от наихудшего случая, %	100	25	22	23	25	28
Процент от наилучшего случая, %	455	114	100	106	111	127

фике нет ежедневного полного резервного копирования, чтобы более подробно показать другие циклы.

Наилучшая длина цикла будет своя в каждой среде. Мы видели пример, в котором 7-дневный цикл был явно наилучшим вариантом, и другой пример, где он не был самым лучшим. Для определения наилучшего в вашей среде варианта требуется тщательная настройка. Если вы начинаете с нуля и у вас нет предыдущих данных для обоснования своего решения, разумно начать с 14-дневного цикла и при необходимости изменять его в дальнейшем. Просмотрев отчеты об использовании пространства и выполнив небольшие математические

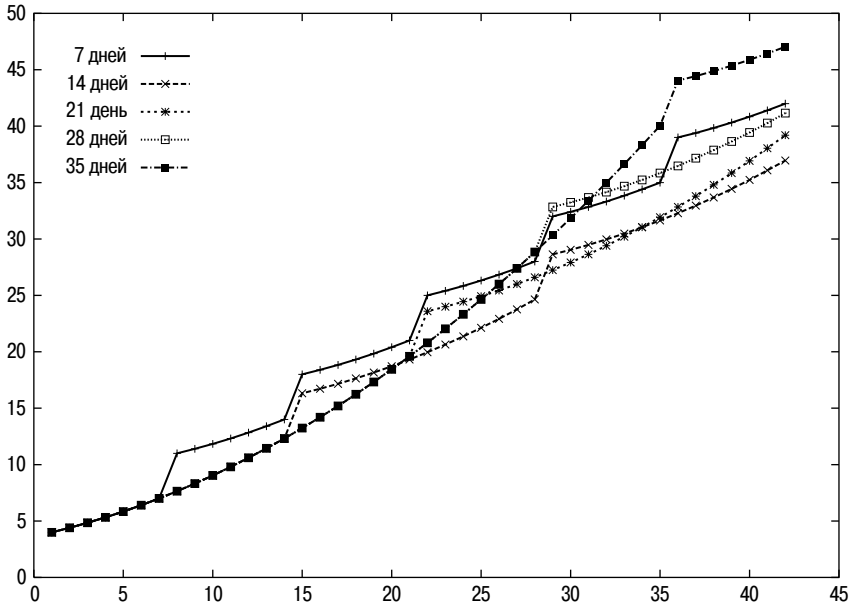

Рис. 26.2. Рост использования ленты при циклах из табл. 26.2

вычисления, вы сможете определить, будет ли при более длинном или более коротком цикле использоваться меньше ленты. Разумеется, эти решения должны соответствовать SLA и политике.

Недавние разработки дали программному обеспечению резервного копирования возможность автоматической настройки. Несмотря на то что человеку (даже системному администратору) может быть тяжело отслеживать растущие потребности сотен дисков, для компьютера это легко. Мы думаем, что в конце концов все коммерческие программы резервного копирования будут поддерживать какую-либо форму динамического графика.

Пример: пузырьковый динамический график резервного копирования

Динамические графики не должны быть сложными. Однажды Том создал следующий простой динамический график. В соответствии с SLA нужно было каждую ночь выполнять резервное копирование каждого раздела на каждом сервере, инкрементальное или полное, и полное резервное копирование должно было выполняться каждые 7–10 дней.

Список разделов сортировался по дате резервного копирования, разделы, после последнего резервного копирования которых прошло больше всего времени, размещались в верхней части списка. Первым разделам назначалось полное резервное копирование этой ночью на отдельном наборе приводов магнитных лент. Для оставшихся разделов выполнялось инкрементальное резервное копирование.

В результате все невыполненные резервные копии «всплывали» в верхнюю часть списка и были первым приоритетом на следующую ночь. Обычно резервное копирование не выполнялось из-за отключения узла или, что было более вероятно, превышения емкости ленты. Программа не могла продолжать резервное копирование на следующей ленте (это было до того времени, когда появились доступные приводы для магнитных лент).

Систему можно было настроить двумя способами. Если полное резервное копирование разделов не выполнялось достаточно часто, для этого выделялись дополнительные устройства записи на ленты. Если ленты с инкрементальными резервными копиями заполнялись, для них выделялось большее количество устройств записи на ленты. В данном случае системные администраторы должны были следить не только за тем, чтобы инкрементальные резервные копии не заполняли свои ленты до опасного уровня, но и за тем, не тратится ли на них большее время, чем выделено на перерыв для резервного копирования.

В некоторых системах имеется только один уровень инкрементального резервного копирования. В других есть инкрементальное копирование, при котором записываются все файлы, измененные с последнего резервного копирования того же уровня, – иногда они называются *истинными инкрементальными*, или дифференциальными[1].

Другой способ сэкономить ленту – выполнять два уровня инкрементального резервного копирования, если ваша система это поддерживает. Например, полное резервное копирование (уровень 0) запускается в первый день месяца с последующим инкрементальным резервным копированием каждую ночь, которое сохраняет все файлы, измененные с первоначального полного резервного копирования. Размер этих инкрементальных резервных копий к середине месяца становится очень большим. Пятнадцатого числа месяца начинается инкрементальное копирование уровня 2, оно записывает все файлы, которые изменились со времени последнего резервного копирования уровня 1. Инкрементальные резервные копии середины месяца должны вернуться к достаточно небольшому разделу. Это экономит ленту таким же образом, как и инкрементальное резервное копирование вместо полного.

Однако в данном случае есть два недостатка. Во-первых, такое резервное копирование гораздо сложнее отслеживать, хотя это не проблема, если система полностью автоматизирована и поддерживает хорошую инвентаризацию. Во-вторых, восстановление становится более сложным и подверженным ошибкам: теперь, чтобы обеспечить восстановление файла, вам нужно прочитать ленты уровней 0, 1 и 2. Это требует больше времени, а дополнительное усложнение означает, что, если процесс выполняется вручную, он больше подвержен ошибкам. Также присутствует фактор надежности: когда вероятность того, что лента будет плохой, равна 1:1000, то риск повышается, если нужно полагаться не на две ленты, а на три.

---

[1] Важно понимать, что ваш разработчик подразумевает под словом «инкрементальный». Лучше перестраховаться, чем потом жалеть, поэтому уделите время самостоятельному тестированию системы, чтобы убедиться, что вы понимаете, как работает система резервного копирования вашего разработчика.

26.1.6. Планирование времени и емкости

Восстановление и резервное копирование ограничено по времени. Восстановление должно происходить в пределах времени, разрешенного SLA службы, которая может быть отключена до завершения восстановления. Резервное копирование может выполняться только в течение определенных временных интервалов. Большинство систем значительно замедляются при выполнении резервного копирования.

Скорость резервного копирования ограничена самым медленным из следующих факторов: скоростью чтения с диска, скоростью записи на резервный носитель, полосой пропускания и задержкой сети между диском и резервным носителем. Время восстановления определяется факторами, обратными упомянутым. Устройства ввода-вывода на магнитную ленту обычно записывают на нее с гораздо меньшей скоростью, чем читают.

Многие неопытные системные администраторы верят, что утверждения производителей о скоростях и емкостях приводов для магнитных лент как-то связаны с их производительностью. Они серьезно ошибаются. Различие может быть очень большим, мы видели разницу в 1500%. Производители постоянно настраивают и улучшают свои алгоритмы резервного копирования для повышения скорости, но часто игнорируют скорость восстановления; большинство их пользователей не думают о том, чтобы просить о быстром восстановлении, а те, кому оно нужно, готовы платить за него дополнительно.

Скорость резервного копирования будет определяться самым медленным звеном цепи. Этот процесс также подвержен влиянию механических проблем. Большинство приводов для магнитных лент записывают на ленту быстро, если данные вводятся в них с такой же скоростью, с какой они могут записывать (потоковый режим), но скорость значительно снижается, если данные не вводятся с достаточной скоростью для соответствия скорости записи на ленту. Если у привода нет данных для записи, он должен остановиться, вернуться на конец записи и ждать, пока данных не будет достаточно для того, чтобы снова начать записывать. Производители приводов называют это **эффектом чистки обуви**, потому что механизм чтения/записи передвигается вперед-назад над одним и тем же участком ленты. Помимо замедления быстродействия записи, он подвергает ленту излишнему напряжению.

Таким образом, если сервер не может достаточно быстро подавать данные, скорость резервного копирования значительно снижается. Например, если перегрузка сети замедляет данные, идущие к узлу с приводом для магнитной ленты, резервное копирование может проходить значительно медленнее, чем при отсутствии перегрузки. Много раз нас просили разобраться с проблемами с медленным резервным копированием только для того, чтобы мы обнаружили, что быстродействие сети в этом месте ниже, чем максимальная скорость записи привода ленты.

Скорость восстановления также зависит от самого медленного звена, но здесь есть дополнительные факторы. Поиск одного файла на диске может занять столько же времени, сколько само по себе полное восстановление диска. Сначала система должна пропустить другие тома, записанные на этой ленте. Затем система должна прочитать конкретный том, чтобы найти определенный файл, для которого требуется восстановление. Если у привода для ленты нет возможности быстрой перемотки или пропуска данных до определенного сегмента, это может быть очень медленным.

Восстановление целого диска также очень медленно. Основная проблема скорости восстановления – скорость не чтения диска, а записи файловой системы. В большинстве файловых систем запись гораздо менее эффективна, чем чтение, и восстановление файловой системы обычно выполняется с наихудшим быстродействием, особенно в случае файловых систем с протоколированием. Мы видели, как восстановление диска занимало в 5–15 раз больше времени, чем его резервное копирование. Для большинства людей это был очень неприятный сюрприз.

Если сервер способен достаточно быстро получать данные, чтобы привод для ленты мог оставаться в потоковом режиме, восстановление может происходить с максимальной скоростью. Однако, если буфер данных привода для ленты заполняется, привод снизит скорость ленты или, возможно, полностью остановит механизм перемотки. Обратная перемотка на нужную позицию и возвращение к высокой скорости требуют большой задержки.

При построении системы резервного копирования и восстановления вы должны учитывать скорость различных соединений и осуществлять планирование так, чтобы самое медленное соединение не помешало вам выполнить задачи по времени. Довольно распространенным является применение выделенной сети, используемой исключительно файловыми серверами для связи со своим узлом резервного копирования. Одним из первых преимуществ, которые привели к популяризации SAN, была возможность убрать трафик резервного копирования из основной сети.

Для смягчения влияния проблем быстродействия во время резервного копирования распространено использование диска в качестве буфера. Раньше системы выполняли резервное копирование данных, копируя их с одного сервера на устройство записи на ленту централизованного узла резервного копирования. Теперь в узле резервного копирования часто размещают много дисков. Серверы копируют свои данные на диски узла резервного копирования, часто по одному файлу на дисковый том одного сервера. Теперь узел резервного копирования может записывать завершенные файлы резервного копирования на полной скорости ленты. Распространены конфигурации, в которых все серверы записывают свои резервные копии ночью, а узел резервного копирования тратит день для записи данных на ленту. Этот подход известен как диск–диск–лента (disk-to-disk-to-tape – D2D2T). Такой подход работает лучше, потому что доступ к локальным дискам является более определенным, чем доступ по сети. Вместо проектирования так, чтобы данные могли идти по всему пути со скоростью, необходимой для приводов лент, нужно только обеспечить, чтобы такой скорости можно было достичь между локальным диском и устройством записи на ленту.

Единственный способ точно узнать, были ли выполнены ваши временные условия, – это протестировать. Оценка времени как тестового резервного копирования, так и тестового восстановления может подтвердить правильность вашей структуры. Со временем опыт поможет вам определять, что будет работать, а что нет. Однако может быть трудно получить полезный опыт, когда системы резервного копирования и восстановления обычно изменяются каждые несколько лет. Вместо этого вы можете положиться на опыт других людей, будь то дружелюбный сотрудник отдела продаж или консультант, который специализируется на системах резервного копирования и восстановления.

26.1.7. Планирование расходных материалов

Ваши политика и график влияют на скорость использования расходных материалов: лент, чистящих лент и т. д. Это также требует выполнения расчетов. Если снова использовать политику из нашего примера, инкрементальные резервные копии могут перезаписываться после полугода хранения, а полные, помимо тех, которые хранятся отдельно в качестве архивов, можно перезаписывать через три года.

Вначале лент для перезаписи нет. Первые полгода для всего, что вы делаете, нужно покупать новые ленты. Вы можете математически подсчитать, сколько вам понадобится лент, изучив график. Предположим, что 6 дней в неделю будет использоваться по 8 лент каждый день. Это составляет 48 лент в неделю, или 1248 лент в первые 6 месяцев. Ленты с цифровой линейной записью (Digital Linear Tape – DLT) стоят около 80 долларов за штуку, то есть 99 840 долларов за первые 6 месяцев[1].

Так как стоимость лент постоянно сокращается, мы рекомендуем вам закупать их по месяцам или кварталам. Практическое правило – первая закупка должна быть вдвое больше, чтобы создать запас пустых лент на случай задержки дальнейших заказов. С другой стороны, стоимость лент часто быстрее падает до меньшего значения, чем вы можете получить за счет оптовых скидок при заблаговременной покупке крупных партий.

В следующие 6 месяцев вы можете перезаписать все инкрементальные резервные копии и вам потребуется покупать новые ленты только для полных резервных копий. Допустим, что для полных резервных копий вам потребуется 9 лент в неделю, а инкрементальные растут такими темпами, что в неделю вам потребуется 1 дополнительная лента. Таким образом, во втором полугодии вам потребуется только 260 лент, которые будут стоить 18 200 долларов, если предположить, что к тому времени стоимость ленты упадет до 70 долларов. Если эти оценки верны, то из-за перезаписи лент ваши расходы на них во втором полугодии будут составлять только около 18% того, что вы платили в первом полугодии:

Расходы на ленты (первый год): 118 040 долларов

На второй и третий годы также потребуется около 260 новых лент в полгода, или 36 400 долларов в год:

Расходы на ленты (второй и третий годы): 36 400 долларов в год

Расходы на ленты (первые три года): всего 190 840 долларов, или в среднем 5301 доллар в месяц

Через три года вы сможете перезаписать все ленты первого года (1508 лент), кроме тех, которые отмечены как архивные. Если вы выполняете полное резервное копирование каждые 14 дней, архивными лентами должны быть все ленты с полными резервными копиями, записанные в первые три недели любого квартала, или 72 ленты в год ($9 \times 2 \times 4$). Остается всего 1436 лент. Таким образом, вам потребуется купить только 70–80 лент в год. Если предположить, что цена одной ленты будет составлять 70 долларов, ваши расходы на новые ленты снизятся до 5–6 тыс. долларов в год:

---

[1] А вы думали, что привод дорогой!

Расходы на ленты (четвертый и последующие годы): 6000 долларов в год

Расходы на ленты (первые четыре года): всего 196 840 долларов, или в среднем 4100 долларов в месяц

Несмотря на то что четвертый год самый дешевый, скорее всего, он станет последним перед тем, как вы должны будете перейти на новую технологию с несовместимыми носителями. Если старая система еще используется для обслуживания прежних версий систем, лент, доступных для перезаписи, должно хватать для ваших сокращенных потребностей.

Давайте рассмотрим, как все было бы по-другому, если бы политика предписывала хранить полные резервные копии, кроме архивных, только один год. Расходы на ленты в течение четырех лет были бы значительно ниже. Во второй и последующие годы вы могли бы перезаписать все ленты, кроме 72, выделенных на архивы. Затраты во второй, третий и четвертый годы обошлись бы менее чем в 6 тыс. долларов в год:

Расходы за три года при измененной политике: всего 129 240 долларов, или в среднем 3590 долларов в месяц

Расходы за четыре года при измененной политике: всего 134 840 долларов, или в среднем 2809 долларов в месяц

Это единственное изменение политики совсем не повлияло на расходы за первый год, но снизило средние расходы как за три, так и за четыре года примерно на 32%.

При создании политики резервного копирования и восстановления техническим специалистам обычно нужны резервные копии, хранящиеся вечно, а финансистам требуется политика, которая экономит максимально возможное количество денег. Нахождение равновесия требует расчетов, основанных на ваших наилучших прогнозах по стоимости расходных материалов. Может быть полезно показать людям модели расходов на то, что они потребовали.

26.1.8. Вопросы процесса восстановления

Важные вопросы, связанные с процессом восстановления, требуют серьезного разбора и планирования. Во-первых, нужно сформировать ожидания пользователей. Они должны знать, какова политика резервного копирования и как запросить восстановление файла. Достаточно будет даже такого простого объяснения:

Резервное копирование выполняется только для данных, которые хранятся на серверах (диск Z: ваших компьютеров, или директория /home в UNIX), каждую ночь с полуночи до 8 ч утра. *Мы никогда не делаем резервных копий локального диска C: вашего компьютера.* Если вам нужно восстановить файл, зайдите на [*вставьте URL*] для получения более подробной информации или отправьте по электронной почте сообщение с запросом «поддержки» с названием сервера, полным путем к файлу и датой, по состоянию на которую вы хотите восстановить файл. При отсутствии проблем простое восстановление выполняется в течение 24 ч.

Хорошая идея – включить эту информацию в любой тип справочных документов или презентаций для новых пользователей и разместить ее в виде баннера на вашем внутреннем веб-портале. Если ваша политика исключает выполнение резервного копирования на определенных машинах, особенно важно, чтобы люди это знали.

Вы должны думать о влиянии любого запроса о восстановлении на безопасность. Есть ли у этого человека право получать данные файлы? Изменятся ли права доступа к файлу или его владелец в результате восстановления? Данные будут восстановлены в том же месте с такими же правами доступа или в новом месте, возможно, с другим влиянием на безопасность? Перезапишут ли они существующие данные?

Вот важнейший вопрос безопасности в данном случае: запросы на восстановление должны подтверждаться. Миллионы долларов, вложенные в инфраструктуру безопасности, могут превратиться в пыль из-за неосмотрительного восстановления. Очевидно, восстановление файлов в чью-то директорию на сервере, где они были изначально, слабо влияет на безопасность. Однако восстановление директории, которая является частью проекта, в чью-нибудь домашнюю директорию может влиять на безопасность, особенно если этот человек не участвует в проекте.

Несмотря на то что такой тип атаки может показаться редким, риск ее совершения возрастает по мере передачи более широких полномочий контроля сторонним исполнителям. В небольшой компании может быть нормальным, если руководитель просит восстановить файлы из директории сотрудника, и системный администратор может проверить, являются ли правомерными отношения персонала и руководителя, поскольку все друг друга знают. Однако как вы проверите, кто входит в какую организацию, в компании из 50 тыс. человек? Таким образом, по мере роста компании существование четко определенной процедуры проверки правомерности запросов на восстановление становится более важным.

Важно, чтобы восстановление могли выполнять несколько человек, а не только тот, кто создал систему. Обычно инженер, создавший систему, уделяет время автоматизации ежедневного процесса замены лент, чтобы процесс был максимально простым. Это позволяет выполнять задачу менее высокооплачиваемому клерку. Однако создатели систем часто забывают, что неразумно быть единственным человеком, который знает, как выполнять восстановление. Процесс восстановления должен быть хорошо документирован. Документация должна находиться в сети, а напечатанную версию следует поместить рядом с оборудованием резервного копирования. Силы, затраченные на документацию и обучение людей определенному типу восстановления, должны быть пропорциональны тому, как часто это восстановление запрашивается. Выполнению наиболее распространенного запроса, простому восстановлению файлов, должно быть обучено много людей. Эта процедура должна быть простой. Несколько человек должны быть обучены тому, как восстанавливать весь диск целиком. Это может потребовать дополнительных технических знаний, потому что может включать замену сломанных дисков, или знание того, кто это умеет. Наконец, несколько старших системных администраторов должны быть обучены тому, как восстанавливать сломанный загрузочный диск. Это может быть трудно документировать, потому что каждый сервер немного отличается от других, но основной вопрос документации заключается в том, как выполнить восстановление на системе, которая находится в частично рабочем состоянии, или как выполнить восстановление, когда машина с приводом для ленты не работает. Во всех этих документах должна присутствовать контактная информация служб поддержки для всех вовлеченных производителей, а также номера контрактов на обслуживание и пароли, необходимые для получения обслуживания.

26.1.9. Автоматизация резервного копирования

Отсутствие автоматизации резервного копирования опасно и глупо. Оно опасно потому, что чем больше вы автоматизируете, тем надежнее вы исключаете фактор человеческой ошибки. Резервное копирование утомительно, и, если оно не автоматизировано, оно не будет надежно выполняться. Если оно не выполнено правильно, то вам будет нечего ответить на вопрос вашего генерального директора: «Но почему не было резервных копий?»

Можно автоматизировать три аспекта процедуры резервного копирования: команды, график, а также управление лентами и их инвентаризацию. Раньше автоматизации не было. Отдельные команды вводились вручную каждый раз, когда выполнялось резервное копирование. Часто резервное копирование выполнялось последней сменой перед уходом с работы вечером. График был простым. Инвентаризация была минимальной или ее не было совсем, кроме меток на лентах. Первым этапом автоматизации стали скрипты, которые просто воспроизводили команды, вводимые раньше вручную. Однако принятие решения о том, для чего выполнять резервное копирование, все еще было человеческой задачей, а управления инвентаризацией практически не было. Вскоре в программах были реализованы алгоритмы создания графиков, которое люди выполняли вручную. Со временем алгоритмы были улучшены, предоставляя динамические графики, которые превосходили то, что могли сделать люди. Наконец задача физической работы с лентами была автоматизирована при помощи приводов с автоматической сменой носителей. Автоматизированные системы просили клерка удалить из привода определенный набор лент и заменить их новыми лентами. С хорошо организованной инвентаризацией в полностью автоматизированной системе можно было даже автоматизировать процессы отслеживания того, какие ленты должны быть перезаписаны, и печати сообщения об этих лентах.

Не везде нужна такая развитая автоматизация, но везде необходимо иметь по крайней мере два первых уровня автоматизации. Все это может казаться очевидным, но в каждой компании есть одна-две машины, на которых резервное копирование выполняется вручную. Часто они находятся за пределами брандмауэра и недостижимы из центральной системы резервного копирования. Очень важно ввести для этих систем по крайней мере простую, примитивную автоматизацию. Если что-то не автоматизировано, оно не будет выполняться.

Мы без колебаний называем отсутствие автоматизации резервного копирования глупым, потому что ручное резервное копирование – это пустая трата сил и времени. При наличии автоматизации ежедневная задача резервного копирования может выполняться кем-то с меньшим уровнем навыков, что обойдется дешевле. Если высокооплачиваемый системный администратор тратит час в день на замену лент – это пустая трата денег. Даже если клерку для выполнения данной задачи потребуется вдвое больше времени, это будет дешевле, потому что за это время опытные системные администраторы смогут работать над задачами, которые могут выполнить только они. Вот почему руководители корпораций не отправляют факсы сами[1]. Для бизнеса лучше, чтобы руководители занимались тем, что могут делать только они, а другие задачи передали менее высокооплачиваемым сотрудникам.

---

[1] Человек в заднем ряду, заявляющий, что многие руководители не умеют пользоваться факсом, может сесть.

Единственное, что хуже отсутствия автоматизации, – это плохая автоматизация. При плохой автоматизации многие аспекты задачи автоматизируются, но объемы умственной работы, которая должна быть выполнена, не уменьшаются. Хорошая автоматизация не просто выполняет за вас работу, она снижает объем умственной деятельности, которой вы должны заниматься.

Система резервного копирования, которая требовала умственной деятельности

Однажды системному администратору пришлось иметь дело с системой резервного копирования, которая автоматизировала основные аспекты поставленной задачи и даже печатала красивые метки на кассетах. Однако система не уменьшала умственный аспект работы. Программа выполняла огромную работу по вводу требуемых команд по резервному копированию в нужное время, применяла динамический график для оптимизации использования ленты и справлялась с имеющимися вопросами безопасности и политики, что имело побочный эффект, требуя около десяти небольших приводов для лент в главном информационном центре и еще десяти, распределенных по лабораториям во всем здании (это было до того, как накопители с автоматической сменой лент стали недорогими). Однако каждое утро системному администратору, который отвечал за резервное копирование, требовалось просмотреть 20 сообщений электронной почты, по одному для каждого привода, и решить, имеется ли на каждой ленте достаточно свободного места для резервных копий следующего дня. Для того чтобы сменить ленту, запускалась программа и затем, гораздо позже, извлекалась лента. В результате выполнение ежедневных замен ленты требовало одного-двух часов. Системный администратор, будучи ленивым, не хотел каждый день думать о 20 лентах и принимать решение для каждой из них. Он знал, что устранение этой ежедневной задачи даст 5–10 ч дополнительного времени на другие проекты.

Его решение было основано на понимании того, что он мог купить больше лент, но не мог купить больше времени. Он заметил, что ленты в приводах, подключенных к крупным серверам, нужно было менять часто, тогда как ленты в приводах, распределенных по лабораториям, редко требовали замены. Вместо того чтобы каждое утро тратить час на выяснение, какие ленты должны быть заменены для оптимизации использования лент, прекращения мирового голода и поиска лекарства от рака, он просто перестал менять ленты по вторникам и четвергам. Это дало ему около четырех часов. Если новая лента начинала использоваться в понедельник, среду и пятницу, риск заполнить ее на следующий день был довольно низким. Он не заметил эту закономерность раньше, потому что не уделил время такому подробному изучению логов. Полученное время было бы более ценным, чем случайная ситуация заполнения ленты и потери резервной копии. Затем он определил, что ленты в приводах лабораторий заполнялись очень редко, и перестал делать большой обход для замены лент во всех приводах лабораторий, кроме одного раза в неделю. Это принесло около 3 ч. За счет реструктуризации выполнения замены лент он получил дополнительный день[1] в неделю.

[1] Сумма 4 + 3 – это восьмичасовой рабочий день, если 3 ч имеют большую ценность.

Используемое программное обеспечение было собственной разработки, и его было политически трудно заменить, пока автор не покинул группу, что он в конце концов сделал. До этого такой новый процесс реально экономил время. На самом деле новую процедуру было так легко объяснить другим, что системные администраторы смогли передать этот процесс клерку, устранив таким образом эту задачу из своей ежедневной нагрузки. Победа!

Ручное резервное копирование и программы резервного копирования собственной разработки были раньше очень распространены. Отслеживание новых технологий, оборудования и операционных систем обходилось дорого. Однако чем сложнее становятся требования по резервному копированию, тем больше у вас причин купить коммерческую программу, а не пытаться создать свою систему. При использовании коммерческих программ стоимость их разработки и поддержки распределяется по всей пользовательской базе.

Автоматизированное резервное копирование позволяет передать его другим

Наш хороший друг, Адам Московиц (Adam Moskowitz), принял решение создать систему резервного копирования, которая была настолько автоматизированной, что он мог бы передать ежедневную работу секретарше своей компании, по крайней мере на бóльшую часть времени. Каждый день система отправляла ей и Адаму по электронной почте сообщение о состоянии резервного копирования предыдущей ночью. Сообщение включало указания о том, какие ленты нужно было заменить, или информировало о проблеме, которую Адам должен был исправить. Адам автоматизировал все больше и больше ситуаций ошибок, поэтому со временем ему приходилось выполнять все меньше и меньше работы. Вскоре без необходимости вмешательства Адама могли проходить месяцы.

26.1.10. Централизация

Другая фундаментальная задача по созданию современной системы резервного копирования – это централизация. Резервное копирование должно быть централизованным, потому что оно дорого и важно. Правильные вложения могут распределить стоимость системы резервного копирования и восстановления по многим системам.

За счет централизации можно сократить два основных типа расходов. Замена ленты является дорогостоящей, потому что это трудоемкая работа. Само оборудование стоит дорого, потому что содержит прецизионные механические элементы, вращающиеся на высоких скоростях. Допустимость ошибки низкая.

Без централизации привод для ленты должен подключаться к каждой машине, которой требуется резервное копирование, а иногда нужно оплачивать обход каждой машины для замены лент. В результате получается оплата большого количества дорогого оборудования и физической работы.

Сетевые системы резервного копирования позволяют вам подключать крупную технику резервного копирования к одному или нескольким узлам, которые для начала резервного копирования связываются с другими. Сетевое резервное копирование было признано сразу же, когда сети стали избыточными и надежными.

Приводы с автоматической заменой лент содержат десятки, сотни или даже тысячи лент и роботизированные манипуляторы, которые извлекают ленты из мест их хранения и помещают в один из нескольких блоков для ленты. Такие устройства дорогие, но их стоимость распределяется по всем системам, для которых они выполняют резервное копирование, а расходы на трудовые ресурсы сильно снижаются. Приводы для лент являются механическими и часто ломаются. Соответствующее программное обеспечение может обнаружить сломанный блок загрузки ленты и просто использовать оставшиеся блоки в устройстве для завершения задач. Без сетевых систем резервного копирования вы должны либо отказаться от резервного копирования системы, если ее привод для ленты сломался, либо установить на каждую систему дополнительный привод для ленты, чтобы обеспечить непрерывную работу хотя бы одного из приводов. Естественно, привод с автоматической заменой лент дешевле! Кроме того, эти устройства обеспечивают большую часть развитой автоматизации, рассмотренной в этой главе.

26.1.11. Инвентаризация лент

Куча лент с резервными копиями без индексов или списка лишь немногим полезнее, чем полное отсутствие резервных копий. Инвентаризация критически важна для возможности своевременно выполнять восстановление. Крупные автоматизированные системы резервного копирования ведут эту инвентаризацию в сети. Часто для резервного копирования описи нужно предпринимать специальные меры, потому что система, выполняющая резервное копирование, захочет обновить опись после ее копирования. Вы можете печатать минимальный указатель лент после ночного резервного копирования и хранить эти распечатки в журнале. Инвентаризация – подходящая кандидатура для хранения в системах, защищенных RAID или подобными технологиями.

Возможность восстановления файлов зависит от качества вашей инвентаризации. Чем лучше инвентаризация, тем быстрее можно выполнить восстановление. Если бы инвентаризации не было, вам пришлось бы читать ленты в хронологическом порядке, пока необходимые данные не были бы найдены. Если в инвентаризации указано только, какие разделы на каких лентах находятся, вам придется читать каждую ленту с данными нужного раздела, пока вы не найдете запрашиваемый файл. Если пользователь помнит время последнего изменения файла, это может помочь в поисках, но они все равно потребуют длительного времени. Полные восстановления будут не такими трудоемкими.

Если система хранит пофайловую опись каждой ленты, весь процесс поиска может быть быстро выполнен при помощи запросов к базам данных, а затем будут загружены точно необходимые ленты. Например, если нужно восстановить пару файлов в различных директориях и пару директорий целиком, программа может точно определить, в каких полных и инкрементальных резервных копиях есть эти данные. Все необходимые ленты будут загружены в привод, и программа выполнит восстановление при помощи всех доступных блоков загрузки ленты в приводе.

Хранение пофайловой инвентаризации требует много дискового пространства. Некоторые коммерческие продукты позволяют найти равновесие, поддерживая

пофайловую опись для недавних лент и простую опись разделов для всех остальных. При необходимости восстановления более старых файлов пофайловый список может быть восстановлен по запросу.

Программа должна иметь возможность перестроить инвентаризацию в случае ее потери или уничтожения. Теоретически у вас должна быть возможность загрузить в привод самые недавние ленты, щелкнуть по кнопке и через несколько часов или дней получить перестроенную инвентаризацию. Можно выполнять резервное копирование ночью, а восстановление инвентаризации – днем.

Хорошая инвентаризация также должна отслеживать, как часто перезаписывается конкретная лента. Большинство технологий хранения на лентах становятся ненадежными после определенного количества перезаписей. Вы должны предусмотреть для программы резервного копирования возможности сообщить вам, когда нужно уничтожить ленту.

В экстренных ситуациях вам может понадобиться восстановление без доступа к инвентаризации, без доступа к серверу лицензий и без полностью работоспособной системы резервного копирования. Несмотря на то что хорошая инвентаризация критически важна для нормальной работы, убедитесь, что система не мешает вам читать данные с лент, когда у вас нет ничего, кроме ленты и инструкции. Изучите все эти возможности при выборе решения для резервного копирования и восстановления.

26.2. Тонкости

Теперь, когда мы рассмотрели основы надежной, развитой системы резервного копирования и восстановления, нужно позаботиться о некоторых тонкостях, чтобы эффективно поддерживать систему в будущем. Во-первых, вы должны проводить проверочные восстановления, чтобы убедиться, что система работает. Хранение лент вне офиса обеспечивает лучшую защиту носителей с резервными копиями, над созданием которых вы так усердно работали. Мы завершим обсуждение техническим, но в какой-то степени философским объяснением того, почему система резервного копирования всегда на шаг отстает от нужд модернизации.

26.2.1. Пробное восстановление

Единственное время, когда вы можете проверить качество носителей для резервного копирования, – это когда вы выполняете восстановление. Обычно это наихудшее время, чтобы узнать о проблемах. Вы сможете лучше оценить свою систему резервного копирования, если периодически будете проводить пробное восстановление. Выберите случайный файл и восстановите его с ленты, чтобы проверить, как работает этот процесс.

Автоматизированные запросы на пробное восстановление

Первый раз, когда Том увидел пробное восстановление резервной копии, он работал с Томми Рейнгольдом (Tommy Reingold) в Bell Labs. Томми написал небольшую программу, которая выбирала сервер случайным

образом, затем выбирала произвольный файл и отправляла системному администратору по электронной почте сообщение, запрашивая копию этого файла в том виде, в каком он был неделю назад. Администратор мог спокойнее спать по ночам, зная, что эти еженедельные запросы успешно выполнялись.

Может быть полезно периодически выполнять пробное восстановление всего диска. Скорость, с которой может быть восстановлен весь диск, часто неизвестна, потому что это требуется очень редко. Восстановление файла или даже директории файлов, которое регулярно требуется пользователям, не поможет вам определить, сколько времени займет восстановление всего диска, из-за значительной разницы в количестве восстанавливаемых данных. Узкие места не будут обнаружены, пока не произойдет экстренный случай. Лучше время от времени выполнять восстановление целого диска, чем обнаружить проблему, когда вам потребуется срочно вернуть систему в рабочее состояние. При выполнении таких пробных восстановлений важно отслеживать их время и такие показатели, как использование диска, ленты и сети. Если вы не видите ожидаемого быстродействия, то можете изучить собранные вами статистические данные, чтобы определить, что нужно улучшить.

Если вы считаете, что у вас недостаточно свободного места для пробного восстановления полного диска, вы можете захотеть сделать это при установке нового сервера, прежде чем вводить его в эксплуатацию. У вас должен быть по крайней мере один свободный раздел, и пробное восстановление будет хорошей проверкой для нового оборудования.

Если некоторые ленты хранятся вне основного местоположения компании, пробное восстановление должно включать использование лент как внутреннего, так и внешнего хранилища, чтобы полностью проверить систему.

Человек, проверяющий правильность данных, полученных в ходе пробного восстановления, не должен быть тем же самым человеком, который отвечает за резервное копирование. Это поддерживает сбалансированность и контролируемость системы.

26.2.2. Резервные носители и внешнее хранение

Ленты с резервными копиями должны храниться в безопасном месте. Бессмысленно тратить много времени и денег на системы безопасности для защиты своих данных и при этом хранить ленты с резервными копиями в незапертой комнате или шкафу. Ваши резервные копии – это драгоценности вашей компании. В современных тесных офисных зданиях может быть трудно найти безопасное и удобное пространство для их хранения. Однако для этого достаточно нескольких надежно запираемых шкафов или большого сейфа в небезопасной комнате.

Если ваши резервные копии нужно оградить от риска стихийного бедствия, которое может уничтожить всю вашу серверную, они не должны храниться в серверной или в комнате, которая будет затоплена, если в вашем информационном центре прорвет трубу.

Внешнее хранение резервных носителей даже лучше. Набор лент с резервными или архивными копиями хранится на безопасном расстоянии от компьютеров, на которых они были созданы. Это необязательно будет дорого или сложно.

Резервные носители или их копии можно хранить вообще в другом здании. Это компромисс удобства и риска. Хранение копий исключает риск того, что ленты могут быть повреждены или утеряны при транспортировке. Однако создание дополнительных копий может быть трудоемким. Вместо этого вне организации обычно хранятся сами ленты. Это влияет на вашу возможность оперативно выполнять восстановление. Вы можете предпочесть хранить вне организации полные резервные копии за последний месяц, так как увидите, что большинство запросов на восстановление касается резервных копий текущего месяца, а пользователи должны понимать, что восстановление с лент, которые хранятся дольше 30 дней, но меньше 60, может предполагать задержку.

При выборе места для внешнего хранения рассмотрите те же самые факторы, которые должны учитываться при хранении внутри организации: является ли место безопасным? У кого есть доступ к хранилищу? Какие действуют политики, гарантии или соглашения о конфиденциальности? Для хранения есть много мест, от неофициальных систем до крупных коммерческих служб хранения электронной информации.

Неофициальное внешнее хранение

В некоторых ситуациях достаточно неформальной политики. В одной начинающей компании было такое правило: каждую среду начальница отдела обработки данных забирала домой ленты с резервными копиями старше недели. На следующей неделе в среду утром она приносила ленты, которые забирала домой на прошлой неделе. Одной из проблем было то, что в случае ее попадания в автомобильную аварию ленты могли быть уничтожены. Риск можно было снизить, увеличив цикл до месяца, и полностью исключить, если бы она отвозила домой только копии лент. Другой проблемой была безопасность ее дома. Компания привезла в ее дом несгораемый сейф для хранений лент. Сейф был надежно укреплен, поэтому его невозможно было украсть.

Многие компании пользуются внешними службами хранения записей. Раньше они была роскошью, которой пользовались только крупные финансовые компании, но теперь это крупный рынок, который служит всем. Эти службы забирают и завозят ленты, возвращают конкретные ленты по запросу со сроком выполнения 4 или 8 ч и т. д. Несмотря на то что на первый взгляд их стоимость может показаться слишком высокой, они решают множество проблем. Они также могут предоставить предложения по распространенным политикам, которые компании используют для внешнего хранения. Они даже выдают милые маленькие коробочки с замком, чтобы класть туда ленты, готовые к отправке.

При внешнем хранении лент возникают вопросы безопасности. Сторонняя компания, которой платят за хранение лент, должна быть должным образом обустроена и застрахована. Внимательно прочитайте контракт, чтобы разобраться с кругом обязательств компании. Вы обнаружите, что он неутешительно мал по

сравнению с ценностью данных на лентах. Страшные истории – правда. Мы получали из служб хранения ленты других людей. В одном случае мы не смогли получить ленту, которая была отправлена им на хранение, и нам пришлось запросить ленту с предыдущей резервной копией этого файла. Автор файла был расстроен.

Важно отслеживать, какие ленты были отправлены, и записывать каждую ленту, полученную назад. Проверяйте перемещение лент и следите за ошибками, ошибки являются показателем общего качества. Это может стать вашей лучшей защитой. Представьте, что вы не можете получить важную ленту, а затем узнаете у своих операторов, что вам случайно отдали не те ленты. Ищите ленты, которые должны были быть возвращены, но не были, ленты, которые не должны быть возвращены, но были, и ленты из других компаний, пришедшие к вам. Если вы собираетесь пожаловаться поставщику услуг, важно иметь письменный протокол всех ошибок, совершенных в прошлом. Очевидно, что, если эти ошибки не являются крайне редкими, вам нужно сменить поставщиков услуг.

Собственное внешнее хранение

Компании с несколькими зданиями могут создать свои собственные системы внешнего хранения. Сотрудники одного подразделения компании были распределены по двум зданиям, которые отстояли друг от друга на 40 миль. Люди регулярно обменивались лентами. Так как они все находились в одном подразделении, они могли даже выполнять быстрое восстановление по своей корпоративной сети, если ждать доставки 1–2 ч было неразумно.

Сетевое внешнее резервное копирование

В одном исследовательском центре в Нью-Йорке между двумя подразделениями был канал связи с большой пропускной способностью, и там обнаружили, что ночью он практически не использовался. В течение нескольких лет подразделения выполняли друг для друга резервное копирование через этот канал WAN. У такого резервного копирования было преимущество внешнего хранения всех лент. Пропускная способность канала между подразделениями была достаточно большой, чтобы время восстановления не превышало разумных пределов. Руководство считало приемлемым риском допущение, что оба здания не будут уничтожены одновременно.

По мере того как пропускная способность сетей дешевеет, выполнение резервного копирования в других местах по сети становится более экономически оправданным. В структурах, предоставляющих доступ в Интернет, выросли коммерческие службы резервного копирования для обслуживания нужд интернет-компаний. Это легко, потому что там можно разместить высокоскоростные сети. Так как пропускная способность дешевеет, а технологии резервного копи-

рования по сети становятся более надежными, безопасными и популярными, можно ожидать даже большего распространения таких услуг.

Системы резервного копирования через Интернет

Когда Тому было 13 лет, он считал резервное копирование через сеть хорошей идеей, но был разочарован, когда понял, что резервное копирование его дискет емкостью 160 Кб через его модем на 300 бод займет несколько часов. Когда благодаря кабельным модемам и xDSL был открыт домашний высокоскоростной доступ в Интернет, появились компании, которые предоставляли услуги резервного копирования через сеть. Даже без высокоскоростного доступа эти услуги очень удобны для резервного копирования небольших объектов, например диссертации аспиранта. Том начал осуществлять резервное копирование данных своего персонального компьютера при помощи одной из этих служб, как только у него дома появился доступ через кабельный модем, чтобы подтвердить актуальность своей изобретательности в 13 лет.

26.2.3. Базы данных высокой доступности

Некоторые приложения, например базы данных, имеют особые требования к успешности резервного копирования. База данных управляет своим пространством и оптимизирует его под конкретные типы доступа к ее сложным наборам таблиц данных. Из-за того что размещение и методы доступа к данным обычно недоступны программам резервного копирования, база данных записывается на ленту как единый блок, или файл. Если данные в этом файле изменяются при записи, информация может быть потеряна или повреждена, так как записи о размещении данных на ленте с резервной копией могут отсутствовать либо быть неправильными. Базы данных часто требуется закрывать для обеспечения целостности, чтобы во время резервного копирования не происходило транзакций.

Если у базы данных высокие требования к доступности, неприемлемо каждую ночь отключать ее для резервного копирования. Однако риски, связанные с отсутствием резервного копирования во время работы базы данных, также неприемлемы. Некоторые разработчики программ резервного копирования предлагают модули для выполнения резервного копирования определенных баз данных. Некоторые из них значительно снижают риски, связанные с резервным копированием работающей базы данных. Однако обычно наиболее безопасно выполнять резервное копирование данных, когда база данных не работает. Часто это достигается при помощи «зеркального отражения» базы данных, например при помощи RAID 1 + 0. База данных может быть остановлена на время, достаточное для отключения зеркального раздела. Отключенные зеркальные диски находятся в целостном состоянии, не затрагиваются транзакциями базы данных и могут быть безопасно записаны на ленту. После завершения резервного копирования зеркальные диски можно снова подключить к работающей базе данных для автоматического обновления.

Во многих системах есть три копии баз данных высокой доступности: один набор дисков активно отражает базу данных, а еще один отключается, и выполняется его резервное копирование.

26.2.4. Изменения технологий

Не думайте, что найдется один-единственный тип оборудования или программного обеспечения, которым вы сможете пользоваться для резервного копирования на протяжении всей вашей карьеры системного администратора. Вместо этого начните мыслить в общих категориях и двигаться вместе с развитием технологий.

Только одно в системах резервного копирования и восстановления постоянно: технологии дисков и лент попеременно опережают друг друга, и всегда с разным темпом. Смиритесь с этим и не пытайтесь противостоять. В какие-то годы вперед вырвется технология хранения на лентах и вы будете считать, что сможете сделать резервную копию чего угодно. В следующие несколько лет вы увидите, что впереди идет технология хранения на дисках, и вы будете сомневаться, сможете ли вообще сделать резервные копии всех ваших данных. Чтобы понять, почему это происходит, рассмотрим исторические тенденции развития каждой технологии.

Размер диска растет понемногу. Каждые несколько месяцев появляются чуть бóльшие по объему диски. Общий объем диска удваивается каждые 15–18 месяцев, и так исторически складывается, что приложения довольно быстро находят применение всему доступному пространству. Это означает, что примерно каждый следующий год вы будете выполнять резервное копирование дисков, содержащих вдвое больше данных.

Емкость лент росла более широкими шагами, но они продолжались по несколько лет, а не месяцев. Потребители менее охотно модернизируют оборудование резервного копирования на ленты, поэтому отрасль предлагает модернизацию с полной заменой оборудования каждые 2–3 года. Сопротивляйтесь призывам модернизировать ваше оборудование слишком часто – вы упростите себе жизнь, отказавшись от необходимости разбираться с большим количеством различных форматов лент. Большинство компаний склонны пользоваться главным образом тем, что было самой совершенной технологией, когда устанавливалась их система, и могут иметь пару старых систем на старой платформе. Эти старые системы либо еще не были модернизированы, либо скоро будут выведены из эксплуатации, и модернизация технологии записи на ленты была бы пустой тратой денег. Кроме того, они хранят 1–2 привода для ленты всех предыдущих технологий, которые еще есть в их архивах.

Оставьте один привод для девятидорожечной магнитной ленты

Вот способ заслужить всеобщее уважение и признательность. Системный администратор одной крупной компании обнаружил, что он был единственным человеком в главном комплексе, который умел читать старые девятидорожечные ленты для катушечных приводов. Хотя читать такие ленты требовалось редко, каждый, кому это было нужно, приходил в отчаяние. Сторонние компании переводили ленты в другой формат за очень большие деньги, и системный администратор знал, что компания не захочет столько платить. Он поставил привод для ленты там, где ему было удобно, чтобы посетители могли им пользоваться, и подключил его к машине, на которой он мог создать гостевые учетные записи. Благодаря этому он каждый год приобретал пару новых благосклонных покро-

вителей, которые оказывались полезны ему в дальнейшем. Это также помогло ему приобрести репутацию хорошего парня, что в крупной компании может быть более ценным, чем кажется на первый взгляд.

Неравномерное развитие технологий хранения на дисках и на лентах влияет на то, как вы можете выполнять резервное копирование. Раньше было очень сложно разделить резервное копирование одного раздела по двум лентам[1]. Большинство программ резервного копирования разрабатывалось своими силами, а ленты были маленькими. Таким образом, когда ленты QIC вмещали 150 Мб, системные администраторы разделяли диски на разделы по 150 Мб. Затем стали популярны 8-мм ленты с емкостью 2,5 Гб, потому что размер дисков обычно составлял 0,5–1 Гб. Системные администраторы подумали, что проблемы с несоответствием размеров дисков и лент закончились, диски с данными могли состоять из одного большого раздела. Переход на 8-мм ленты емкостью 5 Гб произошел примерно в то же время, когда емкость диска выросла до 4 Гб. Однако, когда наступил следующий этап роста емкости дисков (9 Гб), ленты не успели за ними. Это затормозило продажи больших дисков, и наступило очень благоприятное время для развития индустрии коммерческих программ резервного копирования, которая смогла вложить средства в создание приводов с автоматической сменой лент и справиться со сложной задачей разделения резервных копий на несколько лент. Затем появились ленты технологии DLT, на которых могло храниться 70 Гб, что снова превосходило размеры дисков. И история повторилась, когда размер дисков превысил 70 Гб.

Какой из этого следует вывод? Изменения постоянны. Верьте в то, что производители обеспечат рост в обеих областях, но не удивляйтесь, когда он становится несинхронным.

26.3. Заключение

Эта глава о восстановлении данных, для которого неизбежно требуется резервное копирование. Этот вопрос определяется политикой. Мы постоянно удивляемся, находя компании, чьи системы резервного копирования не основаны на целесообразной политике.

Есть три типа запросов на восстановление: случайное удаление файлов, восстановление после поломки дисков и просмотр архивных данных. Для них характерны различные SLA, ожидания пользователей и технические требования. Что более важно, каждый тип восстановления требуется разным группам пользователей и вы можете захотеть тарифицировать их отдельно. Политика устанавливается на основе этих параметров.

После создания политики все решения принимаются легко. На основе политики вы можете разработать график резервного копирования, который точно определит, когда для каких систем будет выполняться резервное копирование. Один из наиболее сложных элементов составления графика – решить, сколько дней инкрементального резервного копирования должно пройти перед очередным полным резервным копированием. Современные программы выполняют

[1] Это до сих пор может быть рискованно, большинство систем индексируют только первую ленту.

такие вычисления и могут создавать динамические графики. Политика помогает вам планировать время, емкость, расходные материалы и другие аспекты. Сообщение о политике пользователям помогает им получить представление о безопасности своих данных, узнавать, для каких систем не выполняется резервное копирование, и понимать процедуру, которую они должны выполнить, если им нужно восстановление данных. Важно сообщать пользователям, для каких систем не выполняется резервное копирование.

Современная система резервного копирования должна быть автоматизирована для минимизации человеческой работы, человеческого интеллектуального труда, человеческих решений и человеческих ошибок. Раньше резервное копирование было значительной частью работы системного администратора и затраты на его выполнение большого количества времени системного администратора было оправданным. Однако сейчас системные администраторы имеют много других обязанностей. Резервное копирование – это четко определенная задача, которая может и должна передаваться другим. Мы передаем разработку программ коммерческим разработчикам. Мы передаем ежедневные процедурные вопросы клеркам. Мы можем даже передать простое восстановление пользователям, которым оно требуется. Вместо этого мы уделяем свое время проектированию архитектуры, установке систем и решению периодически возникающих вопросов расширения. Передача этой работы другим людям оставляет нам больше времени на другие задачи.

Современные системы резервного копирования являются централизованными. Выполнение резервного копирования по сети на центральном крупном устройстве экономит силы. Стоимость больших приводов с автоматической сменой лент распределяется по количеству машин, которые они обслуживают.

В хорошо организованных системах резервного копирования есть отличные системы инвентаризации. В системе должна иметься хорошая опись файлов, чтобы восстановление можно было выполнять быстро, и хорошая опись лент, чтобы они перезаписывались по графику.

Мы также выяснили, что резервное копирование требует больших затрат как на оборудование, так и на расходные материалы. В разделе 10.1.2 рассмотрены экономические подходы, которыми вы можете воспользоваться для снижения риска.

Технологии резервного копирования все время меняются. По мере роста емкости жестких дисков системные администраторы должны совершенствовать свои возможности по резервному копированию. Они должны отказаться от убеждения, что любая установленная ими система резервного копирования и восстановления является окончательным решением. Напротив, они должны быть готовы постоянно ее расширять и заменять каждые 3–5 лет.

После построения основ можно обратиться к некоторым тонкостям. Во-первых, правильность резервного копирования должна проверяться при помощи пробных восстановлений. Для этого выберите случайные данные и проверьте свою возможность успешно восстановить их. Во-вторых, должно быть обеспечено безопасное внешнее хранение резервных носителей. Резервные копии не должны храниться в том же месте, что и компьютеры, с которых они сделаны.

Восстановление – это одна из наиболее важных услуг, которые вы предоставляете своим пользователям. Невозможность восстановить критические данные может привести вашу компанию к банкротству. Безупречное выполнение восстановления может сделать вас героем в глазах всех окружающих.

Задания

1. Какова ваша политика восстановления? Приходится ли вам работать с корпоративными инструкциями? Если да, то в чем они заключаются? Или ваша политика создается локально?
2. В табл. 26.1 и 26.2 не учитывается тот факт, что ленты обычно меняются каждый день вне зависимости от того, полные они или нет. Почему эти примеры все равно статистически справедливы? Почему размещение резервных копий различных дней на одной ленте может быть плохой идеей?
3. Системы инкрементального резервного копирования некоторых разработчиков записывают только те файлы, которые изменились с последнего инкрементального резервного копирования. Как это влияет на выполнение восстановления? Каковы достоинства и недостатки такого подхода?
4. Терминология разработчиков об «инкрементальных» резервных копиях различается. Какой тест вы создали бы, чтобы узнать, какой вариант реализовал разработчик? Выполните этот тест в двух различных ОС.
5. Каковы преимущества и риски использования системы резервного копирования, которая может продолжить запись на вторую ленту, если первая лента заполняется?
6. В примере в разделе 26.1.7 мы предположили, что ленты могут перезаписываться бесконечно. Допустим, что ленту можно переписать 15 раз, а затем она уничтожается. Подсчитайте, сколько лент вам придется уничтожать каждый год из первых четырех лет примера.
7. В разделе 26.1.7 не подсчитано, сколько денег будет потрачено на чистящие ленты. Предположим, приводы надо чистить каждые 30 дней, а чистящую ленту можно использовать 15 раз. Подсчитайте, сколько чистящих лент потребуется для двух примеров из раздела 26.1.7.
8. В разделе 26.1.7 предполагается, что количество данных, для которых выполняется резервное копирование, не изменяется за четыре года. Это нереально. Повторите расчеты в этом разделе, основываясь на предположении, что количество данных удваивается каждые 18 месяцев.
9. В разделе 26.1.7 указана четкая схема повторного использования лент. А если новые ленты можно повторно использовать только 10 раз? Если ленты, которые сохраняются навсегда, обязательно должны быть новыми?
10. Какие аспекты вашей нынешней системы резервного копирования и восстановления должны быть лучше автоматизированы?
11. «Современная система резервного копирования должна быть автоматизирована для минимизации человеческой работы, человеческого интеллектуального труда, человеческих решений и человеческих ошибок». В чем смысл этого утверждения?

Глава 27

Служба удаленного доступа

Служба удаленного доступа предоставляет авторизованным лицам способ доступа к сети компании из дома, иного местонахождения пользователей и других мест в стране, на континенте или в мире. Раньше эта служба была нужна некоторым техническим специалистам, чтобы выполнять часть работы дома вне нормального рабочего графика. В последнее время она стала базовой службой, которой пользуются все в компании. Теперь удаленные сотрудники и коммивояжеры работают вне офиса, подключаясь только для особых служб.

Удаленный доступ может предоставляться многими способами, но есть две основные категории. При некоторых способах компьютер подключается напрямую к сети: телефонные модемы, ISDN и т. п. Другие способы предполагают подключение к Интернету – WiFi, кабельные модемы, DSL, Ethernet и т. д., – а затем подключение к сети через туннель или VPN.

Удаленный доступ связан с множеством проблем. Один из аспектов удаленного доступа заключается в том, что люди хотят иметь возможность проверять свою электронную почту и осуществлять доступ к данным, когда они в пути. Почти так же распространено желание людей работать из дома по вечерам, выходным, несколько дней в неделю или все время. Еще один аспект – некоторые пользователи практически постоянно находятся в каком-либо удаленном местоположении, но им все же нужен регулярный доступ к корпоративной сети. В данной главе показано, что эти три аспекта имеют немного разные требования, но также много общего.

Удаленный доступ – это одна из областей, в которых технологии постоянно меняются. В данной главе рассмотрено, как это влияет на проектирование и администрирование службы удаленного доступа, но не обсуждается, какими технологиями пользоваться, потому что они изменятся даже между написанием и изданием книги. Информация в данной главе должна предоставить вам основу для оценки текущих технологий и методов и принятия архитектурных решений.

27.1. Основы

Для создания службы удаленного доступа вам нужно начать с понимания большого количества разных требований ваших пользователей. Вы также должны решить вместе со своими пользователями, какие уровни обслуживания системные администраторы будут предоставлять по различным аспектам системы, и документировать эти решения для справки в будущем.

Когда вы определите требования и уровни обслуживания, вы будете готовы создавать службу или не создавать ее. Один из основных принципов создания службы удаленного доступа – по возможности передать ее сторонним исполнителям. Однако несколько компонентов должно строиться или управляться изнутри компании. В частности, изнутри должны контролироваться аспекты безопасности аутентификации, авторизации и поддержания безопасности периметра.

27.1.1. Требования к удаленному доступу

Первое требование к службе удаленного доступа, скорее всего, будет предполагаться само собой и не указываться в явном виде: для каждого должно быть реализовано дешевое и удобное решение по удаленному доступу. Если группа системных администраторов не предоставит его, пользователи сами сделают для себя что-нибудь, что не будет таким безопасным или эффективно управляемым, как служба, которую предоставили бы системные администраторы. Довольно вероятно, что от системных администраторов будут ожидать поддержки службы, которую разработали их пользователи, если с ней возникнут проблемы. Кроме того, обычно эту службу будет сложнее поддерживать, чем созданную системными администраторами.

Другие требования основаны на том, как пользователи намерены применять систему удаленного доступа. Наиболее распространенные пользователи удаленного доступа – это люди, которые путешествуют и хотят проверять или отправлять электронную почту. Другая распространенная категория пользователей – люди, которые хотят зайти в систему вечером на час или два и разобраться в чем-то. У этих разных групп пользователей есть кое-что общее: все они пользуются удаленным доступом в течение довольно коротких промежутков времени. Они отличаются в том, что одна группа ожидает возможности пользоваться службой отовсюду, а другая – пользоваться ею дома. Обеим группам требуется надежный и экономичный способ кратковременного подключения к офисной сети. Ни одной из групп не нужна очень высокая пропускная способность, но обе хотят получить максимально возможную. Они отличаются в том, что людям, которые путешествуют, нужна возможность подключаться из любого места, где они могут оказаться. В зависимости от компании это может быть небольшая территория или весь мир. Для предоставления глобального удаленного доступа технология должна быть повсеместно распространенной. При создании системы удаленного доступа для таких пользователей важно, какая территория покрытия необходима для службы и какова модель оплаты для различных регионов.

Если люди хотят регулярно работать дома, нужно учесть три основных принципа. Во-первых, отключения будут значительно влиять на повседневную работу этих людей, поэтому служба должна быть надежной. Во-вторых, им потребуется высокоскоростной доступ, потому что скорость соединения будет влиять на их ежедневную производительность и обычно они будут выполнять задачи, которые требуют более высокой пропускной способности и/или меньшего времени ответа. Наконец, экономические факторы отличаются от кратковременного периодического использования. Человек, который работает дома, обычно пользуется службой удаленного доступа 8–10 ч в день. Поминутная оплата при таком использовании быстро растет, поэтому безлимитное подключение может быть дешевле.

Часто сотрудники компании могут захотеть пользоваться высокоскоростным подключением к Интернету, к которому у них есть доступ, на конференции или дома. Эта ситуация особенно распространена в технических компаниях и часто требует технологии, сильно отличающейся от тех, которые нужны для выполнения ранее описанных требований. Здесь нужно использовать шифрование между компьютером сотрудника и корпоративной сетью, потому что, если конфиденциальная информация компании передается через общедоступный Интернет, ее могут перехватить. Также передача информации через Интернет в незашифрованном виде может, в правовых терминах, считаться публикацией информации, что вызовет потерю компанией прав на интеллектуальную собственность. Кроме того, передача через Интернет незашифрованных паролей является верным способом стать жертвой взлома. Обычно на стороне сервера этого зашифрованного соединения находится часть корпоративного брандмауэра. Механизм шифрования должен обеспечивать доступ ко всему, что нужно человеку в корпоративной сети, быть надежным и иметь достаточно высокую производительность.

Также служба должна удовлетворять потребности людей, которым нужен доступ к корпоративной сети из другой компании, например инженеров по поддержке или консультантов, работающих в местоположении клиента. Этот сценарий вводит дополнительную сложность объединения политик, безопасности и практических вопросов двух, возможно, несвязанных компаний. Обычно эти люди не в том положении, чтобы требовать чего-то от клиента, поэтому им нужна возможность работать с существующими ограничениями, а не пытаться менять политики безопасности или правила брандмауэра. Как правило, создание какого-либо постоянного подключения на рабочем месте человека в местоположении клиента является неприемлемым решением для обеих компаний, потому что человеку нужен доступ к обеим сетям и он может случайно связать их. Иногда приемлемо проведение к рабочему месту аналоговой линии, но это бывает редко. Обычный метод предполагает создание зашифрованного канала между машиной человека и брандмауэром компании, который проходит через брандмауэр клиента и Интернет. Это значит, что вам нужно предоставить механизм удаленного доступа, который, скорее всего, сможет проходить через большинство брандмауэров и который не слишком сложно добавить в брандмауэры, не позволяющие ему проходить[1]. Кроме того, он должен быть достаточно гибким, чтобы человек мог осуществлять доступ ко всему, что ему нужно в корпоративной сети. Часто это не так легко, как может показаться, потому что некоторые приложения используют протоколы, которые трудно пропустить через некоторые механизмы шифрования, удовлетворяющие другим требованиям. Чтобы найти продукты, которые будут работать, может потребоваться поискать какие-то компромиссы между различными требованиями. В идеальном случае в этой ситуации должна быть возможность пользоваться тем же самым программным обеспечением, которое было выбрано для описанной ранее ситуации с высокоскоростным подключением и отсутствием брандмауэра, но это может не получиться. Предоставление удаленного доступа этим людям часто является самой трудной задачей, особенно потому, что в каждом местоположении клиента будут различные политики безопасности, которые нужно соблюдать, чтобы не оказаться в неловкой ситуации.

---

[1] Новый протокол не очень трудно добавить, если он использует только один TCP-порт и не имеет проблем безопасности на стороне клиента, например не позволяет создавать обратное туннельное подключение к сети клиента по открытым соединениям.

Из-за различных требований, соблюдения которых могут ожидать от служб удаленного доступа, последние обычно состоят из нескольких компонентов – каждый из них поддерживает одну или более описанных выше групп людей.

27.1.2. Политика удаленного доступа

Прежде чем начинать предоставление удаленного доступа, компания должна определить его политику. Она должна определять допустимое использование службы, правила безопасности, которые ее касаются, а также обязанности тех, кто ею пользуется. Кроме того, в политике должно быть указано, кто получает какой тип удаленного доступа и кто за это платит. В разделе 11.1.2 политика удаленного доступа и другие политики безопасности рассмотрены более подробно.

27.1.3. Определение уровней обслуживания

Важно четко определить уровни обслуживания различных служб удаленного доступа вместе с пользователями этих служб. Удаленный доступ может быть чувствительной областью, потому что сбои обнаруживаются людьми, которые хотят выполнить какую-то работу и не могут ничего сделать, пока служба не будет восстановлена. Это раздражает их и может сделать проблемы очень заметными. Если уровни обслуживания четко определены, доведены до пользователей и поняты ими до возникновения проблем, пользователи будут знать, на какое приблизительное время ремонта (Estimated Time to Repair – ETR) они могут рассчитывать, что должно снизить уровень напряжения и раздражения.

Единственный системный администратор в небольшой компании должен добиться таких уровней обслуживания, которые позволяли бы ему хоть немного спать, чтобы нормально работать днем. В крупных организациях со службой поддержки, работающей в режиме 24/7, должны быть более ориентированные на пользователей уровни обслуживания. Персонал службы поддержки должен быть обучен работе со службой удаленного доступа и знать, когда передавать проблемы на более высокий уровень. У новых служб на пробном этапе уровни обслуживания должны быть ниже, потому что персонал службы поддержки не будет полностью обучен и только несколько старших системных администраторов будут знакомы с пробной службой. Однако у пользователей пробной службы должен быть запасной метод доступа. Службы, которые были выведены из эксплуатации и используются лишь небольшим количеством людей, также являются кандидатами на более низкие уровни обслуживания, потому что новый персонал может быть не обучен старым технологиям.

Осторожно выбирайте пользователей пробных служб

Несколько лет назад одна компания по разработке программного обеспечения представила службу высокоскоростного удаленного доступа на базе ISDN. Первым этапом этого проекта было определение оборудования, которое нужно использовать на корпоративной и домашней стороне соединения, тестирование надежности, совместимости, возможностей и расширяемости. Была определена пара вариантов для каждой стороны соединения, и их нужно было протестировать. Сетевая группа планиро-

вала задействовать в первоначальных тестах лишь нескольких системных администраторов, чтобы они могли помочь с отладкой. Однако доступа к службе потребовали несколько человек из инженерного отдела, сказав, что они создадут ее сами, если группа системных администраторов не предоставит им ее быстро. Директор группы системного администрирования объяснил инженерам, что служба скоро будет доступна, поскольку уже приступили к начальным испытаниям. Несколько инженеров, которые работали дома и которым был очень нужен высокоскоростной доступ, нашли директора инженерных подразделений и попросили его включить их в тестирование. Группе системного администрирования пришлось согласиться, чтобы инженеры не создавали свою службу. Сетевая группа четко дала понять инженерам, которые участвовали в тестировании, что эта служба еще не является полноценной и что возможны сбои в течение нескольких дней, поэтому они не должны полагаться на нее и у них должен быть запасной метод доступа. Однако спустя некоторое время один инженер, тестирующий пробную версию, столкнулся с проблемой ISDN-соединения и быстро передал ее по цепи руководства, так что она стала заявкой на устранение неисправности наивысшего приоритета, требуя у системных администраторов уделить внимание ей, а не большому количеству заявок, связанных с поддерживаемыми службами. Он не был подходящим пользователем пробной версии, потому что начал постоянно требовать высокоскоростного доступа и не хотел терпеть сбои или возвращаться к старому модемному методу доступа.

Первопричина проблемы заключалась в том, что проект развития ISDN не финансировался, пока инженеры не начали настойчиво требовать этого, что произошло более чем через год после того, как запрос на финансирование был сделан специалистом по архитектуре сетей, который прогнозировал потребность. На этом этапе было невозможно ограничить группу пробного использования подходящими людьми, что привело к большому стрессу и раздражению как системных администраторов, так и инженеров.

К сильному повышению пропускной способности легко привыкнуть. Возвращение к старой системе – это неподходящий вариант после использования более быстрого решения, вне зависимости от того, насколько ясно системные администраторы пытаются объяснить уровни обслуживания, которых можно ожидать от прототипа службы. Прежде чем давать доступ к системе первым пользователям, служба должна пройти этап первоначального прототипа и, по крайней мере, нужно определить оборудование на стороне пользователя, иначе это путь к катастрофе. Пытайтесь протолкнуть такие важные проекты в бюджет, прежде чем они станут зоной политического конфликта, даже если они не финансируются официально.

27.1.4. Централизация

Удаленный доступ – это область, которая выигрывает от централизации. С точки зрения безопасности элемент аутентификации службы удаленного доступа должен быть централизован, чтобы обеспечить нормальную проверку

и контроль доступа. С точки зрения расходов новые технологии все время развиваются, а затраты на исследование того, как лучше всего реализовать и поддерживать новую технологию, велики и не должны дублироваться в компании. Кроме того, за счет концентрации всего использования на централизованном оборудовании и линиях можно достичь значительной экономии масштаба. Окончательная форма централизации – это передача службы удаленного доступа сторонним исполнителям.

27.1.5. Привлечение сторонних исполнителей

Лучший способ справиться с постоянно изменяющимися технологиями удаленного доступа – заставить это делать кого-то еще. Бесполезно постоянно пытаться продолжать оценивать новые технологии и выяснять, как их расширять и поддерживать, только для того, чтобы через год-два перейти на более новую технологию.

Некоторые компании по предоставлению услуг удаленного доступа, обычно интернет-провайдеры, могут взять на себя хотя бы некоторые аспекты службы удаленного доступа компании. Один из способов это сделать, – установка программного обеспечения VPN на машины пользователей, которые будут набирать обычные номера модемных пулов провайдера или применять другие возможности подключения, а для соединения с корпоративной сетью использовать VPN. Другой способ заключается в использовании виртуальных каналов, которые устанавливают фильтры безопасности и перенаправляют трафик пользователей на основании их данных аутентификации. Обычно пользователи применяют модемные пулы, выделенные для этой службы у провайдера, и выделенные соединения провайдера с компанией.

Более ощутимое преимущество передачи удаленного доступа сторонним исполнителям – значительное снижение времени, которое тратится на его поддержку. Расходы становятся видимой и предсказуемой цифрой, которую можно внести в бюджет, а не скрытой переменной, не поддающейся количественной оценке. С точки зрения системного администратора, передача удаленного доступа сторонним исполнителям означает меньшее количество звонков по поддержке в нерабочее время и отсутствие необходимости искать неизвестный сломанный модем, который не дает пользователям подключиться. Некоторые компании могут справиться со всеми вопросами удаленного доступа, остальные могут решить все вопросы, кроме, например, программного обеспечения для VPN. Каждый, кому приходилось поддерживать модемный пул, согласится с тем, что желательно передать это кому-нибудь другому.

Экономия масштаба означает, что для компании, предоставляющей услуги, проще и экономически выгоднее оценивать новые технологии и их поддержку. Это элемент их главного бизнеса, поэтому проекты по оценке будут финансироваться.

Некоторые аспекты удаленного доступа не должны передаваться сторонним исполнителям. В частности, база данных аутентификации должна поддерживаться внутри компании, чтобы она могла быть включена в выходной процесс для увольняющихся сотрудников и подрядчиков, могла быть проверена и использована, чтобы незаметно и в короткие сроки обрабатывать прекращение важных отношений.

Когда компания решает передать сторонним исполнителям любой элемент компьютерной среды, системные администраторы должны внимательно выби-

рать поставщика услуг. Поставщики услуг должны оцениваться по следующим критериям:

- *Территория покрытия.* Компания, предоставляющая услуги, должна покрывать по крайней мере территории, которые нужны базе пользователей, включая дома пользователей и места, куда люди скорее всего могут поехать. Лучше всего найти поставщика услуг с глобальным покрытием и возможностью выбирать и платить за меньшие территории покрытия. При необходимости вы сможете расширить территорию покрытия. Территория может считаться полностью покрываемой, если любое подключение к службе удаленного доступа оплачивается по местным тарифам или предоставляется бесплатно для того, кто подключается, за исключением оплаты провайдеру удаленного доступа. Если вам требуется только небольшая зона покрытия, передача удаленного доступа сторонним исполнителям может быть менее выгодна.
- *Поддерживаемые технологии.* Оценка компаний, предоставляющих услуги, также включает рассмотрение технологий, которые они поддерживают, и их темпов принятия технологий на вооружение. Если они не успевают за новыми технологиями, возникнет проблема создания пользователями собственных, более быстрых систем доступа.
- *Непосредственная поддержка.* Предоставляет ли компания непосредственную поддержку или только через системных администраторов? Несмотря на то что проблемы, которые связаны с неправильной конфигурацией машин пользователей, могут быть решены внутренними системными администраторами, последние не будут так хорошо знакомы со службой, которая не была создана в компании, и не будут иметь доступа ко всем необходимым для устранения проблем элементам системы. Дополнительный уровень посредничества увеличивает время разрешения проблемы пользователя.
- *Соглашение об уровне обслуживания.* Прежде чем выбрать поставщика услуг, важно получить и оценить письменное SLA. Каково время ответа? Каковы условия неисполнения? Как вы можете отслеживать выполнение провайдером условий соглашения? Какие скорость и задержка являются стандартными и гарантируются?
- *Структура тарификации.* Какова модель и структура тарификации обслуживания? В идеальном случае все расходы должны быть включены в плату провайдеру, чтобы компании и сотрудникам не приходилось иметь дело с получением и обработкой счетов за удаленный доступ. Разберитесь, что представляют из себя все расходы и как они отличаются по областям обслуживания. Проверьте, можно ли предоставить провайдеру базу данных, в которой пользователи распределены по подразделениям, чтобы провайдер мог пользоваться ею при отдельной тарификации для каждого подразделения или, по крайней мере, предоставить компании схему распределения расходов.
- *Интерфейс аутентификации.* Проверьте, какие механизмы аутентификации поддерживаются провайдером. Он должен поддерживать несколько стандартных протоколов аутентификации и авторизации, чтобы системные администраторы могли выбрать подходящий протокол для использования со своей схемой аутентификации. Провайдер должен обеспечить средства, чтобы база данных аутентификации и авторизации управлялась компанией-пользователем.

- *Безопасность.* Группа обеспечения безопасности компании по-прежнему отвечает за ее общую безопасность, которая включает переданную сторонним исполнителям систему удаленного доступа. Персонал по обеспечению безопасности должен поддерживать связь с провайдером, чтобы обеспечить поддержание необходимого уровня безопасности архитектуры удаленного доступа, возможно, за счет реализации на стороне корпорации каких-то средств, которые работают совместно с информацией аутентификации, передаваемой провайдером. Перед выбором компании, предоставляющей услуги, выясните, какова ее архитектура безопасности и какие возможны варианты.
- *Сквозная пропускная способность.* Убедитесь, что у вас достаточная пропускная способность канала связи с точкой доступа. Мы часто видели узкие места в сети у провайдера службы или в точке его подключения к сети. Оцените пиковое количество пользователей, пропускную способность, которой каждый может пользоваться, и подсчитайте общую пропускную способность. Если вы передаете сторонним исполнителям модемный доступ, убедитесь, что ваша выделенная линия к провайдеру модемного доступа имеет достаточную пропускную способность, чтобы справиться с ожидаемой нагрузкой пользователей. Если вы предоставляете доступ через Интернет при помощи VPN, убедитесь, что у вас достаточная пропускная способность, чтобы обрабатывать этот трафик быстрее всего остального. Кроме того, проверьте, что любое оборудование, которое будет поддерживать VPN-соединения, имеет достаточные ресурсы процессора для обработки пикового количества соединений. Шифрование очень сильно загружает процессор.

Уделите время детальной оценке провайдеров и внимательному принятию решения. Трудно сменить провайдера удаленного доступа, если он будет плохо работать, потому что это включает смену конфигурации и, возможно, программного обеспечения на машинах всех сотрудников, заказ прокладки новых линий во все места, в которых были постоянные соединения с этим провайдером, и доведение до каждого пользователя новых данных, которые необходимо знать при путешествиях.

27.1.6. Аутентификация

Система аутентификации и авторизации – это компонент, который всегда должен создаваться и поддерживаться своими силами, даже если все остальное передается сторонним исполнителям. Все методы удаленного доступа должны использовать одну базу данных аутентификации для снижения затрат на администрирование и вероятности того, что одна из баз данных может быть упущена при отключении доступа сотрудников после их увольнения. В случае необходимости для доступа к этой базе данных по различным протоколам может использоваться много интерфейсов.

Механизм аутентификации должен использовать одну из нескольких доступных систем с одноразовым паролем или маркером. Он не должен быть основан на паролях с возможностью многократного применения. Возможно, небольшим компаниям придется начать с простой системы с паролем из экономических соображений, но они должны выделить средства для перехода на более безопасную систему, как только это будет возможно.

27.1.7. Безопасность периметра

Служба удаленного доступа – это часть периметра компании, даже если она передана другой компании. Если компания основывает часть своей безопасности на наличии безопасного периметра, этот периметр должен поддерживаться. Службы удаленного доступа могут прорвать безопасность периметра из-за неправильной настройки некоторых компонентов. В частности, узлы или сетевое оборудование могут быть настроены на динамическую маршрутизацию вне зависимости от того, какой трафик они перенаправляют и по каким маршрутам. Это может привести к тому, что служба удаленного доступа создаст уязвимость в безопасности сети.

Запрещайте трафик и маршрутизацию через соединения удаленного доступа

Некоторое время одна семейная пара работала в компьютерной индустрии на прямых конкурентов. Обе компании использовали модели безопасности периметра. В обеих компаниях был высокоскоростной доступ из дома сотрудников. В семье была домашняя сеть с несколькими общими ресурсами, например принтерами. Сетевое оборудование каждой компании не было ограничено в том, какой трафик направлять и по каким маршрутам. В конце концов у каждой компании появилась полная таблица маршрутизации другой компании. Внутри и вне компании А использовалась одна и та же таблица DNS, что вызвало отправку почтовыми серверами компании В всех своих сообщений через домашнюю сеть семейной пары напрямую на внутренний почтовый сервер. Проблема была обнаружена и отслежена только тогда, когда в одной из компаний заметили, что заголовки электронной почты были не совсем правильными.

Компании должны были ограничить маршруты, которые могли попасть в их таблицы маршрутизации, и обеспечить для этих соединений по крайней мере минимальную безопасность, разрешая передачу трафика только одному авторизованному узлу на этом соединении. Эти меры предотвратили бы случайное соединение двух сетей, но не намеренную попытку взлома. Для полного обеспечения безопасности этих соединений удаленного доступа требуются более сложные меры и политики.

27.2. Тонкости

Есть несколько способов улучшить службу удаленного доступа, когда она будет работать. Для людей, которые постоянно работают дома, обратите внимание на другие потребности бизнеса, помимо простого доступа к сети. Рассмотрите способы снижения расходов и автоматизации некоторых элементов анализа затрат. Для системных администраторов, которые предоставляют удаленный доступ, есть несколько способов успевать за новыми технологиями, не превращая поддержку удаленного доступа в полный кошмар.

27.2.1. Домашний офис

Удаленный доступ – только часть полного решения по удаленной работе. Работа из дома неизбежно включает больше чем просто обеспечение сетевого соединения. Часто для решения других проблем обращаются к группе системных администраторов.

Одна из проблем, которая напрямую затрагивает группу системных администраторов, – это вопрос, кто обеспечивает оборудование для домашнего офиса, кто его поддерживает и на каком уровне. Очень дорого предоставлять поддержку, при которой требуется заходить к кому-то домой, чтобы установить новое оборудование или заменить сломанное. SLA должно очень четко оговаривать такие вопросы, и если обеспечивается такой уровень поддержки, то должна быть модель возмещения расходов на поддержку подразделением сотрудника, который работает дома.

Другие вопросы, которые неизбежно возникают, заключаются в том, что сотрудникам, работающим дома, нужно использовать телефон для нужд бизнеса, отправлять и получать факсы, печатать, копировать, устанавливать конференц-связь и присоединяться к конференциям. В зависимости от профессии им может потребоваться возможность оставаться подключенным к сети, телефону и одновременно получать факс. Кроме того, они не захотят каждый месяц изучать свои телефонные счета и запрашивать оплату всех своих деловых звонков. Компания может выбрать службы удаленного доступа, которые включают телефонную связь, или просто провести дополнительные телефонные линии, которые оплачиваются компанией. Если линии не могут оплачиваться компанией напрямую, то время, которое сотрудники тратят на составление отчетов о расходах по своим индивидуальным счетам, может представлять собой крупные скрытые издержки не просто за счет потери времени сотрудниками, но и за счет раздражения, которое может вызвать служба. Группа системных администраторов должна иметь эти требования в виду при выборе решения домашнего удаленного доступа и быть готова предоставить решение пользователями.

Другая проблема, возникающая у людей, которые работают дома, заключается в том, что им кажется, что они теряют связь с происходящим в компании, поскольку не участвуют в разговорах в коридорах, групповых собраниях или обедах. Найдите способы исключить барьер расстояния и упростить неформальное общение. Некоторые распространенные решения включают персональные системы видеоконференций и обеспечение для всех конференц-залов возможности транслировать презентации по сети.

27.2.2. Анализ и сокращение расходов

Расходы на удаленный доступ могут быстро накапливаться, и обычно они являются скрытыми для тех, кто их несет. Когда система удаленного доступа будет работать, ищите способы сокращения расходов без негативного влияния на службу. Большинство служб удаленного доступа предоставляют бесплатные номера телефонов, на которые люди могут звонить, что дорого обходится компании. Предоставление местных номеров в области с большим количеством

пользователей удаленного доступа может снизить расходы[1]. Кроме того, обратите внимание на людей, которые пользуются службой больше всего (из фиксированного места), и посмотрите, возможно ли установить здесь постоянное безлимитное соединение и может ли оно быть более выгодным. Максимально автоматизируйте этот процесс, в том числе создайте механизм уведомления людей, которые пользуются бесплатным номером, если они могут использовать местный номер.

Пример: снижение расходов за счет анализа информации о тарификации

В Lucent смогли значительно снизить расходы на службу модемного удаленного доступа при помощи некоторых интересных подходов. Система предоставляла модемные пулы в местах, населенных большим количеством сотрудников, поэтому звонки были местными, а следовательно, бесплатными. Люди, для которых модемные пулы не были местными, предоставляли отчеты о части своих телефонных счетов, что отнимало у них много времени, было дорого для обработки в Lucent и расточительно, потому что индивидуальная поминутная тарификация обычно была выше, чем Lucent могла согласовать с телефонными компаниями. Применение бесплатного (1-800) телефонного номера сильно сократило объемы подачи отчетов о расходах и уменьшило затраты. Номер 800 был достаточно развитым, чтобы направлять звонок на ближайший модемный пул и обходить модемные пулы низкой емкости. Бесплатный номер был таким удобным, что иногда люди пользовались им, даже если существовал местный номер, использование которого было дешевле для компании.

Была создана система, которая определяла телефонный номер при входящем звонке и динамически создавала баннер входа в систему, который показывал человеку телефонный номер, на который он должен звонить. Если пользователь подключался по наиболее выгодному номеру, появлялся нормальный баннер. Информация о тарификации изучалась, и сотрудники, которые не пользовались самыми выгодными номерами модемного доступа, каждый месяц получали по электронной почте сообщение, в котором объяснялось, сколько денег они могли бы сэкономить компании, если бы звонили по правильному номеру.

Когда впервые появились VPN, информация о тарификации использовалась для того, чтобы определить, поддержка каких пользователей была бы дешевле, если бы они пользовались службой VPN через постоянное подключение к Интернету, например по кабельному модему или xDSL. Люди, чей переход сэкономил бы компании больше всего денег (первые 10%), активно разыскивались, чтобы стать первыми пользователями этой новой службы. Время от времени информация о тарификации снова изучалась, чтобы определить новых кандидатов.

---

[1] Это особенно эффективно в странах с бесплатными местными звонками или даже с фиксированной платой за местные звонки, но не так полезно в странах с поминутной тарификацией местных звонков. Избегайте этого подхода, если он приведет к оплате людьми своих расходов на модемный доступ.

27.2.3. Новые технологии

Системные администраторы, которые вынуждены строить и поддерживать службы удаленного доступа, сталкиваются с проблемой попытки не отставать от новых технологий и принятия решений, какие из них реализовывать. В таком случае системным администраторам требуется одновременно поддерживать все новые и старые технологии, что приводит к постоянному росту расходов на поддержку. В этой области традиционные модемы имеют преимущество, потому что они поддерживают обратную совместимость. Можно обновить модемный пул компании до самой современной и быстрой технологии и при этом поддерживать людей, у которых есть более старые модемы. У других технологий удаленного доступа нет такого преимущество.

Введение новой технологии значительно повышает расходы на поддержку, пока эта технология не будет широко признана и хорошо понята. Поддержка старых технологий также имеет высокую стоимость: оборудование становится менее надежным и системные администраторы хуже знают систему, когда ею пользуются лишь несколько человек.

Ключ к удержанию звонков по поддержке под контролем – избежать высоких расходов на поддержку в конце жизненного цикла, когда технология все еще используется небольшим количеством людей. Достигайте этого за счет поддержки максимум двух технологий помимо традиционного модемного доступа. Когда вы собираетесь перейти на новую технологию, жестко выведите из эксплуатации более старую из двух имеющихся технологий посредством перевода ее пользователей на более новую технологию и установления жесткой даты, когда старая служба будет выведена из эксплуатации.

27.3. Заключение

Поддержка службы удаленного доступа может быть очень неблагодарной задачей, отнимающей много времени. Технологии быстро развиваются, и ваши пользователи хотят двигаться вместе с ними, но вы можете не располагать средствами для этого. Прежде чем пытаться построить службу удаленного доступа, разберитесь с требованиями – их может быть много и они могут быть разными. Определите политику удаленного доступа, с которой пользователи должны согласиться, прежде чем получат доступ к службе. Согласуйте и доведите до людей уровни обслуживания различных компонентов службы.

Служба удаленного доступа выигрывает за счет централизации из-за темпов изменения технологий. Это подходящая область для передачи сторонним исполнителям, чтобы выиграть от экономии масштаба и больших территорий покрытия, которые может обеспечить провайдер. Основное преимущество передачи сторонним исполнителям заключается в том, что она освобождает группу системного администрирования от бремени поддержки модемного пула и решения проблем удаленного доступа. Однако сохраняйте контроль над элементами аутентификации и авторизации службы удаленного доступа и уделяйте внимание безопасности службы, особенно если ваша компания полагается на безопасность периметра.

Совершенствуйте службу удаленного доступа, решая некоторые другие вопросы домашнего офиса даже до того, как они возникнут. Найдите способы снижения расходов и максимально автоматизируйте их. Если вы столкнетесь с трудностя-

ми поддержки службы удаленного доступа, контролируйте расходы на поддержку, ограничивая количество используемых технологий.

Задания

1. Какие технологии поддерживает ваша служба удаленного доступа? Какие из них дороже всего поддерживать и почему?
2. Какую следующую технологию вы введете в эксплуатацию? Опишите, как будет проходить ее внедрение.
3. Какова политика удаленного доступа в вашей компании? Как она доводится до пользователей?
4. Какие требования должна выполнять ваша система удаленного доступа?
5. Проведите нового сотрудника через процесс получения услуг удаленного доступа от вашей организации. Следите за тем, как человек выяснит, что доступно, подаст заявку на обслуживание, выполнит установку и сможет работать, но не помогайте ему. Что нужно улучшить в этом процессе, чтобы он стал более приятным для пользователя?
6. Как бы вы предоставляли удаленный доступ сотрудникам, которые находятся в местоположении клиента? На какие компромиссы вам пришлось бы пойти?
7. Каковы уровни обслуживания различных элементов системы удаленного доступа в вашей компании?
8. Если вы не передаете никакие элементы своего удаленного доступа сторонним компаниям, какова была бы цена такой передачи? Каков ее уровень по сравнению с внутренней поддержкой? Какие были бы преимущества? Недостатки?
9. Если вы передаете какие-либо элементы своего удаленного доступа сторонним компаниям, как вы решаете, какие элементы передавать, и определяете провайдера?
10. Какой механизм аутентификации вы используете для своей службы удаленного доступа?
11. Сколько баз данных аутентификации в вашей системе?
12. Какие средства обеспечения безопасности есть в вашей службе предоставления удаленного доступа?
13. Сколько людей в вашей компании регулярно работают дома? Какова модель поддержки оборудования у них дома? Какие услуги предоставляет компания помимо простого подключения к сети?
14. Если бы вам нужно было создать службу удаленного доступа для пользователей, которые работают дома, на значительном расстоянии от основного офиса, какую модель поддержки вы выбрали бы? Какой технологией вы воспользовались бы и почему? Как бы вы удовлетворяли дополнительные потребности своих пользователей, например телефонную и факсимильную связь? Как бы изменился ваш ответ, если бы люди находились на расстоянии 2000 миль от ближайшего офиса?
15. Как вы можете сократить расходы на службу удаленного доступа?

Глава 28

База программного обеспечения

База программного обеспечения – это способ обеспечить доступность большого количества программных пакетов для многих узлов. В UNIX традиционно есть глобально доступная директория /usr/local/bin, которая совместно используется всеми узлами в кластере. В Windows есть другая традиция, предполагающая хранилище устанавливаемых дистрибутивов.

UNIX известна предоставлением большого количества средств для выполнения различных задач. Однако это количество кажется маленьким по сравнению с числом средств, доступных через Интернет. Выбор и установка таких средств – это огромная ответственность. Распространение этих средств на десятки, сотни или тысячи машин невозможно без автоматизации. Если базы программного обеспечения нет, нетехническим пользователям будет просто недоставать этих средств и они не достигнут своей полной производительности, а технические пользователи установят эти средства сами, скорее всего, дублируя работу других. В любом случае пользователи потеряют в производительности, если системные администраторы не предоставят эту услугу.

Хорошая база программного обеспечения делает самую слабую операционную систему богатой и полезной. Пользователи могут привыкнуть принимать эти преимущества как должное.

Мы забываем, насколько неполными могут быть комплекты разработчиков

В одной рассылке пользователь Solaris спрашивал, как загрузить веб-страницу на диск в shell-скрипте. В одном из ответов было написано, что лучше пользоваться Linux, потому что тогда у него был бы доступ к замечательной программе под названием `wget` (Nicsic 1998). Том был удивлен, потому что у него `wget` был на каждой машине под каждой ОС UNIX и подобной UNIX, к которой у него был доступ. Он забыл, что не у каждого в UNIX-среде есть богатая база программного обеспечения, которая отслеживала все последние программы. Если ваша база программного обеспечения богатая и широко распространяется по всем машинам, пользователи забудут, что она не является частью ОС разработчика. Этот случай заставил Тома осознать, что значительная часть привлекательности дистрибутивов Linux заключается в том, что они включают такую богатую коллекцию средств, не требуя выделенного специалиста, ответственного за базу программного обеспечения, в отличие от Solaris. Это была роскошь, которой он всегда пользовался и поэтому воспринимал

как должное. (*Примечание:* В последнее время Solaris стала гораздо лучше в этом плане.)

С другой стороны, хотя такой подход снижает барьер для нововведений, он затрудняет дальнейшие обновления. Обновление до новой версии каждой из этих программ требует работы на всех машинах без исключения, потому что они не имеют доступа к хранилищу по сети. Компаниям, которые начали пользоваться Linux, в ответ пришлось усовершенствовать или переписать свои системы баз программного обеспечения, поддерживая базу программ под Linux и автоматизируя контролируемое распространение этих программ по всем машинам.

Исторически базы под Windows и UNIX очень отличаются друг от друга. Базы под Windows – это обычно хранилища программ для установки, а базы под UNIX – это, как правило, хранилища программ, которые используются в реальном времени из базы.

Часто UNIX-программы поставляются в виде исходного кода, а процесс их установки гораздо сложнее, чем может выполнить средний пользователь. Даже коммерческие UNIX-программы может быть так же трудно установить. Установка UNIX-программ часто требует `root`-доступа, которого обычно не имеют пользователи UNIX. Таким образом, в среде UNIX разумно, чтобы один человека или группа людей собирали пакеты и распространяли их по всем узлам, часто поддерживая синхронизацию сотен и тысяч узлов. Такая централизация повышает эффективность обслуживания. Часто UNIX-программы не устанавливаются на локальной машине, а просто доступны на файловом сервере, чтобы можно было смонтировать базу в конкретной директории – например, /sw или /opt/net, – добавить местоположение в вашу переменную $PATH – например, /sw/bin или /opt/net/bin, – и пользоваться программой прямо с сервера. Такая система может монтироваться только для чтения, чтобы клиенты не смогли случайно или злонамеренно изменить содержимое.

Базы программного обеспечения под Windows обычно бывают одного из трех видов. Один из видов – **сетевой диск**, который содержит определенные программные пакеты, специально написанные для работы с сетевого диска. Первое выполнение такой программы устанавливает необходимые логические файлы и параметры реестра. Другой вид – какая-либо **сетевая система распространения программ**, например Microsoft System Management Service (MS-SMS), которая позволяет администраторам централизованно распространять пакеты по всем машинам. Последний вид – это **модель сервера распространения**: хранилище программных пакетов – обычно файлов .ZIP – делается доступным местному сообществу для ручной установки.

Техническое различие заключается в том, что UNIX-программы обычно можно установить на сетевой диск, а затем все клиенты, которые монтируют этот диск, могут пользоваться программой. В системах Windows эта модель обычно не используется, потому что, прежде чем программа будет работать, программа установки должна определить параметры реестра.

Для целей данной главы, *база программного обеспечения под Windows* будет означать модель сервера распространения, где доступ к установочным файлам осуществляется через Веб или локальную сеть. Запуск программ с сетевого

диска аналогичен базам программного обеспечения в UNIX и таким системам, как MS-SMS (рассмотрена в главе 3).

Часто о базах программного обеспечения думают как о чем-то, что можно встретить в корпоративных или университетских компьютерных системах общего назначения, а не в компаниях, например, электронной коммерции, которым нужно жестко контролировать, какие программы на каких узлах имеются. Но, хотя количество программных пакетов в среде электронной коммерции может быть не таким большим, важные принципы, например целостность и эффективное использование, все-таки справедливы.

28.1. Основы

Мы начнем с обоснования для бизнеса и технических требований баз программного обеспечения. Затем мы рассмотрим политики и документации, которую вам нужно создать. С этими принципами мы пройдем через процесс выбора из многих существующих программ управления базами программного обеспечения, а затем спроектируем простые системы баз программного обеспечения для UNIX и Windows. Система, которую мы спроектируем, будет служить нашим нуждам и потребует очень мало программирования.

28.1.1. Обоснование

База программного обеспечения – это пользовательская служба, которая находит, устанавливает и поддерживает библиотеку программ. Снижая дублирование усилий за счет использования базы программного обеспечения, можно достичь значительного снижения расходов.

База избавляет людей от поиска программ в Интернете, предоставляет простой буфер, который экономит пропускную способность сети, и объединяет закупки программного обеспечения (в разделе 21.2.1 рассмотрены экономические преимущества и результаты оптовых закупок программ).

Без базы пользователи и системные администраторы будут тратить зря много времени на поиск программ в Интернете, в каталогах и в других местах. База предоставляет единое место, где пользователи могут искать программы. Без базы программы будут устанавливаться во многих местах по всей сети. Люди, которые поддерживают базы программного обеспечения, – это библиотекари. Они сортируют новые программы и выбирают то, что, по их мнению, понадобится их пользователям. Кроме того, они принимают заявки.

Если один человек запросил программу, высока вероятность того, что другие люди также посчитают эту программу полезной. Вокруг некоторых программ могут возникнуть сообщества с собственной поддержкой.

Базы максимально эффективно используют знания об установке программ. Компиляция и установка программ могут быть такими трудными, что даже опытные системные администраторы могут что-то забыть, хотя и выполняют это довольно часто.

Системные администраторы, поддерживающие базы, всегда должны отслеживать и устанавливать новые версии программ по мере их выхода. В частности, важно искать исправления ошибок, особенно связанных с безопасностью. Поддержание централизованной базы обеспечивает доступ всех пользователей к новой версии, если применяется модель распространения.

Целостность, которая обеспечивается наличием одних и тех же программ на всех узлах, выгодна как системным администраторам, так и пользователям. Системные администраторы выигрывают, потому что их усилия распространяются на все узлы. Пользователи выигрывают, потому что все машины, у которых есть доступ к базе, становятся в какой-то мере взаимозаменяемыми. Пользователи могут выбирать узлы на основании их аппаратных различий, таких как скорость, память и т. д., а не по тому, какие программы там установлены.

В небольших компаниях часто считают, что им не нужна база программного обеспечения. Мы утверждаем, что всем машинам нужна целостная структура для хранения программ, иначе нарушения целостности создадут большую путаницу. Несмотря на то что сложная система базы программ может и не требоваться, целостная структура и процесс приобретают большую значимость по мере того, как маленькие компании вырастают в более крупные. Маленькие компании должны следить за признаками того, что они растут и скоро смогут пользоваться преимуществами более сложной базы программного обеспечения. Среди таких признаков можно назвать минимальный контроль библиотеки программ, дублирование процесса сборки без необходимости и наличие нецелостного набора программ на ваших машинах.

28.1.2. Технические требования

База программного обеспечения должна быть основана на требованиях людей, которые ею пользуются. Поймите, чего пользователи хотят от базы. Их потребности могут быть узкими или широкими, ограниченными руководством или правовыми требованиями либо не ограниченными вообще. Пользователям также может понадобиться, чтобы несколько версий главного инструмента, например компилятора, было доступно одновременно, когда они переходят на более новую версию.

Рассмотрите требования к надежности. Если файлы хранятся локально, то проблем будет меньше, потому что локальные файлы обычно доступны, если доступна машина. Если файлы расположены на удаленном файловом сервере, надежность и расширяемость сети и сервера являются важными факторами. Если база больше похожа на FTP-сервер, доступ к которому осуществляется время от времени, пользователи будут более снисходительны к сбоям. Если вам нужны еще более высокие уровни надежности, рассмотрите применение репликации или методов RAID, рассмотренных в разделе 25.1.1.2, чтобы повысить степень доступности базы.

28.1.3. Установите политику

Необходима политика, которая указывает, кто может размещать программные пакеты в базе. Может быть опасно разрешать всем предоставлять программы, которые каждый будет запускать. Кто-нибудь может установить «троянского коня», вредоносную программу с таким же названием, как у какой-то другой программы, либо кто-то, не знающий требований пользователей, может обновить инструмент и неумышленно создать проблемы совместимости. В политике должны быть разобраны следующие вопросы.

- Кто может собирать и устанавливать пакеты? Может быть назначен один или несколько человек, которые станут заниматься только этим полный рабочий день. Может быть, все системные администраторы могут создавать пакеты,

но один человек проверяет качество и устанавливает их. Возможно, некоторые пользователи могут обновлять определенные пакеты, но первоначальная установка должна контролироваться системным администратором.

- Что произойдет, если поддерживающий базу специалист покинет организацию? Если конкретные пакеты поддерживаются конкретными людьми, в политике должно быть указано, что делать, если этот человек уволится.
- Какие ОС поддерживаются? Существует ли база для каждой используемой ОС или только для нескольких? В UNIX можно иметь одну базу для всех ОС и использовать **скрипты-оболочки**, чтобы обходить различия систем. Скрипт-оболочка – это пакетный файл, который определяет, на какой платформе он запущен, и вызывает соответствующий двоичный файл. Обычно двоичные файлы переименованы таким образом, чтобы у скрипта-оболочки было имя, соответствующее ожиданиям пользователей. Оболочки могут устанавливать переменные среды, проверять, существуют ли файлы конфигурации, и т. д. В качестве альтернативы, если есть база для каждой ОС, предполагается ли работа пакетов на всех версиях этой ОС или оболочки используются, если различные двоичные файлы нужны даже для разных версий этой ОС?
- Если вы используете оболочки, существует ли стандартная оболочка или шаблон, который все должны применять?
- Как осуществляется обновление? Когда появляется новая версия или пакет, кто отвечает за его установку?
- Как решается проблема ошибок? Предполагается ли, что поддерживающий базу специалист будет отлаживать пакеты с открытым исходным кодом, или пользователей лишь просят сообщать об ошибках этим специалистам и ждать следующей версии?
- Как пакеты удаляются из базы? Во многих компаниях есть строгая политика удаления. Пакеты могут удаляться по мере перехода официальной среды разработки на более новые средства либо храниться постоянно, если только популярные программы переносятся в новую базу, создаваемую для следующей версии ОС.
- Каков охват распространения? Создана ли эта база для кластера, подразделения или всей организации?
- Как пользователи запрашивают внесение программ в базу? Существует ли комиссия по базе, которая решает такие вопросы?

Политика должна быть доведена до людей и опубликована, предпочтительно там, где пользователи ее увидят.

> **Отслеживание лицензий**
>
> В разделе 12.1.5 есть два не требующих серьезных усилий приема отслеживания лицензий программ.

28.1.4. Выберите программу для базы

Для систем UNIX мы рекомендуем выбор существующей системы управления базой, а не написание ее с нуля. Даже если вы считаете, что ваша среда особен-

но специфична, проще настроить существующую программу, чем изобрести новую. Есть много бесплатных пакетов для управления базами программного обеспечения. Depot (Colyer and Wong 1992) – одна из классических программ для администрирования баз программного обеспечения. Есть много других программ, например, LUDE (Dagenais at al. 1993), Modules (Furlani and Osel 1996) и SEPP (Oetiker 1998b). GNU Stow (Glickstein 1996) – полезное средство для управления символическими ссылками UNIX в базе.

Для нашего определения базы программного обеспечения для Windows также есть варианты. Вы можете сделать общую сетевую папку FTP-сервером или веб-сайтом, который предоставляет программы. В разделе 28.1.6.2 описано, как можно решить вопросы организации и документации базы для Windows в архитектуре системы базы.

В вашей компании может быть уже устаревшая система хранилища. В таком случае определите, будет ли лучше усовершенствовать новую систему или создать полностью новую.

28.1.5. Создайте руководство для процесса

Вне зависимости от того, какую программу вы выберете, важно документировать локальную процедуру внесения в систему новых программных пакетов. Хотя документация, поставляемая с диспетчером пакетов, полезна, данный документ должен содержать местные особенности, например имена узлов, управляющих системой, и т. д.

После того как люди воспользуются этой документацией для внесения пары пакетов, может быть полезно создать более краткое руководство, которое обобщает шаги без подробного объяснения того, почему их нужно выполнять. Этот документ просто помогает опытным системным администраторам не пропустить никаких шагов. У системного администратора должна быть возможность копировать и вставлять команды из этого документа в командную строку, чтобы процесс шел быстро.

28.1.6. Примеры

28.1.6.1. UNIX

Теперь мы опишем простую, но мощную базу программного обеспечения для UNIX. Ею можно пользоваться как в одной системе, так и в средней распределенной сети. Можно расширить ее для крупных сетей при помощи небольшой автоматизации[1]. В нашем примере устанавливаемые пакеты – это различные версии языка программирования Perl и почтового клиента mutt.

Для каждой поддерживаемой ОС пакеты собираются на определенном сервере. Важно документировать, какие машины используются для сборки, чтобы процесс можно было точно повторить. Это упрощает отслеживание проблем, особенно странных вопросов с библиотеками, которые периодически возникают.

Исходный код каждого пакета хранится в директории /home/scr с поддиректорией для каждого пакета. В поддиректории находятся tar-файлы для всех

[1] Мы хотим настоятельно порекомендовать вам не ставить программы сторонних производителей напрямую в директорию /bin или /usr/bin, как рекомендуют в других книгах и статьях. Слишком трудно отслеживать модификации, когда вы изменяете пространство имен, предоставленное разработчиком.

версий пакета, которые поддерживаются на данный момент, а также не упакованные при помощи tar исходные коды, на которых выполняется сборка. Например, директория /home/scr/perl может содержать файлы perl-6.0.tar.gz и perl-6.1.tar.gz, а также соответствующие поддиректории. В среде с несколькими ОС еще один уровень поддиректорий может разделять копии исходного кода, скомпилированные для каждой ОС, хотя некоторые пакеты используют в команде make переменную VPATH, чтобы разрешить использование одной копии исходного файла при сборке для различных ОС.

Кроме того, в директории /home/src находится скрипт под названием SOURCEME, который предназначен для правильной установки параметров среды. Если для конкретного пакета требуется определенная среда, то файл SOURCEME, определенный для этих требований, хранится в поддиректории пакета, например /home/scr/perl/SOURCEME или /home/scr/perl/SOURCEME-6.1. Создание такого файла не требует времени, и он способствует изучению структур, позволяет не изобретать велосипед и предоставляет документальное свидетельство системным администраторам, которые должны повторить процесс. Большие усилия, затраченные на сборку первой версии пакета, максимально эффективно используются при появлении новых выпусков.

Пакеты устанавливаются в директориях, которые именуются по названию пакета и номеру версии. Например, /sw/perl-6.0 содержит директории bin, man и lib для Perl 6.0. Другие программы могут храниться в директориях /sw/perl-6.1, /sw/mutt-1.2.6 и /sw/mutt-2.0.1. Это позволяет системным администраторам удовлетворять требования по обеспечению одновременного наличия нескольких версий.

Название пакета без версии – это ссылка на последнюю поддерживаемую версию пакета. Например, /sw/perl будет символической ссылкой, указывающей на /sw/perl-6.1. Это означает, что для того, чтобы специально воспользоваться старой (6.0) версией Perl, вам нужно включить /sw/perl-6.0/bin в переменную PATH[1]. Однако, чтобы идти в ногу со временем и пользоваться последней стабильной версией Perl, вы должны включить в PATH /sw/perl/bin.

Новые программы можно устанавливать и тестировать перед их представлением всем пользователям, просто не обновляя основную (/sw/perl) символическую ссылку, пока эта версия не будет готова для массового использования. Например, если версия Perl 6.1 постоянно используется, а Perl 7.0 только вышла, последняя будет установлена в директорию /sw/perl-7.0. Тестирующие сотрудники могут включать /sw/perl-7.0/bin перед своей переменной PATH. После того как они сертифицируют новую версию, символическая ссылка /sw/perl настраивается на директорию 7.0. Из-за принципа работы символических ссылок процессы, осуществляющие в этот момент доступ к старой версии, обычно продолжат работу без проблем, потому что старая версия не удалена. Вместо этого новый пакет будет виден только при новой инициации работы программы.

Если вы пользовались системой, как было описано до сих пор, переменная PATH каждого пользователя будет очень длинной и трудной в управлении при большом количестве пакетов. Чтобы решить эту проблему, создайте директорию под названием /sw/default/bin, которая содержит символические ссылки на все

[1] Вы также должны включить /sw/perl-6.0/man в MANPATH. В дальнейшем, когда мы будем предлагать включить что-то в PATH, мы будем подразумевать, что соответствующая директория man включена в MANPATH.

самые популярные программы. Теперь типичным пользователям базы нужно будет добавить в свою переменную PATH только эту директорию для доступа к распространенным программам. Например, /sw/default/bin/perl будет ссылкой на /sw/perl/bin/perl. Подобные ссылки должны включаться для других частей пакета Perl, таких как a2p, s2p и perldoc. Имейте в виду, что эти ссылки должны быть связаны с/sw/perl, а не с /sw/perl-6.1, поскольку /sw/default/bin должна ссылаться на самые популярные, а не какие-то особые версии. Кроме того, если бы была установлена новая версия Perl, стало бы трудно обновлять все ссылки в /sw/default/bin. Если кому-то нужен доступ ко всему пакету, он может добавить себе в PATH его директорию bin.

Возможно, угадывать популярные программы в пакете – это непродуманно, но без автоматизации проще гадать, чем создавать ссылки на каждый объект в пакете. Небольшая автоматизация может здесь помочь за счет упрощения создания ссылок на все файлы в пакете, а не на те, которые системные администраторы считают нужными типичному пользователю. Для управления символическими ссылками можно пользоваться такой программой, как GNU Stow (Glickstein 1996). Stow проста в использовании и всегда создает минимальное количество символических ссылок на все двоичные файлы в bin, а также на страницы man, библиотеки и другие файлы.

До сих пор мы описывали работу для одного узла. В случае сети узлов нам нужно дать клиентам доступ к одному и тому же программному обеспечению. Мы можем сделать это путем копирования пакетов на соответствующие машины либо предоставить доступ по сети, возможно, через NFS. Можно воспользоваться средством автоматического монтирования, чтобы /sw других серверов появлялась на клиентах.

Допустим, что bester – это файловый сервер, который поддерживает узлы под Solaris 8.0, карта автоматического монтирования /sw для Solaris 8.0 будет выглядеть следующим образом

```
default      bester:/sw/default
perl-6.0     bester:/sw/perl-6.0
perl-6.1     bester:/sw/perl-6.1
perl         bester:/sw/perl-6.1
mutt-1.2.5   bester:/sw/mutt-1.2.5
mutt-1.2.6   bester:/sw/mutt-1.2.6
mutt-2.0.1   bester:/sw/mutt-2.0.1
mutt         bester:/sw/mutt-2.0.1
```

Когда в среду будет введена Solaris 9.0, карта автоматического монтирования для Solaris 9.0 создается путем копирования карты из 8.0. Однако не все пакеты, скомпилированные для Solaris 8.0, совместимы с Solaris 9.0 на уровне двоичных файлов. Особые пакеты, которым нужна повторная компиляция, могут указывать на эти новые двоичные файлы. В нашем примере mutt совместима с версиями Solaris 8.0 и 9.0, но Perl требует повторной компиляции. Предположим, что сервер для Solaris 9.0 называется lyta, тогда наша карта для 9.0 будет выглядеть следующим образом:

```
default      lyta:/sw/default
perl-6.1     lyta:/sw/perl-6.1
perl         lyta:/sw/perl-6.1
mutt-1.2.5   bester:/sw/mutt-1.2.5
mutt-1.2.6   bester:/sw/mutt-1.2.6
```

```
mutt-2.0.1   bester:/sw/mutt-2.0.1
mutt         bester:/sw/mutt-2.0.1
```

Обратите внимание, что perl-6.0 отсутствует. Это сделано, чтобы показать, что старые пакеты не переносятся на новую ОС, если этого не потребуют специально.

Вы можете приспособить несколько политик для поддержки старых ОС. Очевидно, для последней ОС должен собираться новый пакет. Однако, если для старых ОС требуется особая повторная компиляция, может оказаться, что вы будете тратить много времени и сил на поддержку лишь нескольких старых узлов. Вы должны решить, что активно поддерживаемые базы будут у текущей и одной предыдущей версии ОС. Базы для других версий ОС замораживаются, за исключением, возможно, исправления ошибок, затрагивающих безопасность. Это означает, что узел `bester` не может быть выведен из эксплуатации, пока он не останется последним узлом под Solaris 8.0. В качестве альтернативы можно скопировать данные на любой NFS-сервер и после простой перенастройки карты автоматического монтирования вывести `bester` из эксплуатации.

С дополнительными ОС можно работать таким же образом: одно дерево на ОС и дополнительная карта автоматического монтирования, настроенная на клиентах. Обычно эти новые базы сначала будут почти пустыми, потому что какой-то пакет редко можно использовать в совершенно другой ОС.

Требования к надежности вашей базы часто могут быть реализованы при помощи возможностей средств автоматического монтирования. Репликацию можно обеспечить при помощи более сложных опций синтаксиса средства автоматического монтирования, которые позволяют вам указывать несколько серверов. На самом деле некоторые средства автоматического монтирования позволяют картам принимать решения в зависимости от ОС, которой пользуется клиент. В таком случае можно создать одну карту самого высокого уровня, которая все делает правильно в зависимости от того, какая ОС используется и какие серверы работают.

Управление символическими ссылками и большим количеством карт автоматического монтирования может быть утомительным. Даже если новый пакет совместим со многими версиями ОС на уровне двоичных файлов, нужно обновить многие карты средств автоматического монтирования. Если синхронизация карт нарушится, могут возникнуть странные проблемы. У людей не очень хорошо получается поддерживать такую синхронизацию, но компьютеры с этим справляются. Поэтому может быть полезно автоматизировать этот процесс, чтобы снизить его трудоемкость и количество ошибок. Создайте главный файл, в котором описаны различные пакеты, версии, операционные системы и серверы. Используйте этот главный файл для создания карт автоматического монтирования и команд GNU Stow, которые нужно запустить. Такая программа, как `make`, может автоматизировать все вышеописанное, поэтому вам останется только отредактировать главный файл и ввести `make` (многие системные администраторы не думают об использовании `make` для автоматизации задач, однако это может быть очень полезно, когда имеется ряд задач, которые зависят друг от друга).

Продолжая наш пример, мы вводим `talia`, сервер, который является резервным для `lyta` в том плане, что он предоставляет те же программы на другом узле. Главный файл может выглядеть следующим образом:

```
default     sol80         bester      /sw/default
default     sol90         lyta.talia  /sw/default
perl-6.0    sol80         bester      /sw/perl-6.0
perl-6.1    sol80         bester      /sw/perl-6.1
perl        sol80         bester      /sw/perl-6.1
perl-6.1    sol90         lyta.talia  /sw/perl-6.1
perl        sol90         lyta.talia  /sw/perl-6.1
mutt-1.2.5  sol80,sol90   bester      /sw/mutt-1.2.5
mutt-1.2.6  sol80,sol90   bester      /sw/mutt-1.2.6
mutt-2.0.1  sol80,sol90   bester      /sw/mutt-2.0.1
mutt        sol80,sol90   bester      /sw/mutt-2.0.1
```

Использование такого главного файла требует определения стандартного способа указывать ОС. В нашем примере мы определили, что `sol80` и `sol90` означают Solaris 8.0 и Solaris 9.0, соответственно. В некоторых компаниях созданы сложные коды, чтобы указывать точного разработчика, процессор, ОС и версию ОС в виде строки из 4 символов, но мы рекомендуем, чтобы вы придерживались простоты и пользовались кодами, которые вам понятны.

Удаление программ просто: нужно удалить директорию с сервера и соответствующую строку в главном файле. Более консервативный подход может заключаться в переименовании директории на сервере, чтобы она была недоступна. Разумно не удалять файлы около недели. Если в течение этого времени кто-то пожалуется, что пакет отсутствует, его легко можно снова добавить (конечно, удаление должно объявляться вашим пользователям при помощи любого метода, подходящего для вашей компании).

Описанная система имеет свойство бесконечно потреблять дисковое пространство, пока она не заполнит все доступные диски. Однако мы видим, что система сама управляет дисковым пространством. Периодически в эксплуатацию вводятся новые ОС, которые настолько несовместимы, что ни один из старых пакетов не может быть перенесен в новую карту автоматического монтирования. Вместо того чтобы заново собирать каждый пакет для новой ОС, собираются только критически важные и популярные пакеты. В конце концов все старые ОС устраняются из среды, унося с собой старые, неиспользуемые пакеты. Пока это происходит, система в какой-то степени сама ограничивает свое потребление дискового пространства.

Контроль над тем, кто может добавлять в эту систему пакеты, основан на правах доступа в UNIX к используемым файлам и директориям. Очевидно, непривилегированные пользователи должны иметь ко всем этим пакетам доступ только для чтения. На самом деле вы должны по возможности экспортировать пакеты в NFS только для чтения.

Если пользователи хотят иметь возможность поддерживать программы в этом дереве, лучше всего позволить им передавать программы системному администратору, который их устанавливает. Это обеспечит централизованное сохранение носителя установки. Если программа распространяется в виде исходного кода, это предотвращает ситуацию, в которой единственный человек, знающий исходный код, уходит из компании.

Может быть полезно выделить область, где пользователи смогут сами устанавливать программы, чтобы делиться ими с другими. Это снимает часть обязанностей с системных администраторов, что всегда хорошо. Дополнительный контроль, предоставляемый владельцу пакета, означает, что он может обеспе-

чивать быстрое обновление. Без этой возможности размещение таких программ для общего доступа приведет к тому, что пользователи будут включать директории bin других пользователей в свои переменные PATH. Обычно это небезопасно. Рассматривая систему, описанную выше, мы можем расширить ее, чтобы разрешить размещение программ пользователями. Вы можете создать директорию /sw/contrib, которая доступна для записи любому ID пользователя, возможно, только с определенного узла. Пользователи могут создавать в этой области поддиректории для пакетов, которые они хотят установить. Нужно создать несколько правил для обеспечения некоторого уровня безопасности. Очевидно, что, если кто-то установит вредоносную программу, можно будет отследить источник, потому что этот человек владеет файлами, размещенными в /sw/contrib. Обычно это достаточная мера, чтобы внимательно выбирать, что устанавливается. Человек, владеющий файлами, должен отвечать за обновление пакета.

Было бы неразумно ожидать от системных администраторов поддержки пакетов пользовательской разработки в /sw/contrib. Другая мера предосторожность – запретить людям включать /sw/contrib в свою переменную PATH. К сожалению, это можно обеспечить только при помощи обучения и давления коллектива. Вместо того чтобы напрямую вносить такие пакеты в свои переменные PATH, людям нужно создавать символические ссылки из $HOME/bin на конкретные программы в /sw/contrib, доступ к которым им нужен. И хотя это тоже не является совершенным, достигается равновесие удобства и безопасности. Вам следует документировать политики, связанные с директорией /sw/contrib, в файле /sw/contrib/POLICY или, по крайней мере, использовать этот файл для направления людей на веб-страницу, где объясняется политика.

Одно из преимуществ описанной нами системы заключается в том, что она не требует использования оболочек. Мы видели хорошо и плохо написанные оболочки и, честно говоря, предпочли бы не видеть их совсем. Иногда оболочки странно влияют на программы, которые плохо реагируют на переименование, принимают опции в странном формате и т. д. В UNIX оболочка, которая начинается с `#!/sw/bin/perl`, не будет работать, если /sw/bin/perl сама по себе является консольным скриптом – первая строка начинается с `#!/bin/sh`. Конечно, будут такие крайние случаи, в которых оболочки все-таки необходимы. Вы можете разместить все оболочки в специальной области, например /sw/wrappers/bin, либо можно напрямую устанавливать их в /sw/default/bin. Некоторые считают более правильным использовать /sw/default/bin, другие полагают, что символические ссылки и оболочки могут располагаться в одном месте.

Эти оболочки могут устанавливать переменные среды, а затем вызывать программу из директории пакета bin, но они способны на большее. Если ваши пользователи технически продвинутые, то может быть достаточно просто вывести указания для оболочки по установке параметров среды, чтобы работала программа, которую пытаются запустить.

Оболочки могут быть опасны. Если вы пользуетесь оболочкой, чтобы не создавать карту автоматического монтирования для новой версии ОС, внезапно может появиться гораздо больше оболочек, которые нужно поддерживать. Лучше потратить время на облегчение создания новых карт автоматического монтирования, чем начинать создавать оболочки.

Система может вырасти достаточно сильно за счет добавления пакетов, репликации различных пакетов на дополнительных серверах и создания новых карт

автоматического монтирования для новых ОС. По мере роста системы имеет смысл автоматизировать процессы, особенно репликацию.

В данном разделе мы рассмотрели простую, но мощную базу программного обеспечения под UNIX. Она эффективно использует ранее существовавшие элементы, например систему прав доступа UNIX, средства автоматического монтирования и NFS. Она сама себя документирует – главный файл и структура файловой системы описывают саму систему. Она достаточно проста, чтобы ее хватало для одного узла или небольшого кластера, и имеет ясный путь развития до более крупных, даже глобальных систем.

28.1.6.2. Windows

В средах Windows узлы исторически администрируются более самостоятельно, чем в средах UNIX. Традиционная база программного обеспечения для Windows больше похожа на FTP-сервер или директорию файлового сервера, которая содержит устанавливаемые пакеты программ – ZIP-файлы или автоматически устанавливаемые .EXE, – которые могут устанавливаться пользователями компьютеров.

Среды отличаются по политикам, которые касаются самостоятельно установленных программ. Некоторые полностью запрещают их, другие разрешают установку только одобренных программ, третьи позволяют пользователям ставить на свои компьютеры все, что те хотят. База программного обеспечения должна отражать эту политику.

Вот пример простой базы программного обеспечения, которая подошла бы для среды, где некоторые продукты одобрены для всех систем, а у других есть специальные ограничения и контроль установки. В данном хранилище на файловом сервере под Windows (CIFS) создается «общая папка» под названием software. Пользователи осуществляют к ней доступ как к \\server1\software. В ней они могут найти документ под названием POLICY, объясняющий общую политику, которая касается программ, устанавливаемых на компьютерах пользователями, а также особые политики, связанные с конкретными программными пакетами. Например, этот документ может объяснять, как получать лицензионные программы. В папке будет следующий набор подпапок:

- *Стандартные*. В этой папке содержатся программы, которые одобрены для всех машин, но не устанавливаются по умолчанию на новых компьютерах. Это первое место, куда будут заглядывать люди, ищущие в базе какую-либо программу. Здесь может быть приемлемо размещение программ с корпоративной лицензией.
- *Предустановленные*. Здесь содержатся программы, которые уже должны быть установлены при получении компьютеров и/или будут автоматически обновляться через MS-SMS. Несмотря на избыточность, полезно, чтобы предустановленные программы были доступны для повторной установки или установки на машины, которые не прошли через обычный процесс установки компьютера. В качестве примеров программ, которые могут здесь быть, можно назвать программы с корпоративной лицензией, например WinZip, антивирусы и офисные пакеты.
- *Образы дисков*. В этой папке содержатся образы CD-ROM и DVD, для которых есть лицензия или они распространяются бесплатно. Например, здесь хранятся образы дистрибутивов BSD и Linux. Преимущество размещения

здесь таких образов заключается в том, что это экономит пропускную способность на вашем интернет-шлюзе.

- *Экспериментальные.* Эта папка – для программных пакетов, которые еще не одобрены, но их одобрение рассматривается. Она должна быть защищена паролем или может иметь ограниченный список контроля доступа (Access Control List – ACL), чтобы доступ к содержимому был разрешен только тем, кто занимается его оценкой.
- *Администратор.* Здесь находятся средства, доступ к которым должны иметь только системные администраторы, или, что более важно, программы с индивидуальными лицензиями. Это должна быть защищенная паролем или ACL папка, доступ к которой есть только у системных администраторов. Структура этой области может включать папки для стандартных, предустановленных, экспериментальных программ и образов диска. Один из способов управления вопросами лицензий – потребовать, чтобы программы без корпоративных лицензий устанавливались системным администратором или каким-либо доверенным лицом, чтобы были выполнены все связанные с лицензией процедуры. Например, перед установкой программы человек может проверять и подтверждать, что конкретно для этого узла была получена лицензия. Если программы массово закупаются заблаговременно, как описано в разделе 21.2.1, системный администратор может просто записать эту установку как использование одной из предварительно закупленных лицензий.

Каждая папка может содержать подпапки для различных версий Windows, где хранятся пакеты для этих версий. Может быть папка под названием Устаревшие, куда перемещаются старые программы, которые больше не поддерживаются. Несмотря на то что старые пакеты могут больше не требоваться, время от времени возникают экстренные ситуации, в которых полезно наличие под рукой старых программ. Это баланс управления риском и дисковым пространством.

Полезно создавать отдельную папку для каждого пакета, а не иметь одну папку, полную программ. Названия пакетов не всегда понятны неопытному новичку, тогда как названия папок могут быть очень конкретными: FooSoft Accounting Client 4.0 понятнее, чем FSAC40.ZIP. В большинстве пакетов есть отдельный файл README, который должен быть в этой папке. Если все пакеты хранятся в одной папке, велика вероятность того, что имена README будут конфликтовать.

Для каждой папки полезно создать документ под тем же названием – конечно, с расширением .txt, – который содержит данные о программе, ограничениях лицензии и наличии особых нюансов при установке. Вы должны создать стандартный формат для первой части файла, а затем можно писать произвольный текст.

Если база программного обеспечения окажется удачной, вы можете решить распространить ее в различных частях компании. Это может снизить использование пропускной способности сети, повысить скорость установки и обеспечить большую надежность. Момент, когда такая репликация становится полезной, существенно отличается от аналогичного момента для баз под UNIX. Базы программного обеспечения под Windows создают относительно небольшую нагрузку на сеть по сравнению с сетевой активностью, необходимой для базы в UNIX, где сеть требуется для каждого запуска программы. Кроме того, база программного обеспечения под Windows не рассчитана на работу в реальном времени, в отличие от баз в UNIX, потому что установка происходит один раз

и доступ к серверу больше не требуется. Медленная установка утомительна, но не останавливает работу. Однако медленный NFS-доступ к базе в UNIX может подорвать производительность. Поэтому вы можете предпочесть не распространять базу программного обеспечения для Windows, а вместо этого просто разместить ее в каком-то месте с хорошим сетевым подключением.

В данном разделе мы описали простую, но мощную базу программного обеспечения под Windows. Она учитывают уникальную культуру систем Windows, касающуюся установки программного обеспечения. Она не требует никаких программ, если не нужна ее репликация, а в этом случае можно воспользоваться одной из хороших систем репликации папок. Для необходимого ограничения доступа она эффективно использует средства управления доступом протокола доступа к файлам Windows CIFS. Она сама документирует себя, потому что иерархия папок описывает, какие программы доступны, а указания по локальной установке и документы политик для простоты доступа могут быть размещены вместе с пакетами.

28.2. Тонкости

Несмотря на то что задача базы программного обеспечения – предоставлять всем узлам одни и те же программы, высший уровень – обеспечивать индивидуальную настройку для различных узлов. Здесь мы рассмотрим предложения по обеспечению часто требуемой индивидуализации: небольших отличий в конфигурации, локальной репликации пакетов, коммерческих программ и меньших баз для ОС, которые не получают полной поддержки.

28.2.1. Различные конфигурации для разных узлов

Часто требуемая функция баз программного обеспечения в UNIX – возможность обеспечения немного отличающихся конфигураций для различных узлов или кластеров узлов. Если конфигурация пакета должна сильно отличаться для разных узлов, может быть удобно, чтобы файл конфигурации в базе был просто символической ссылкой на локальный файл. Например, /sw/megasoft/lib/megasoft.conf может быть символической ссылкой на /etc/megasoft.conf, который может иметь особое содержимое для конкретного узла.

Если вы хотите выбирать между несколькими различными стандартными конфигурациями, их можно включить в пакеты. Например, /etc/megasoft.conf может сам быть символической ссылкой на один из многих файлов конфигурации в папке /sw/megasoft/lib. У вас могут быть стандартные конфигурации сервера и клиента (megasoft.conf-server и megasoft.conf-client) или конфигурации для определенных групп пользователей (megasoft.conf-mktg, megasoft.conf-eng, megasoft.conf-dev и megasoft.conf-default). Из-за того что последовательность символических ссылок перенаправляется с базы на локальный диск, а затем опять на базу, они часто называются перенаправляющими ссылками.

28.2.2. Локальная репликация

Если доступ к вашей базе под UNIX выполняется по сети, может быть удобно скопировать часто используемые пакеты на локальный диск. Например, на рабочей станции разработчика, на которой есть свободное дисковое пространство, могут локально храниться самые последние версии средств разработки.

Локальная репликация снижает нагрузку на сеть и повышает быстродействие. Вы должны убедиться, что доступ к локальному диску быстрее, чем к сетевому файловому серверу, что бывает не всегда. Проблемой становится анализ данных о том, какие пакеты локально хранятся на каких машинах, чтобы можно было управлять обновлениями.

Программы управления базами должны упростить все это. Они должны предоставлять статистику, чтобы помочь в выборе пакетов, которые должны кэшироваться, или, по крайней мере, позволять системным администраторам и пользователям указывать, какие пакеты должны сохраняться локально. В нашем примере с UNIX используемое развитое средство автоматического монтирования может указать, что для конкретной машины пакет находится на локальном диске.

Новые версии пакетов требуют особой обработки при ручном выполнении локальной репликации. В некоторых системах новая, несохраненная версия имеет приоритет над локальной копией. Если задача в том, чтобы пользователи всегда видели последнюю версию пакета, это именно то, что нужно, хотя, если никто не потрудился переписать новую версию на локальный диск своей машины, пострадает быстродействие. Но медленные правильные процессы лучше, чем неправильные с отличным быстродействием. С другой стороны, если кто-то напрямую изменил оригинал пакета, не меняя номер версии, системный администратор должен не забыть также обновить все копии пакета, которые могут находиться на других машинах. Если отслеживание всех локальных копий выполняется вручную, это может стать кошмаром.

Локальная репликация файлов базы программного обеспечения может влиять на правила резервного копирования. Либо систему резервного копирования нужно будет настроить так, чтобы она избегала резервного копирования локальных хранилищ, которые, в конце концов, можно восстановить при помощи программы управления базой, либо вам придется планировать, как справиться с дополнительными требованиями по хранению данных. Преимущество резервного копирования локально сохраненных программ заключается в том, что полное восстановление отражает истинное последнее состояние машины, программ и т. п.

Общее решение для этого – пользоваться кэшем NFS, где все файлы, к которым осуществляется доступ через NFS, сохраняются на локальном диске. Кэши NFS, например `cachefs` в Solaris, лучше всего работают с данными только для чтения, такими как база программного обеспечения. Такая система имеет значительный потенциал для повышения быстродействия. А главное, она является адаптивной и автоматически кэширует то, что используется, поэтому от системных администраторов не требуется определять, что и когда должно кэшироваться. Это система типа «установил и забыл».

28.2.3. Коммерческие программы в базе

Включение в базу коммерческой программы трудно настолько, насколько сложна ее лицензия. Если у вас есть корпоративная лицензия, коммерческие программы можно включать в базу, как все остальное. Если программа автоматически связывается с определенным сервером лицензий, который, в свою очередь, принимает решение о наличии или отсутствии лицензии, программа может быть доступна любому, потому что для неавторизованных пользователей она будет бесполезна.

Однако, если доступ к программе разрешен только конкретным пользователям, а механизма проверки авторизации пользователя в программе нет, то убедиться в выполнении лицензии – обязанность системного администратора.

В нашем примере с базой для Windows мы рассмотрели контроль установки лицензионных программ посредством запроса системным администраторам на выполнение установки. В среде UNIX есть дополнительные возможности. Если программа лицензирована для всех пользователей конкретного узла, ее можно устанавливать только на этот узел. По возможности вам следует установить ее в обычной номенклатуре базы (другими словами, программа управления базой не должна паниковать, когда она обнаруживает в своем пространстве имен локально установленную программу). В качестве альтернативы можно создать в UNIX группу для людей, которые авторизованы для использования программы, а ключевые файлы в пакете можно сделать исполняемыми только для членов этой группы.

Среды UNIX часто сталкиваются с ситуацией, когда различные небольшие группы пользуются одним пакетом программ, но каждая группа должна осуществлять доступ к своему серверу лицензий[1]. Это еще одна проблема, которую можно решить при помощи перенаправляющих ссылок, указывая различным клиентам на разные файлы лицензий.

Наличие сложных требований к распространению программ – это обычная проблема (Hemmerich 2000). Это область, которую люди постоянно стараются улучшить. Прежде чем пытаться решить проблему своими силами, обратитесь к опыту других людей, изложенному в материалах конференций и журналах. Может быть, кто-то уже решил именно вашу проблему.

28.2.4. Граждане второго сорта

Базы программного обеспечения также должны справляться с редкими ОС, которые могут существовать в сети. Эти узлы, часто называемые «гражданами второго сорта», имеют ОС, которые не получают полную поддержку, положенную «гражданам первого сорта» (см. раздел 3.1), но существуют в вашей сети и требуют минимальной поддержки. Поддержкой, которую получают эти «граждане второго сорта», может быть просто выделение IP-адреса и настройка других простых параметров конфигурации, чтобы устройство работало.

База программного обеспечения, необходимая для ОС «граждан второго сорта», обычно минимальна: приложения, требуемые для особых задач этой машины, возможно, компиляторы, и средства, которые требуются системным администраторам. Мы настоятельно рекомендуем не пытаться предоставить каждый пакет, который есть в полных базах. Это потребует больших усилий при малой отдаче.

Важно иметь письменную политику по ОС «граждан второго сорта». Укажите уровень поддержки, на который можно рассчитывать, и области, в которых для пользователей предполагается самостоятельная поддержка. В политике для небольшой базы программного обеспечения должен быть указан минимальный набор пакетов, которые пользователи могут рассчитывать найти в базе.

Мы рекомендуем включать в небольшую базу несколько групп инструментов. Установите средства, необходимые для выполнения задачи машины. Например,

[1] Мы рекомендуем централизацию серверов лицензий, но включили этот пример, поскольку часто видим, что по политическим причинам они не централизованы.

если это машина для переноса программ на данную ОС, установите соответствующую цепочку инструментов компилятора. Если узел нужен для запуска конкретного приложения или службы, установите необходимые для этого программы. Средства, необходимые для процессов системного администрирования – автоматизированные или нет, – также должны быть установлены. Они включают программы сбора информации об оборудовании, средства обновления логов, резервного копирования, обновления базы программного обеспечения, инструменты отладки и т. д. Наконец, у каждой компании есть небольшой список средств для повышения удобства, которые можно предоставить для вашей же пользы, – в их числе консольная версия корпоративного телефонного справочника, минимальные конфигурации электронной почты («только отправка») и т. д.

Цепочка инструментов

Цепочка инструментов разработчика – это специальные программы, необходимые для создания программ. В некоторых системах она может включать программы от различных разработчиков или из разных источников. Обычно в нее входят средства сборки, например `make` и `autoconf`, компиляторы, ассемблеры, компоновщики, интерпретаторы, отладчики, системы контроля исходного кода, например SubVersion, CVS, Perforce, ClearCase и Source Safe, а также различные собственные утилиты, используемые в процессе разработки. Термин *«цепочка»* означает, что один инструмент часто передает данные другому, например, как в последовательности компиляции/ассемблирования/компоновки.

28.3. Заключение

В данной главе мы рассмотрели базы программного обеспечения. Базы программного обеспечения – это организованный способ распространения программных пакетов на большое количество узлов, хотя хорошая организация полезна даже для одного узла. Хорошая база программного обеспечения предоставляет полный набор инструментов, которые становятся частью культуры ваших пользователей и самой сети.

В системах Windows базы программного обеспечения обычно организуются иначе по историческим, техническим и культурным причинам. Базы в Windows – это обычно хранилища программ для установки, а базы в UNIX – хранилища программ, используемых в реальном времени из базы.

В организациях должна быть письменная политика, охватывающая различные вопросы баз программного обеспечения: как и кем устанавливаются программы, какие системы обслуживаются базой, как выполняются запросы и поддержка и т. д.

Мы описали простые базы как для Windows, так и для UNIX, показав, что политика и организация являются основными принципами и можно создать очень мощную базу при помощи даже малого количества программ. Есть много пакетов с открытым исходным кодом для управления базами, поэтому мы не рекомендуем создавать их с нуля. Найдите тот, который вам понравится, и приспособьте его под свои потребности.

Несмотря на то что задача базы программного обеспечения – предоставлять одни и те же программы большому количеству узлов, вы также будете получать запросы на индивидуальную настройку конкретных узлов или групп узлов. Мы рассмотрели наиболее распространенные типы запросов и некоторые простые решения.

Задания

1. Опишите базу программного обеспечения, используемую в вашей среде, ее преимущества и недостатки. Если у вас нет базы, расскажите, куда устанавливаются программы, а также перечислите преимущества и недостатки создания базы.
2. Каковы политики вашей базы программного обеспечения? Если у вас нет никаких политик или базы, разработайте набор политик для базы вашей компании. Обоснуйте решения, принятые в политике для вашей базы.
3. Что происходит с модулями и другими дополнительными пакетами perl в примере для UNIX (раздел 28.1.6)? Как бы вы разрешили эту ситуацию?
4. Сравните свою базу программного обеспечения с одним из примеров, описанных в этой главе. Насколько она лучше или хуже?
5. Хорошая система управления базой программного обеспечения может также отслеживать использование. Как можно воспользоваться статистикой использования для лучшего управления базой?
6. Если вы работаете в небольшой организации, которой не требуется сложная база программного обеспечения, опишите, какой тип простой базы программного обеспечения у вас есть. На каком этапе компания вырастет настолько, что вам потребуется более сложная база? Какой она может быть? Как вы перейдете на эту новую систему?
7. Разработайте набор кодов для каждой ОС и различных версий каждой системы, которая у вас используется, подобный описанным в разделе 28.1.2. Объясните и обоснуйте ваши решения.

Глава 29

Веб-службы

Управление веб-системами стало такой крупной и важной частью системного администрирования, что, помимо простой загрузки Apache или IIS, возникли особые подходы и специальности. Теоретически мы уже охватили весь материал, необходимый для успешного запуска веб-службы или веб-приложения. Просто купите серверное оборудование, установите нужные службы, создайте быструю сеть с тщательно организованными пространствами имен в информационном центре, задокументируйте все, создайте надежный план аварийного восстановления, учитывайте вопросы безопасности, устраняйте возникающие проблемы, придерживайтесь строгих правил управления изменениями, при необходимости обновляйте систему, применяя хорошую стратегию технических перерывов, осуществляйте мониторинг системы для обнаружения неполадок и планирования емкости, обеспечьте достаточное пространство для хранения данных и хорошую систему резервного копирования и восстановления. Все это было рассмотрено в главах 4–10, 11, 15, 17, 18, 20, 22, 25 и 26. Однако некоторые важные методы и вопросы все-таки не были рассмотрены в этих главах.

Веб-сайт – это способ представления пользователями информации и приложений при помощи модели клиент/сервер. Доступ к веб-контенту обычно осуществляется клиентской программой, называемой **броузером**, но может выполняться любой программой, поддерживающей HTTP. Веб-сервер предоставляет документы, называемые **страницами**, в формате HTML, а также любое содержимое, присутствующее на странице HTML, например графику, аудиофайлы и т. д. Иногда содержимое включает программы, написанные на языках программирования, например на JavaScript, которые будут запускаться броузером клиента.

Сеть основана на открытых стандартах, это означает, что они разрабатываются международным комитетом, а не одной корпорацией. Они могут использоваться без оплаты за использование собственности или лицензию. Веб-стандарты определяются WWW-консорциумом (World Wide Web Consortium – W3C), а лежащие в их основе протоколы Интернета определяются IETF.

Преимущество веб-приложений в том, что один броузер может осуществлять доступ ко многим веб-приложениям. Веб-броузер – это **универсальный клиент**.

Кроме того, веб-приложения и небольшие веб-серверы есть в прошивках многих устройств, например небольших маршрутизаторов и коммутаторов, интеллектуальных дисковых массивов и сетевых компонентов.

Возможности открытых стандартов

Представьте, что вместо применения открытых стандартов какая-то компания установила бы свои стандарты и назначила плату за их использование на веб-сайте или в броузере. Сеть никогда не стала бы такой развитой, как сейчас. На самом деле предпринималась одна попытка создания чего-то подобного незадолго до того, как Сеть стала набирать популярность: Network Notes был результатом сотрудничества AT&T, Lotus и Novell. Можно было пользоваться только программами Novell/Lotus и сетью AT&T и связываться только с другими пользователями Network Notes.

Люди не хотели платить деньги за программы, потому что не было сайтов, на которые они могли зайти; никто не хотел создавать сайты, поскольку ни у кого не было программ для доступа к ним. Разработчики не хотели предоставлять программы бесплатно, потому что им нужно было возместить свои расходы на ее разработку.

Даже если бы эта служба стала популярной, такая инновация была бы подавлена другими способами. Без возможности производителей создавать собственное клиентское программное обеспечение никто не смог бы экспериментировать с созданием броузеров для других устройств. Броузеры для сотовых телефонов могли бы никогда не появиться.

Эта информация актуальна, потому что, даже учитывая успех Интернета, компании постоянно упрямо повторяют эти ошибки. Постоянно совершаются попытки расширить веб-броузеры такими способами, которые ограничивают пользователей, – на самом деле они отпугивают потенциальных пользователей.

29.1. Основы

В данном разделе мы рассмотрим основные элементы, которые составляют веб-службу, распространенные используемые архитектуры и меры, необходимые для создания безопасной, расширяемой, наблюдаемой и простой в управлении службы.

29.1.1. Основные элементы веб-службы

Унифицированный указатель ресурса (Uniform Resource Locator – URL) – это адрес информации в Сети. URL состоит из имени узла и пути к ресурсу, например *http://www.EverythingSysadmin.com/*.

Веб-сервер получает HTTP-запросы и предоставляет в ответ какие-то данные. Вот некоторые распространенные программные пакеты веб-серверов: Apache HTTP, AOLServer и Microsoft IIS.

Ответ обычно является статическим файлом. Однако иногда ответ генерируется по запросу при помощи интерфейса CGI (Common Gateway Interface – общий шлюзовой интерфейс). Сгенерированное, или динамическое, содержимое часто является результатом запроса к базе данных. Есть два типа скриптов CGI: `GET` и `POST`. `GET` получает входные данные – значения, присвоенные именам перемен-

ных, – и использует их для чтения результата. Например, `http://google.com/finance?q=aapl` – это запрос `GET`. `POST` получает входные данные и использует их для какого-либо изменения, например обновления корзины в интернет-магазине, отправки сообщения в блог или удаления файлов.

`POST` не помещает входные данные в URL, а размещает их в самом HTTP-запросе. Следовательно, входные данные могут быть гораздо больше, так как для них не действует ограничение на длину URL.

Здесь важно отметить, что `GET` – это только чтение, а `POST` – обновление. Когда механизм поиска идет по Сети для создания базы поиска, он не следует запросам `POST`. Были известные случаи, когда программисты случайно писали приложение, в котором кнопка УДАЛИТЬ была создана при помощи скрипта `GET`, а не `POST`, и каждый раз, когда поисковый робот находил этот сайт, данные удалялись.

Другие технологии динамически создаваемых веб-страниц включают внутренний интерпретированный код с использованием таких систем как PHP (*www.php.net*) и Microsoft Active Server Pages. Нормальная во всех других отношениях HTML-страница хранится на сервере, но в нее включены специальные инструкции, которые веб-сервер интерпретирует перед подачей страницы. Инструкция может предписывать выполнить запрос в базе данных и показать результаты в виде таблицы. Пользователь видит веб-страницу с динамически генерируемой таблицей в середине.

Веб-клиент получает страницу, интерпретирует ее и отображает пользователю. Веб-броузер – это **универсальный клиент**. Раньше каждому серверному приложению требовалось развертывание особых клиентских программ, что тормозило прогресс. Революционной Сеть делает возможность создания новых служб без необходимости написания новых клиентских программ.

Броузер интерпретирует и отображает страницу, которая была предоставлена. HTML-данные интерпретируются и отображаются. Иногда включается и интерпретируется на клиенте встроенный язык программирования, например ECMAScript, более известный как JavaScript. Другие форматы файлов также требуют интерпретации, например форматы фотографий, видео, аудио и т. д.

AJAX – это не протокол, а метод создания интерактивных веб-страниц. Часто они так же интерактивны, как традиционные PC-приложения. Доступ к серверу осуществляется только в определенное время для обновления и серьезных изменений состояния, что снижает нагрузку на сервер и повышает гибкость. Термин складывается из названий двух основных элементов – JavaScript и XML. Пользовательский интерфейс реализован главным образом на JavaScript, который имеет возможность асинхронной связи с сервером для получения при необходимости дополнительной информации, не ожидая, пока пользователь щелкнет по кнопке ПОДТВЕРДИТЬ, как в операциях `GET` и `POST` в HTTP.

Веб-клиенты существуют не только для компьютеров, и сейчас они есть в сотовых телефонах, телевизорах и автономных терминалах. Даже бытовая техника конфигурируется, используя HTTP для загрузки файла конфигурации с центрального сервера или операцию HTTP `POST` для соединения с производителем и запроса на обслуживание.

В 2007 году около 1 млрд человек осуществляли доступ в Интернет исключительно с мобильных телефонов. Миллионы никогда не видели Интернет с компьютера.

В Сети используется много форматов данных. Веб-сервер обычно выдает веб-страницы, мультимедийные файлы или сообщения об ошибках.

Обычно веб-страницы имеют формат HTML или производный от него, например XHTML, DHTML, XML и т. д. Некоторые из этих форматов старые, и их употребление не приветствуется, другие – новые и развивающиеся. Мультимедийные файлы включают изображения, аудио и видео. Все время появляются новые мультимедийные форматы. Обычно данными нельзя пользоваться, пока не будет получен последний байт, хотя веб-броузеры прекрасно справляются с отображением промежуточных результатов по мере получения данных, чтобы создать ощущение более быстрого просмотра. Однако некоторые мультимедийные ресурсы используют **потоковые** форматы, которые отображаются в реальном времени и предоставляют функции паузы и перемотки вперед и назад. Потоковые данные особенно важны для аудио и видео в прямом эфире. Было бы бессмысленно загружать весь эфир радиостанции за день, а затем прослушивать его после полной загрузки. В формате потокового аудио радио можно слушать в прямом эфире.

Существует много специальных форматов, которые часто строятся на основе других. XML – отличный формат для создания других форматов, или **микроформатов**. Одним из популярных микроформатов является **RSS-канал**, формат, который указывает таблицу содержимого ресурса, например блога или новостного сайта. Сайты википедий (см. главу 9) часто представляют в виде RSS-канала список недавно измененных страниц. Специальные программы для чтения RSS сканируют много RSS-каналов и показывают пользователю новое содержимое.

Для неудачных HTTP-запросов есть стандартный набор кодов ошибок и состояний. Их содержимое обычно неважно для пользователей, но очень значимо для системных администраторов. Коды представляют собой трехзначные числа. Первая цифра, 1, используется для информационных сообщений, 2 показывает успех, 3 – перенаправление, а 4 – ошибку. Вот несколько распространенных кодов:

- *200* (OK); запрос выполнен.
- *301* (Перемещено навсегда); результат: мы хотим, чтобы вы запомнили новый URL и в следующий раз заходили на него напрямую.
- *302* (Перенаправление на указанный URL).
- *307* (Перенаправление на указанный URL в качестве временной меры).
- *401* (Пожалуйста, попробуйте еще раз с аутентификацией).
- *403* (Нет авторизации, неверный пароль или другая проблема).
- *404* (Такая страница не найдена).

Системным администраторам часто требуется знать эти коды ошибок для устранения проблем или предоставления лучшего обслуживания. Например, при отладке аутентификации важно знать, что страница, которая требует аутентификации, обычно сначала запрашивается без аутентификации и броузер получает код 401. Затем страница повторно запрашивается с прикрепленной информацией аутентификации, например именем пользователя и паролем. Ошибка 404, «Страница не найдена», является важной, поскольку все, что в этом случае получает пользователь, – это сообщение об ошибке, которое не надо путать с искомой веб-страницей. Эту страницу сообщения об ошибке можно настроить.

29.1.2. Роль веб–мастера

Веб-мастер – это человек, который управляет содержимым веб-сайта, во многом подобно тому, как редактор управляет содержимым газеты. Он отвечает за установку политики веб-сайта. Эту роль часто путают с системным администратором веб-сервера, который устанавливает сервер, программы и т. д. Веб-мастер занимается содержимым, системный администратор веб-сервера поддерживает технические устройства – физические и виртуальные, – которые составляют веб-сайт.

Эту путаницу можно понять, потому что в небольших компаниях один человек может выполнять обе задачи, но даже в крупных компаниях эти две роли путают, если руководители не являются технически осведомленными. Подчеркните различие, четко объяснив его руководителям в терминах, которые они понимают, и разместите эти роли в различных подразделениях или двух разных бюджетах.

Для системных администраторов, которых вынуждают выполнять обязанности веб-мастера, у нас есть следующая рекомендация. Сосредоточьтесь на том, чтобы позволить людям выполнять обновления. Создайте структуру, но используйте программное обеспечение, которое обеспечивает самообслуживание вебсайта.

Если от вас требуют обновлять веб-страницы, согласуйте политику, чтобы такие требования не были сюрпризом. Есть довольно много историй о том, как системные администраторы уже собирались уходить домой на выходные, когда их внезапно просили внести ряд изменений, на которые требовалось несколько часов. Установите SLA, указывающее, что изменения должны запрашиваться за определенное количество часов или дней, или определяющее график, например, с выполнением существенных обновлений по понедельникам, незначительных изменений в течение 8 ч, и процесс для обработки экстренных запросов. Если это вообще возможно, примите участие в процессах, которые приведут к таким изменениям на веб-сайте, которые снизят число неожиданностей. В разделе 29.1.8.2 рассмотрено больше примеров.

29.1.3. Соглашения об уровне обслуживания

Как и любой другой службе, веб-службе требуется SLA и мониторинг для обеспечения его соблюдения. Многие пользователи привыкли думать о Сети, как о критической службе в режиме 24/7, но SLA конкретной веб-службы может довольно сильно отличаться. У большинства внутренних веб-служб будут такие же SLA, как и у других офисных служб, таких как печать или хранение.

Если вам трудно создать подходящее SLA для веб-службы, обратитесь к группе пользователей, которые будут ее применять. В идеальном случае, как и с любым SLA, уровень обслуживания должен устанавливаться в контакте с сообществом пользователей. Мы рекомендуем вам отклонять любое SLA, которое не позволяет проводить периодическое обслуживание, если служба не построена на избыточной инфраструктуре. Если служба предоставляется одним узлом или общим веб-узлом и должна быть доступна круглосуточно, пора обсудить повышение избыточности службы.

Показатели, которые входят в SLA для веб-службы, должны включать задержку для определенного уровня запросов в секунду (Queries Per Second – QPS). То

есть сколько времени займет определенный запрос при определенной нагрузке системы? Задержка обычно измеряется как время между приемом первого байта запроса и отправкой последнего байта ответа.

29.1.4. Архитектуры веб-служб

Различным типам содержимого требуются разные инфраструктуры подачи. Потребности одиночного веб-сервера, предоставляющего неизменный документ, отличаются от потребностей страницы, предоставляющей динамическое содержимое. Веб-серверы, которые будут доступны из Интернета, а не только внутри организации, требуют особого внимания к безопасности.

29.1.4.1. Статический веб-сервер

Статический веб-сервер – это сервер, который предоставляет только те документы, которые не изменяются или изменяются редко. Документы статичны в том плане, что они читаются напрямую с диска и не изменяются в процессе доставки веб-сервером. Сами документы – это обычные документы любого типа, например веб-страницы, изображения, текст, электронные таблицы и т. д.

Документы предоставляются из **корневого каталога документов**. Если это общий том, для различных групп пользователей можно создать поддиректории с соответствующими правами доступа. Тогда каждая группа сможет публиковать информацию, просто создавая и обновляя файлы. Веб-страницы можно редактировать в обычных офисных приложениях или в специальных редакторах веб-страниц, которые имеются для большинства операционных систем.

При больших уровнях QPS важно, чтобы у такого сервера было достаточно оперативной памяти для кэширования наиболее часто запрашиваемых файлов.

29.1.4.2. CGI-серверы

CGI-серверы динамически генерируют страницы, как было описано выше. Из-за того что для каждой страницы выполняется большое количество работы, эти серверы часто не могут предоставлять в секунду столько же страниц, сколько статические серверы.

При высоких уровнях QPS у такого сервера должно быть достаточно ресурсов процессора, чтобы справляться с запросами. Программное обеспечение также может зависеть от других факторов, таких как оперативная память и сеть.

29.1.4.3. Веб-сайты на основе баз данных

Один из наиболее распространенных типов веб-приложений – доступ к информации в базе данных и ее модификация. Примеры веб-приложений, основанных на базе данных – это обновление ваших настроек на сайте социальной сети, каталоги интернет-магазинов или выбор курсов на следующий семестр. Веб-приложения заменяют бумажные формы и позволяют людям напрямую взаимодействовать с базой данных.

Сайты на основе баз данных создают шаблон для определенного типа данных, а не отдельные веб-страницы. Например, книжному интернет-магазину не нужно создавать веб-страницу для каждой книги, которая в нем продается. Вместо этого его каталог записан в базе данных, а любой конкретный объект может отображаться при заполнении шаблона информацией из базы данных.

Информация может доставляться из нескольких источников, например цены и информация о наличии товара могут располагаться в разных базах данных. Для глобального изменения формата можно просто обновить шаблон.

Представьте, что при необходимости изменить меню требовалось бы вручную редактировать каждую страницу на сайте. Такой сайт был бы неуправляем. Однако мы постоянно удивляемся, находя веб-сайты, которые начинали с ручного редактирования каждой страницы и до сих пор не перешли на систему на основе базы данных. Ваша обязанность как системного администратора – призывать такие сайты переходить на модель на основе базы данных в минимальные сроки.

При высоких уровнях QPS такой сайт должен расширяться, как любая база данных, при помощи обычных средств повышения быстродействия баз данных.

29.1.4.4. Мультимедийные серверы

Мультимедийный сервер – это в первую очередь веб-сервер, на котором есть содержимое, включающее медиа-файлы, например, видео или аудио. Медиа-файлы часто являются очень большими, и доступ к ним иногда осуществляется при помощи специального клиента или броузера, чтобы соответствовать управлению правами на цифровую информацию. При предоставлении медиа-файлов более важными становятся хранение данных и пропускная способность сети.

Медиа-серверы предоставляют поддержку **потоковой передачи**. Обычно потоковая передача – это просто применение веб-приложения на сервере для предоставления медиа-файла по отличному от HTTP протоколу, чтобы его можно было просмотреть в реальном времени. Сервер предоставляет поток данных специализированному приложению. Например, вы можете слушать интернет-радиостанцию в своем проигрывателе или аудиоклиенте компании. Часто задача приложения медиа-сервера – обеспечивать защиту от копирования или управление правами. Другая задача – контролировать скорость передачи информации по соединению, чтобы данные отображались с правильной скоростью, если веб-сайт не позволяет конечному пользователю просто загрузить медиа-файл. Приложение обычно осуществляет буферизацию данных за несколько секунд, чтобы можно было компенсировать задержки. Кроме того, потоковые серверы предоставляют функции прямой и обратной перемотки.

При работе с медиа-сервером, который передает много одновременных потоков, при выборе возможностей сети и системы хранения важно учитывать скорость воспроизведения типа данных, который вы предоставляете. В главе 25 мы указали некоторые характеристики массивов хранения, которые оптимальны для работы с редко обновляемыми большими файлами. Уделяйте особое внимание памяти и пропускной способности сети, потому что полная загрузка файла может потребовать много памяти и других системных ресурсов.

Для потоковых серверов делается все возможное, чтобы не перегрузить диск. Если несколько человек смотрят один и тот же поток, но начали в разное время, система может повторно читать одни и те же данные для предоставления обслуживания, но вам лучше избегать этого. Некоторые потоковые приложения загружают весь медиа-файл в память и отслеживают отдельные подключения к нему, выбирая, какие биты каким открытым соединениям отправлять. Если только один пользователь просматривает файл, хранить его в памяти неэффективно, но для нескольких пользователей это оправданно. При использовании

этого метода производительность значительно превосходит чтение с диска, но может потребоваться много памяти. К счастью, существуют альтернативы.

При других реализациях в память загружается фиксированная часть медиафайла для каждого соединения и отправляются соответствующие биты. Это может быть очень эффективно, так как многие операционные системы хорошо кэшируют данные в памяти. Размер часового видеоклипа может составлять несколько гигабайтов. Но в системной памяти не нужен одновременно весь файл, только несколько мегабайтов, которые приложение отправит каждому открытому соединению в следующий раз. Пользователи, которые подключаются через небольшое время друг за другом, увидят хорошую реакцию, потому что сегменты еще будут находиться в памяти и их не понадобится читать с диска. Этот подход обеспечивает быстрое время реакции за счет использования кэша, но возможно более эффективное потребление ресурсов.

Для любого типа потокового медиа-сервера важна также скорость процессора. Иногда аудио- или видеофайл хранится в высоком качестве и по запросу перекодируется в меньшем разрешении в зависимости от потребностей пользователя, который его запрашивает. Выполнение этого процесса в реальном времени – очень дорогая операция, которая требует значительного количества процессорного времени. Во многих случаях для выполнения обработки используются специализированные аппаратные платы, что позволяет снизить загрузку на процессор и обеспечить для него лучшую возможность выполнять остальную работу по перемещению данных с диска, через карту и в сеть.

LAMP и другие технические термины

Некоторые комбинации технологий, или платформы, являются достаточно распространенными и поэтому получили собственное название. Обычно эти платформы включают ОС, веб-сервер, базу данных и язык программирования, используемый для создания динамического содержимого. Наиболее распространенная комбинация – это **LAMP**: Linux, Apache, MySQL и Perl. LAMP также может означать «Linux, Apache, MySQL и PHP» и «Linux, Apache, MySQL и Python».

Преимущество присвоения названия определенной платформе заключается в том, что, когда все пользуются одним словом для обозначения чего-либо, снижается путаница.

29.1.4.5. Несколько серверов на одном узле

Есть два основных варианта предоставления отдельного сервера без необходимости наличия отдельной машины. В первом методе веб-сервер может располагаться на той же самой машине, но устанавливаться в другую директорию и настраиваться для ответа по порту, отличному от обычного порта 80. Например, при настройке на порте 8001 адрес веб-сервера будет *http://my.web.site:8001/*. В некоторых системах, где использование больших номеров портов не ограничено только для привилегированных пользователей или администраторов, применение альтернативного порта позволяет группе поддерживать собственный веб-сервер без необходимости привилегированного доступа. Это может быть очень полезно для администратора, который хочет минимизировать

привилегированный доступ для персонала, не занимающегося системным администрированием. Проблема этого подхода в том, что многие пользователи будут просто забывать указывать номер порта, и придут в замешательство, когда увидят не тот веб-сайт, который ожидали.

Другой вариант размещения нескольких веб-сайтов на одной и той же машине *без* использования альтернативных портов – это наличие нескольких сетевых интерфейсов, каждый со своим IP-адресом. Так как сетевые службы на машине можно привязать к отдельным IP-адресам, сайты можно поддерживать отдельно. Если не добавлять дополнительного оборудования, большинство операционных систем позволяют одному физическому сетевому интерфейсу работать как несколько *виртуальных интерфейсов* (Virtual InterFace – VIF), каждый из которых имеет свой IP-адрес. Все сетевые службы на машине можно привязать к отдельному адресу VIF и таким образом совместно пользоваться сетевым интерфейсом без конфликтов. Если определить VIF таким образом, что у каждой внутренней группы пользователей или подразделения будет собственный IP-адрес на общем узле, для каждой группы можно создать отдельную установку веб-сервера в ее директорию.

Дополнительное преимущество этого подхода заключается в том, что, несмотря на несколько больший объем работ в начале, он очень быстро расширяется. Так как сервер каждой группы настраивается отдельно и работает на собственном IP-адресе, отдельные группы можно очень легко переводить на другие машины, если первоначальный узел перегружается. IP-адрес просто отключается на первоначальной машине и устанавливается на новом узле, а веб-службы полностью переносятся, включая скрипты автозагрузки в операционной системе.

29.1.5. Мониторинг

Мониторинг ваших веб-служб позволяет вам выяснить, насколько хорошо вы расширяетесь, определить направления совершенствования и убедиться в том, что вы выполняете свое SLA. Большая часть информации, необходимой вам для организации мониторинга веб-служб, рассмотрена в главе 22.

Вы можете захотеть внести в свой мониторинг несколько элементов, характерных именно для Сети. Ошибки веб-серверов чаще всего связаны с проблемами с содержимым сайта, и информация о них часто является ценной для группы веб-разработчиков. Определенные ошибки или тенденции повторения ошибок могут быть показателем проблем пользователя со скриптами сайта. Другие ошибки могут показывать попытку вторжения. Такие ситуации требуют дальнейшего изучения.

Обычно веб-серверы поддерживают сохранение типа броузера и URL страницы, содержащей ссылку, которая привела на ваш сайт (сославшийся URL). На некоторых веб-серверах имеется характерная для сервера информация, которая также может быть полезной, например данные в активных потоках и использование памяти по потокам. Мы призываем вас ознакомиться с любой особой поддержкой расширенного мониторинга, доступной на платформе вашего веб-сервера.

29.1.6. Расширение веб-служб

Майк О'Делл (Mike O'Dell), основатель первого интернет-провайдера (UUNET), как-то сказал: «Расширение – это единственная проблема Интернета. Все остальное – это следствия».

Если ваш веб-сервер будет успешным, вы будете перегружены запросами. Возможно, вы уже слышали фразу «slashdot-эффект» или «они попали под slashdot». Эта фраза относится к популярному новостному интернет-сайту (Slashdot.org) с таким большим количеством читателей, что любой сайт, упомянутый в его статьях, часто перегружается и не справляется с запросами.

Есть несколько методов расширения. Небольшая организация с базовыми потребностями может повысить быстродействие веб-сервера просто за счет модернизации процессора, дисков, памяти и сетевого подключения – по отдельности или вместе.

Когда дело касается нескольких машин, двумя основными типами расширения являются *горизонтальный* и *вертикальный*. Они получили свое название из схем архитектуры. При изображении схемы кластера веб-службы машины, добавляемые для горизонтального расширения, обычно находились в одном ряду, или на одном уровне, а для вертикального – группировались вертикально, вдоль пути прохождения запроса через различные подсистемы.

29.1.6.1. Горизонтальное расширение

При **горизонтальном расширении** веб-сервер или ресурс веб-службы воспроизводится, а загрузка разделяется между воспроизведенными ресурсами. В качестве примера можно привести два веб-сервера с одним содержимым, каждый из которых получает примерно половину запросов.

Исходящие запросы должны направляться на различные серверы. Один из способов добиться этого – пользоваться *циклическими* записями на DNS-серверах. DNS настраивается таким образом, чтобы в ответ на запрос IP-адреса одного имени (*www.example.com*) в случайном порядке выдавались разные IP-адреса. Клиент обычно пользуется только первым полученным IP-адресом, таким образом, нагрузка распределяется по различным копиям.

У этого метода есть недостатки. Некоторые операционные системы или броузеры, которые в них работают, кэшируют IP-адреса, что делает циклическую службу имен бессмысленной. Кроме того, такой подход может стать проблемой при сбое сервера, так как служба имен может продолжать предоставлять адрес нефункционирующего сервера в ответ на входящие запросы. Для запланированных обновлений и обслуживания адрес сервера обычно удаляется из службы имен. Срок действия записи об имени обычно истекает через некоторое время, и это время контролируется в DNS. Для запланированного обслуживания срок действия можно заранее снизить, чтобы удаление прошло быстро. Однако внимательное отношение ко времени окончания срока действия записей DNS для запланированных отключений не помогает при неожиданных сбоях. Лучше иметь способ выбора, адрес какого сервера предоставлять в ответ на любой запрос.

Наличие аппаратного *устройства балансировки нагрузки* является лучшим решением, чем использование DNS. Устройство балансировки нагрузки расположено между веб-броузером и серверами. Броузер подключается к IP-адресу устройства балансировки нагрузки, который прозрачно направляет запрос одному из дублирующих серверов. Устройство балансировки нагрузки следит за тем, какие серверы отключаются, и перестает направлять трафик на узел, пока тот не вернется в рабочее состояние. Также можно реализовать другие усовершенствования, например направление запросов на наименее загруженный сервер.

Устройства балансировки нагрузки обычно являются формирователями протоколов и трафика общего назначения, при необходимости направляя запросы не

только HTTP, но и других протоколов. Это предоставляет гораздо бóльшую гибкость в создании архитектуры веб-служб. Перераспределять можно практически любую нагрузку, и это может быть отличным способом улучшения как быстродействия, так и надежности.

> Один из ранних проектов веб-службы Страты, казалось, шел хорошо, но во время долгих тестов система обмена сообщениями была подвержена непонятным ошибкам. Казалось, что проблема была связана с балансом нагрузки обращений к директории LDAP, – когда разрешались прямые подключения к серверам LDAP, проблема не возникала. Внимательная отладка системными администраторами показала, что устройства балансировки нагрузки отключали неактивное соединение из-за превышения времени ожидания, не выполняя необходимой операции закрытия TCP-соединения. Сервер обмена сообщениями не открывал новое соединение после того, как старое превышало интервал ожидания, потому что операционная система не освобождала соединение.
>
> К счастью, один из системных администраторов другой части проекта был знаком с таким поведением и только он знал двух производителей, чьи коммутаторы балансировки нагрузки выполняли TCP-команду `FIN` при закрытии соединения с превышением интервала ожидания. Системные администраторы заменили оборудование – и архитектура заработала, как было задумано. После этого разработчик операционной системы исправил свой стек обработки протокола TCP, чтобы стало возможно закрывать соединение после определенного времени ожидания `FIN_WAIT`. Подобные проблемы будут возникать в будущем с расширением протоколов и изменением оборудования.

29.1.6.2. Вертикальное расширение

Другой способ расширения – разделить различные виды служб, используемых при создании веб-страницы, а не дублировать всю машину. Такое **вертикальное расширение** позволяет вам создать архитектуру с более тонкой обработкой, выделить больше ресурсов на наиболее интенсивно используемые этапы создания страницы. Кроме того, исключается конкуренция различных типов запросов на ресурсы одной системы.

В качестве хорошего примера такого расширения можно привести сайт, содержащий некоторое количество больших видеоклипов и приложение с кратким опросом о видеоклипе. Чтение больших видеофайлов при одновременной попытке записать много небольших обновлений в базу данных на том же диске – это неэффективный способ использования системы. В большинстве операционных систем есть алгоритмы кэширования, которые автоматически настраиваются для чего-то одного, но плохо работают при одновременном выполнении двух действий. В этом случае все видеоклипы должны размещаться на отдельном веб-сервере, возможно, с оптимизированным под получение крупных файлов массивом хранения. Оставшаяся часть веб-сайта должна оставаться на первоначальном сервере. Теперь, когда большие видеоклипы находятся на отдельном сервере, первоначальный сервер может обрабатывать больше запросов.

Как вы могли догадаться, горизонтальное и вертикальное расширения можно объединить. Веб-сайту с опросом о видеоклипах может быстрее понадобиться

еще один сервер для видеоклипов, чем возникнет необходимость расширять приложение формы опроса.

29.1.6.3. Выбор метода расширения

Вашему сайту может требоваться горизонтальное или вертикальное расширение либо какая-то их комбинация. Чтобы разобраться, что вам нужно, классифицируйте различные компоненты, используемые с вашим веб-сервером, по ресурсам, которые они больше всего потребляют. Затем определите, какие компоненты конкурируют друг с другом и не вмешивается ли какой-то компонент в работу других компонентов.

Сайт может включать статические файлы, CGI-программы и базу данных. Статические файлы могут варьироваться от сравнительно небольших документов до крупных мультимедийных файлов. CGI-программы могут интенсивно использовать память или ресурсы процессора, а также выдавать большие объемы выходных данных. Базы данных обычно требуют львиную долю системных ресурсов.

Пользуйтесь диагностикой системы и логами, чтобы посмотреть, какие типы ресурсов используются этими компонентами. В некоторых случаях, таких как сайт опроса о видеоклипах, вы можете предпочесть перенести часть службы на другой сервер. Другой пример – веб-сервер подразделения информационных систем, который также используется для создания графиков системных логов. Этот процесс может очень интенсивно загружать процессор, поэтому скрипты построения графиков и данные логов можно перенести на другую машину, а другие скрипты и данные – оставить.

В расширении хорошо то, что его можно выполнять поэтапно. Вы можете на каждом этапе повышать общую производительность, и вам необязательно определять точный профиль использования ресурсов после первой попытки.

Заманчиво оптимизировать много элементов сразу. Однако мы рекомендуем поступать наоборот. Определите наиболее перегруженный компонент и отделите его или продублируйте. Затем, если проблема еще не исчезла, повторите процесс для следующего перегруженного компонента. Выполнение расширения по одному компоненту за раз дает лучшие результаты и существенно упрощает тестирование. Кроме того, может быть проще обеспечить финансирование постепенных усовершенствований, чем одной крупной модернизации.

29.1.6.4. Проблемы расширения

Расширение подсистем, которые используют общий ресурс, может быть сложным. Если веб-сайт содержит приложения, которые поддерживают состояние, например если вы заполнили какие-то страницы регистрационной формы, это состояние должно либо поддерживаться броузером клиента, либо быть каким-то образом доступным для любых систем, которые могут обрабатывать следующий запрос.

Это было общей проблемой первых систем балансировки нагрузки, и Страта помнит создание громоздких архитектур сетевой топологии для обхода проблемы. Современные устройства балансировки нагрузки могут отслеживать виртуальные сеансы между клиентом и веб-сервером и направлять дополнительный трафик от данного конкретного клиента на правильный веб-сервер. Методы, позволяющие это сделать, до сих пор совершенствуются, так как в наше время

многие организации скрыты за шлюзами трансляции сетевых адресов (Network Address Translation – NAT) или брандмауэрами, из-за которых все запросы выглядят так, как будто они были отправлены с одного IP-адреса.

CGI-программы или скрипты, которые управляют информацией, часто используют локальный файл блокировки для контроля доступа. Если эти программы будут размещаться на нескольких серверах, лучше всего изменить GCI-программу, чтобы она использовала базу данных для хранения информации. Тогда процедуры блокировки базы данных могут заменить файл блокировки.

Расширение использования базы данных может быть проблемой. Обычный метод расширения – купить более быстрый сервер, но он работает только до определенного момента, а цены все растут. Лучший способ расширения сайтов на основе баз данных – разделить данные на предназначенные только для чтения и для чтения и записи. Данные только для чтения могут быть продублированы в дополнительных базах данных для использования при построении страниц. Когда требуется частый доступ к базе данных для записи, лучше всего структурировать базу данных так, чтобы запись происходила в различные таблицы. Затем можно расширяться за счет размещения определенных таблиц на различных серверах для записи.

Другая проблема, вызванная расширением, заключается в том, что странице может потребоваться получать данные из различных источников и использовать их для совместного отображения. Продукты для репликации баз данных, например Relational Junction, позволяют системному администратору дублировать таблицы из различных типов баз данных, например MySQL, Postgres или Oracle, и объединять их для общего просмотра. Мы прогнозируем расширение применения средств этих типов по мере роста необходимости расширения доступа к базам данных.

Важность расширения

Все думают, что расширение для них не важно, пока не становится слишком поздно. На сайте избирательной комиссии Флориды было очень мало информации, а соответственно, и трафика. Во время выборов 2000 года в США сайт был перегружен людьми, которые думали, что могут найти там что-то полезное. Так как веб-сайт находился в той же сети, что и все подразделение, последнее не могло выходить в Интернет, поскольку соединение было перегружено людьми, пытающимися найти обновления.

Для подведения итогов приведем общую схему расширения типичного веб-сайта, который предоставляет статическое и динамическое содержимое, а также содержит базу данных. Первоначально эти три компонента располагаются на одной машине. С ростом нагрузки мы обычно переносим каждую из этих функций на отдельную машину. По мере перегрузки каждого из этих элементов его можно расширять отдельно. Статическое содержимое легко дублировать. Часто многие серверы со статическим содержимым получают свое содержимое из крупного, расширяемого сетевого устройства хранения – NFS-сервера или SAN. Серверы с динамическим содержимым можно специализировать и/или дублировать. Например, динамические страницы, связанные с обработкой кредитных

карт, переносятся на одну выделенную машину, а связанные с конкретным приложением, например отображением страниц каталога, – на другую. Затем каждую из этих машин можно модернизировать или дублировать, чтобы получить возможность справляться с более высоким уровнем нагрузки. Базу данных можно расширять таким же образом – отдельные базы данных для определенных видов связанных данных, каждая из которых дублируется при необходимости справляться с нагрузкой.

29.1.7. Безопасность веб-службы

Реализация мер безопасности – жизненно важный элемент обеспечения работы веб-служб. Безопасность является проблемой, потому что к вашему серверу осуществляют доступ люди, которых вы не знаете. Некоторые люди считают, что для них безопасность не важна, так как у них нет конфиденциальных документов или доступа к финансовой информации и другим подобным важным данным. Однако само использование веб-сервера и пропускной способности, к которой у него есть доступ, является для некоторых людей ценной возможностью.

Злоумышленники часто взламывают узлы для использования с целью развлечения или получения доходов. Они могут даже не изменять внешний вид или содержимое веб-сайта, так как это быстро приведет к обнаружению. Вместо этого злоумышленники просто используют ресурсы. Обычно цели применения взломанных сайтов и их пропускной способности включают распространение пиратских программ (вареза), рассылку рекламных объявлений (спама) по электронной почте, запуск автоматизированных систем для атаки на другие системы и даже состязание с другими злоумышленниками для выяснения того, кто может собрать самую большую группу машин для запуска всего вышеперечисленного (группа-бот). Группы-боты часто используются для выполнения атак за деньги и становятся все более распространенными.

Даже для внутренних веб-служб должна обеспечиваться безопасность. Даже если вы можете доверять сотрудникам своей организации, все-таки есть несколько причин для обеспечения хорошей безопасности внутренних веб-служб.

- Многие вирусы передаются с машины на машину через электронную почту, а затем заражают внутренние серверы.
- Внутренние сайты могут содержать конфиденциальную информацию, для просмотра которой требуется аутентификация, например кадровые или финансовые данные.
- В большинстве организаций есть посетители – временные сотрудники, подрядчики, поставщики, журналисты, – у которых может быть доступ к вашему веб-сайту через сетевые порты конференц-зала или с ноутбука на территории компании.
- Если безопасность вашей сети нарушена, злонамеренно или случайно, например человек без злого умысла настроил беспроводную точку доступа так, что она стала доступна извне здания, вам требуется минимизировать потенциальный ущерб, который может быть нанесен.
- Некоторые патчи или исправления конфигурации для безопасности веб-служб также защищают от возможных атак отказа в обслуживании и делают ваш сервер более надежным.

В добавление к проблемам, которые могут быть вызваны попытками вторжения на ваш веб-сервер, существуют способы вторжения через веб-службы, позволяющие добраться до ваших пользователей через броузеры их рабочих станций. Мы поговорим об этом отдельно после рассмотрения безопасности веб-сервера.

Новые уязвимости безопасности часто обнаруживаются и объявляются, поэтому наиболее важный элемент безопасности – быть в курсе новых угроз. Мы рассмотрели источники такой информации в главе 11.

29.1.7.1. Безопасные соединения и сертификаты

Обычно доступ к веб-сайтам осуществляется при помощи незашифрованной связи. Неприкосновенность и аутентичность передачи может быть защищена шифрованием веб-трафика при помощи HTTP через протокол SSL (Secure Sockets Layer)[1]. Мы делаем это, чтобы исключить случайный перехват информации веб-сессий наших пользователей, даже если они подключаются через беспроводную сеть в общественном месте, например в кафе. URL, в которых вместо http:// пишется https://, используют шифрование SSL.

Реализация HTTPS на веб-сервере относительно проста и зависит от программного обеспечения веб-сервера. Правильно управлять криптографическими сертификатами не так легко.

SSL основан на криптографических сертификатах, которые представляют собой строки битов, используемые в процессе шифрования. В сертификате есть две части: частная половина и общая половина. Общую половину можно открыть любому. На самом деле она дается любому, кто подключается к серверу. Однако частная половина должна храниться в тайне. Если она попадет к посторонним, они могут воспользоваться ею, чтобы выдать себя за тех, кем не являются. Таким образом, задача системного администратора заключается в поддержании хранилища сертификатов, или **системы депонирования ключей**, для целей аварийного восстановления. Относитесь к этим данным как к другой важной секретной информации, например паролям `root` или Администратора. Один из методов – хранить их на ключевом USB-накопителе в запертом ящике или сейфе с четко определенными процедурами записи новых ключей, восстановления ключей и т. д.

Одно из опасных мест для хранения частной половины – это веб-сервер, который будет их использовать. Веб-серверы обычно имеют больший риск попадания под угрозу, чем другие. Хранить важную информацию на машине, которая имеет самую высокую вероятность взлома, – это плохая идея. Однако веб-серверу нужно прочитать частный ключ, чтобы им воспользоваться. Как можно разрешить этот конфликт? Обычно частный ключ хранится на машине, которой он требуется, в зашифрованной форме. Для чтения ключа требуется пароль. Это означает, что при каждом перезапуске веб-сервера, который поддерживает SSL, должен присутствовать человек, вводящий пароль.

В организациях с высоким уровнем безопасности может быть разумным, чтобы человек, который может ввести пароль, был доступен всегда. Однако в большинстве организаций используются различные альтернативы. Самая популяр-

[1] SSL 4.0 также известен как Transport Layer Security (TLS) 1.0, его более старые версии – SSL 2.0 и 3.0.

ная из них – хранить пароль в зашифрованном виде, то есть закодированным таким образом, чтобы кто-то, читающий его из-за вашей спины, не смог его запомнить, например в виде base64, в скрытой и уникальной директории, чтобы злоумышленник не мог найти его, догадавшись по названию директории. Чтобы получить пароль, запускается программа-помощник, которая читает файл и передает пароль веб-серверу. Сама программа защищается таким образом, что ее невозможно прочитать, чтобы определить, на какую директорию она ссылается, и она может быть выполнена только определенным ID, имеющим возможность запускать ее. Это более рискованно, чем наличие кого-то, кто каждый раз может ввести пароль, но это лучше, чем ничего.

Криптографический сертификат создается системным администратором веб-службы при помощи программы, которая поставляется с пакетом шифрования; одной из популярных систем является OpenSSL. Теперь сертификат является «самостоятельно подписываемым» – это означает, что ему можно доверять ровно настолько, насколько вы можете безопасно его хранить. Когда кто-то подключается к веб-серверу при помощи HTTPS, соединение будет зашифровано, но клиент, который подключается, никак не сможет узнать, что он подключен к правильной машине. Кто угодно может создать сертификат для любого домена. Если клиент может быть подключен к злоумышленнику вместо реального сервера, он не увидит различия. Вот почему большинство веб-броузеров при подключении к такому веб-сайту отображают предупреждение, указывающее, что используется самостоятельно подписываемый сертификат.

Что может остановить кого-то, выдающего себя за крупный сайт электронной коммерции, от сбора информации учетных записей людей при помощи создания поддельного сайта? Решением является криптографический сертификат с внешней подписью от зарегистрированного сертифицирующего органа (Certification Authority – CA). Общая половина самостоятельно подписываемого сертификата зашифровывается и отправляется доверенному CA, который подписывает ее и возвращает подписанный сертификат. Теперь сертификат содержит информацию, которой клиенты могут пользоваться, чтобы проверить, что сертификат был подтвержден более высоким уполномоченным органом. При соединении с веб-сайтом клиент читает подписанный сертификат и знает, что сертификату сайта можно доверять, потому что CA говорит ему об этом. Несмотря на то что криптографические методы находятся за пределами того, что здесь можно рассмотреть, информация, необходимая для проверки таких утверждений, хранится в сертификатах, встроенных в броузер, поэтому ему не нужно связываться с CA для каждого веб-сайта, использующего шифрование.

Иерархия доверия строится от CA к вашему подписанному сертификату и затем к броузеру, каждый уровень подтверждает уровень ниже. Иерархия является деревом и может быть расширена. Можно создать свой собственный CA, доверенный для центрального CA. Тогда у вас будет возможность подписывать сертификаты других людей. Так часто делают в крупных компаниях, которые предпочитают управлять своими собственными сертификатами и CA. Однако эти сертификаты заслуживают доверия так же, как самая слабая связь: между вами и более высоким CA.

Криптография – это функция, требующая интенсивных вычислений. Веб-сервер, который может обработать 500 незашифрованных запросов в секунду, за такое же время способен обработать только 100 запросов, зашифрованных при помощи SSL. Вот почему веб-сайты разрешают HTTPS-доступ на все страницы только в очень редких случаях. Для помощи в расширении таких веб-серверов есть аппаратные SSL-ускорители. Более быстрые процессоры позволяют быстрее

выполнять операции SSL. Какая скорость является достаточной? Пока пропускная способность канала сервера перегружается быстрее, чем его процессор, шифрование не является ограничивающим фактором.

29.1.7.2. Защита приложения веб-сервера

Некоторые атаки бывают направлены против самого веб-сервера, чтобы получить учетную запись доступа к машине или административный доступ к службе. С любыми уязвимостями, которые есть в операционной системе, можно справиться стандартными методами обеспечения безопасности. Уязвимости, характерные именно для Сети, могут присутствовать на различных уровнях реализации веб-сервера: на HTTP-сервере, в модулях или дополнениях, расширяющих сервер, а также в оболочках веб-программирования, выполняемых на сервере как программы. Мы считаем эту последнюю категорию отдельной от собственных приложений сервера, поскольку оболочка веб-программирования работает как уровень системного программного обеспечения для сервера.

Наилучший способ быть в курсе последних данных по безопасности веб-серверов на этих уровнях зависит от разработчика вашего оборудования. У различных HTTP-серверов, модулей и систем веб-программирования часто есть активные списки рассылки или группы обсуждения и почти всегда имеется список уязвимостей безопасности, а также доступных дополнений.

Реализация мониторинга службы может упростить обнаружение попыток использования уязвимостей, так как необычные записи в логах, скорее всего, будут обнаружены средствами автоматизированного просмотра логов (см. раздел 5.1.13 и главу 22).

29.1.7.3. Защита содержимого

Некоторые попытки вторжения в веб-службу направлены на получение содержимого службы, а не доступа к серверу. Уязвимостей в безопасности веб-контента слишком много, чтобы перечислять их здесь, и все время появляются новые. Здесь мы рассмотрим несколько распространенных способов вторжений.

Мы настоятельно рекомендуем, чтобы системный администратор, ответственный за безопасность веб-контента, изучал особенности имеющихся уязвимостей на ресурсах по безопасности Интернета, например, указанных в главе 11. Правильная оценка защищенности сервера от всевозможных угроз является серьезным мероприятием. К счастью, для этого существуют бесплатные и коммерческие продукты.

- **Обход директорий** – этот способ обычно используется для получения данных, которые иначе были бы недоступны. Данные могут представлять интерес сами по себе или служить для выполнения какого-либо способа прямого вторжения на машину. Этот способ обычно принимает форму использования иерархии директорий для прямого запроса файлов, например `../../../некоторый_файл`. При использовании на веб-сервере, который автоматически создает индекс директорий, обход директорий можно применять очень эффективно. Большинство современных веб-серверов защищаются от этого способа путем реализации специальных мер защиты корневого каталога документов и отказа предоставлять какие-либо директории, не указанные в явном виде с полными путями в файле конфигурации. Более старые реализации веб-серверов, а также новые, облегченные или экспериментальные реализации, например в прошивках оборудования, могут быть

подвержены этой проблеме. Распространенным вариантом такой атаки является CGI-запрос, который указывает нужную информацию, представляющую собой имя файла на сервере. Запрос `q-maindoc` возвращает содержимое `/repository/maindoc.data`. Если в системе нет необходимой проверки, то пользователь, запрашивающий `/paidcontent/prize`, сможет получить бесплатный, но неправомерный доступ к файлу.

- **Изменение поля формы** – это способ, который использует собственные веб-формы сайта, содержащие названия полей или переменных, соответствующих данным, вводимым пользователем. Эти названия видны в исходном коде HTML или в веб-форме. Злоумышленник копирует легальную веб-форму и изменяет ее поля для получения доступа к данным или службам. Если программа вызывается при помощи некоторой формы строгого подтверждения введенных данных, планы злоумышленника можно легко сорвать. К сожалению, злоумышленники могут быть очень умными и изобретательными и найти способы обойти ограничения.

  Например, предположим, что форма корзины покупок имеет скрытую переменную, в которой хранится цена покупаемого товара. Когда пользователь отправляет форму, для подсчета суммы покупки и выполнения транзакции с кредитной картой используются количества, указанные пользователем и скрытые цены в форме. Злоумышленник, изменивший форму, может произвольно устанавливать любые цены. Известны случаи, когда злоумышленники изменяли цены на отрицательные значения и получали сумму, равную компенсации за товары, которые не были куплены.

  Этот пример показывает хорошую идею, которая касается данных форм. Предположим, что злоумышленник изменил цену товара за 50 долларов на 25 центов. Программа подтверждения, вообще говоря, может не знать об этом. Лучше, чтобы в форме хранился идентификатор продукта, а система обращалась к базе данных цен для определения фактической стоимости.

- **Внедрение SQL** – это вариант изменения поля формы. В простейшем варианте *внедрение SQL* состоит из создания злоумышленником элемента SQL, который всегда будет определяться базой данных как «настоящий» при введении в легальное поле ввода. На сайтах на основе баз данных или с приложениями, управляемыми серверами баз данных, этот способ позволяет злоумышленникам нанести разнообразнейшие повреждения. В зависимости от операционной системы злоумышленники могут получить доступ к привилегированным данным без пароля и создать привилегированную базу данных либо системные учетные записи или даже выполнять произвольные системные команды. Злоумышленник может вводить целые SQL-запросы и выполнять обновления и удаления! Некоторые системы баз данных имеют возможности отладки, которые позволяют запускать произвольные команды операционной системы.

29.1.7.4. Безопасность приложений

Вероятность успеха усилий злоумышленников можно снизить. Ниже приведены некоторые фундаментальные принципы, которые нужно соблюдать при написании кода для веб-сайтов или при расширении возможностей сервера. Мы настоятельно рекомендуем работу Джеймса Уиттейкера[1] (James Whittaker) для более близкого ознакомления с этой темой.

[1] См. *www.howtobreaksoftware.com*.

- **Ограничивайте потенциальный ущерб.** Одна из лучших мер защиты, доступных для реализации, – это ограничить объемы ущерба, которые может нанести злоумышленик. Предположим, что содержимое и программы хранятся во внутренней эталонной среде и просто копируются на веб-сервер после внесения и проверки изменений. Злоумышленник, который изменит внешний вид сайта, сделает очень мало, потому что машину можно легко восстановить при помощи необходимой информации из незатронутой внутренней системы.

  Если веб-сервер изолирован от своей собственной сети и не имеет возможности инициировать соединения с другими машинами и ресурсами внутренней сети, то злоумышленник не сможет воспользоваться системой в качестве средства для получения контроля над другими локальными машинами. Необходимые соединения, например, для резервного копирования, сбора информации логов и установки обновлений содержимого, можно настроить таким образом, чтобы они всегда инициировались из сети организации. Соединения из Интернета с внутренними машинами будут отклоняться.

- **Подтверждайте входные данные.** Очень важно подтверждать входные данные, предоставляемые интерактивным веб-приложениям, чтобы максимизировать безопасность. Должна проверяться длина входных данных, чтобы не допустить переполнения буфера, при котором исполняемые команды могут быть помещены в память. Пользовательские входные данные, даже правильной длины, могут скрывать попытки запуска команд при помощи символов кавычек или перехода.

  Заключение пользовательских входных данных в так называемые безопасные кавычки или запрет определенных символов в некоторых случаях может работать и предотвращать вторжения, но также может вызвать проблемы с правомерными данными. Фильтрация или отклонение некоторых символов, например апострофа или дефиса, может не позволить Патрику О'Брайену (Patrick O'Brien) или Эдварду Балверу-Литтону (Edward Bulwer-Lytton) зарегистрироваться в качестве пользователей.

  Лучше подтверждать правомерность входных данных при помощи включения, а не исключения. То есть, вместо того чтобы пытаться выбрать символы, которые нужно запретить, удалите все символы, которые не входят в определенный набор.

  Что еще лучше, применяйте схемы программирования, которые не интерпретируют и не разбирают данные для вас повторно. Например, используйте двоичные API вместо ASCII, который будет разобран системами более низкого уровня.

- **Автоматизируйте доступ к данным.** Программы, которые осуществляют доступ к базе данных, должны быть максимально специализированы. Если веб-приложению нужно только читать данные из базы данных, пусть оно открывает базу данных в режиме только для чтения или запускается как пользователь с доступом только для чтения. Если ваша база данных поддерживает сохраненные процедуры – особенно предварительно скомпилированные запросы, – создайте их для выполнения необходимых вам действий и пользуйтесь ими вместо команд SQL.

  Многие базы данных и/или языки написания скриптов имеют *функцию подготовки* – ею можно воспользоваться для перевода потенциально исполнимых входных данных в форму, которая не будет интерпретироваться базой данных и таким образом не сможет перейти в попытку вторжения.

- **Пользуйтесь правами и привилегиями доступа.** Веб-серверы обычно хорошо взаимодействуют с методами аутентификации, существующими в операционной системе, и имеют возможность поддержки локальных прав и привилегий доступа на самом веб-сервере. Пользуйтесь этими функциями, чтобы избежать предоставления привилегий веб-программам без необходимости. Базовые принципы безопасности минимума привилегий доступа действуют для веб-служб и веб-приложений, чтобы любые несанкционированно полученные привилегии не могли быть использованы в качестве средства для атаки на следующее приложение или сервер. Межсайтовая обратная подделка (Cross-Site Reversed Forgery – XSRF) является хорошим примером злонамеренного использования прав доступа и аутентификации.
- **Ведите логи.** Ведение логов – это важная мера защиты и ваша последняя надежда. После попытки вторжения подробные логи позволят выполнить более полную диагностику и восстановление. Следовательно, умные злоумышленники будут пытаться удалять записи логов, связанные с вторжением, укорачивать файлы логов или полностью их удалять. Логи должны храниться на других машинах или в нестандартных местах, чтобы затруднить их подделку. Например, злоумышленники знают о директории /var/log в UNIX и будут удалять в ней файлы. Многие сайты можно было бы проще восстановить после вторжения, если бы логи не хранились в этой директории.

  Другой способ хранения логов в нестандартном месте – использовать сетевое ведение логов. Несколько веб-серверов сами поддерживают сетевое ведение логов, но большинство можно настроить для использования средств ведения логов операционной системы. Большинство средств ведения логов уровня ОС имеют возможность перенаправлять логи по сети на централизованный узел логов.

29.1.8. Управление содержимым

Ранее мы кратко упомянули тот факт, что системному администратору не стоит непосредственно заниматься обновлением содержимого (контента). Это не только добавляет работу и без того загруженным системным администраторам, но также создает узкое место между создателями содержимого и процессом публикации. Есть значительная разница между тем, чтобы сказать: «Системный администратор не должен этим заниматься», и созданием надежного процесса управления содержимым. Для понимания этого различия мы более подробно рассмотрим некоторые принципы управления содержимым и его делегирования другим людям.

Во многих организациях пытаются объединить роли системного администратора и веб-мастера или контент-менеджера. Обычно веб-серверы настраиваются с такой защитой или правами доступа, что для изменения или обновления различных объектов нужен привилегированный доступ. В таких случаях обновление содержимого становится «естественной» обязанностью системного администратора, даже если первые несколько обновлений выполнялись «временно», чтобы «продержаться первое время». Организация, которая полагается в обновлении веб-сайта на системных администраторов, а не на собственные силы отдела информационных систем, плохо использует свои ресурсы.

Эта проблема продолжает существовать и вырастает в бремя для системных администраторов. Пользователи, которые не учатся непосредственно обновлять

веб-сайт, также могут сопротивляться изучению веб-средств, которые позволят им создавать выходные данные в формате HTML. Тогда системного администратора просят форматировать, а не только обновлять данные. Требования ввести должность веб-мастера или контент-менеджера могут отклоняться, так как работа уже выполняется системным администратором или их отделом. Это обеспечивает существование проблемы и устраняет стимул для ее исправления.

29.1.8.1. Веб-группа

Как для внутренних, так и для внешних сайтов организации очень выгодна жесткая привязка управления веб-контентом к тем людям, которые создают это содержимое. В большинстве организаций это будет группа продаж, маркетинга или связей с общественностью. Наличие выделенного *веб-мастера* не решит проблему реально, даже в очень маленьких организациях, потому что веб-мастер тогда становится дефицитным ресурсом и потенциально узким местом.

Наилучший подход – создать *веб-группу*, которая обслуживает как внутренние, так и внешние сайты. Такая группа может использовать стандарты и программы для создания унифицированного подхода к обновлению веб-контента. Сотрудники группы могут изучать более специализированные методы веб-программирования, которые используются для современных веб-сайтов. Если ваша организация недостаточно крупная для поддержки веб-группы, хорошая альтернатива – создать *веб-комиссию*, состоящую из веб-мастера и представителя каждой из основных заинтересованных групп, в том числе системных администраторов. Дополнение веб-мастера такой комиссией усиливает идею того, что группы отвечают за свой контент, даже если работа выполняется веб-мастером. Она также объединяет людей для совместного использования ресурсов и улучшения скорости обучения. Что самое лучшее, это происходит без затрат на данный процесс ресурсов системных администраторов.

Они правда прочитают это в ближайшие выходные?

Для многих компаний характерно такое отношение к обновлению содержимого своих веб-сайтов, которое можно, мягко говоря, назвать наивной безотлагательностью. Один из друзей Страты долгое время находился в неудобном положении единственного человека, который мог обновлять содержимое веб-сервера. По крайней мере раз в месяц, а иногда и чаще, кто-нибудь из отдела маркетинга ловил этого человека по пути с работы в конце рабочего дня со «срочным» обновлением, которое нужно было разместить на сервере максимально быстро. Так как системные администраторы не имели возможности даже заставить сотрудников отдела маркетинга пользоваться функцией Сохранить как HTML в текстовых процессорах, это означало трудоемкое форматирование, а также обязанность загрузки и тестирования. Что еще хуже, обычно это происходило по пятницам и подрывало многие планы на выходные.

Если вы еще не смогли доказать своей организации, что ей нужен веб-мастер, и если вы – системный администратор, которого сделали ответственным за обновление веб-контента, первый шаг к свободе – создание веб-комиссии. Несмотря на то что это может показаться просто еще одним или несколькими собрани-

ями в вашем графике, на самом деле вы увеличиваете заметность своей работы. Объем работы, которую вы выполняете для поддержки веб-сайта, станет очевидным для заинтересованных групп, входящих в веб-комиссию, и вы получите поддержку для создания выделенной должности веб-мастера. Учтите, что члены комиссии необязательно будут это делать из желания помочь вам. Когда вы регулярно взаимодействуете с ними в роли веб-мастера, вы создаете потребность большего взаимодействия. Наилучший для них способ удовлетворить эту потребность – нанять другого человека на должность веб-мастера. Понятное объяснение того, какая степень подготовки необходима хорошему веб-мастеру, поможет вам обеспечить, чтобы они не предложили сделать вас веб-мастером и не наняли другого системного администратора для выполнения вашей работы.

29.1.8.2. Контроль изменений

Создание веб-комиссии существенно упрощает распределение областей ответственности за содержимое веб-сайта, потому что основные «голоса» каждой группы уже работают с веб-мастером или системным администратором, который является временным веб-мастером. Веб-комиссия – это естественный владелец процесса контроля изменений.

Этот процесс должен иметь конкретную политику по отношению к обновлениям, а в идеальном случае политика должна различать три типа изменений, с которыми следует связать различные процессы:

1. *Обновление* – добавление нового материала или замена версии документа более новой.
2. *Изменение* – смена структуры сайта, например добавление новой директории или перенаправление ссылок.
3. *Исправление* – коррекция содержимого документа либо поведения сайта, которое не соответствует стандартам.

Например, процесс внесения исправления должен предполагать открытие заявки на устранение неисправности или сообщение об ошибке, а исправление должно пройти контроль качества. Процесс внесения изменения должен предполагать наличие подтверждающего письма о файле от члена веб-комиссии из группы, запрашивающей изменение, прежде чем оно будет передано в группу контроля качества, а контроль качества должен подтвердить обновление до его публикации на сайте. Подобная методика используется во многих инженерных процессах, где действия классифицируются как исправления ошибок, запросы на реализацию функции и типовые процедуры.

Правила + автоматизация = меньше политической борьбы

Когда Том работал в небольшой начинающей компании, вопрос публикации обновлений на внешнем веб-сайте стал серьезным политическим конфликтом. Маркетинг хотел контролировать все, обеспечение качества хотело тестировать обновления перед их выходом, инженеры мечтали об их безопасности, а руководство желало, чтобы все перестали спорить.

Содержимое веб-сайта было, главным образом, статичным и не обновлялось чаще раза в неделю. Вот что сделали Том и его коллега. Сначала они установили три веб-сервера:

1. *www-draft.example.com*: область работы веб-дизайнера, недоступная внешнему миру.
2. *www-qa.example.com*: веб-сайт, недоступный внешнему миру, который просматривался специалистом по контролю качества и всеми, кто подтверждал обновление сайта.
3. *www.example.com*: действующий веб-сервер, видимый из Интернета.

Веб-дизайнер напрямую редактировал www-draft. Когда работа была сделана, содержимое переносилось на www-qa, где люди проверяли его. После одобрения содержимое переносилось на действующий сайт.

(*Примечание:* Более ранняя версия их системы не включала неизменяемую копию для проверки специалистом по контролю качества. Вместо этого веб-дизайнер просто прекращал что-либо изменять, пока просматривалось предлагаемое обновление. И хотя эта система была проще в реализации, она не исключала проникновения в систему обновлений без тестирования, сделанных в последний момент. Оказалось, что это очень плохо.)

Первоначально системные администраторы были вовлечены в перенос содержимого с одного этапа на следующий. Это помещало их в центр политического конфликта. Кто-то мог попросить системных администраторов перенести текущее содержимое на действующий сайт, а затем в содержимом могли найти ошибку – и все обвиняли системных администраторов. Их могли попросить перенести на сайт один файл для устранения проблемы, а сотрудники группы по обеспечению качества могли быть расстроены тем, что вопрос не согласован с ними. Руководство пыталось реализовать систему, где системные администраторы получали бы подтверждение для копирования на действующий сайт содержимого, проверенного группой обеспечения качества, но такое подтверждение хотели давать все, и это стало катастрофой: в следующий раз, когда нужно было обновлять содержимое сайта, не все, кто должен был дать подтверждение, были на месте, и отдел маркетинга взбесился, обвиняя системных администраторов за то, что они недостаточно быстро вносили изменения. Группе системных администраторов нужно было выйти из этого процесса.

Решением было создание списка людей, которым разрешалось перемещать данные из различных систем, и автоматизация функций для предоставления самообслуживания, чтобы системные администраторы не участвовали в процессе. Для переноса данных на каждом этапе были созданы небольшие программы, и при помощи UNIX-команды `sudo` были установлены права доступа, чтобы только определенные люди могли выполнять те или иные команды.

Вскоре системные администраторы исключили себя из процесса вообще. Да, на веб-сайте воцарился беспорядок. Да, первый раз, когда отдел маркетинга воспользовался своим правом в экстренных случаях переносить

содержимое из черновика напрямую на действующий веб-сайт, стал последним разом, когда они воспользовались этой командой. Но со временем все научились быть осторожными.

Но самое важное – процесс был автоматизирован таким образом, что системные администраторы больше не участвовали ни в самом процессе, ни в политических конфликтах.

29.1.9. Создание типового управляемого веб-сервера

Системных администраторов часто просят создать веб-сервер с нуля, не предоставляя никакой конкретной информации о том, как этот сервер будет использоваться. Мы собрали некоторые типичные вопросы, которые помогут вам точнее определить просьбу. Подобный список должен быть доступен для всех запросов на установку веб-серверов. Полезно иметь несколько вопросов, на которые нетехнический пользователь может ответить сразу, не передавая весь список кому-то еще.

- Станет ли веб-сервер использоваться только внутренними пользователями или он будет доступен через Интернет?
- Есть ли у веб-сервера особая задача по размещению конкретной службы или программы? Если да, какой службы или программы?
- Кто будет пользоваться сервером и какие типичные варианты использования предполагаются?
- Каковы требования по безотказной работе? Можно ли отключать веб-сервер для техобслуживания на час в неделю? На шесть часов?
- Будем ли мы создавать для этого веб-сервера учетные записи или группы?
- Сколько места для хранения должно быть на этом сервере?
- Какой предполагаемый трафик будет поступать на этот сервер и как он будет расти со временем?

29.1.9.1. Любой сайт

Есть ряд базовых принципов, которые нужно помнить при планировании любого веб-сайта, вне зависимости от того, будет ли его применение внутренним или внешним. Один из наиболее важных принципов – планирование вашего пространства имен URL. Общие указания, данные нами в главе 8, будут очень полезны. Изменять URL-ссылки, встроенные в HTML-документы, может быть трудно, так что это стоит сделать с самого начала. Люди обычно видят определенные URL и делают предположения, какие другие URL будут работать, поэтому грамотно подобранная последовательность может улучшить ощущения пользователей.

Например, предположим, что кто-то может найти веб-директорию коллеги в сети по адресу *http://internal/user/strata*. Что случится с этим URL, когда компания будет приобретена другой компанией? Будет ли он перенесен на новый общий внутренний сайт? Если да, останется ли он таким же или изменится на *http://internal/oldcompany/user/strata*? Может быть, в новой компании вместо /user используют /home или даже /users.

Внимательно планируйте свое пространство имен URL, чтобы избежать конфликтов назначения имен и непоследовательных либо неупорядоченных URL. Некоторые типичные варианты – `/cgi-bin`, `/images`, `/user/$USER` и т. д. Альтернативные варианты могут включать `/student/$USER`, `/faculty/$USER` и т. д. Будьте осторожны с использованием идентификационных номеров вместо имен пользователей. Это может показаться более простым и управляемым, но если пользователь даст свой URL другим людям, идентификационный номер, входящий в URL, потенциально может быть конфиденциальной информацией.

Одно важное свойство URL заключается в том, что, когда вы кому-то его даете, предполагается, что URL будет доступен всегда. Так как это редко бывает на самом деле, можно реализовать обход для URL, которые меняются. Большинство веб-серверов поддерживают функцию, называемую *перенаправлением*, – она позволяет сайту хранить список URL, которые должны перенаправляться на альтернативный URL. И хотя команды перенаправления почти всегда поддерживают символы-заместители, например `my-site/project*` становится `my-new-site/project*`, часто нужно выполнить много утомительной ручной работы.

Хороший способ предупредить проблемы до их возникновения – использовать функцию `include` скрипта препроцессора или собственного файла конфигурации веб-сервера для создания отдельных файлов конфигурации для различных разделов вашего веб-сайта. Эти файлы конфигурации могут редактироваться веб-группой, ответственной за изменение содержимого этого раздела, в том числе перенаправлений при изменении ими своего раздела веб-сайта. Это полезно для исключения участия системных администраторов в обновлении содержимого. Однако основной задачей является минимизация риска того, что веб-группа может случайно изменить или неправильно настроить параметры всего сайта в главном файле конфигурации веб-сервера.

На большинстве сайтов пользователи хотят размещать контент, а не приложения. Пользователи могут потребовать, чтобы системные администраторы устанавливали приложения, но не будут часто требовать доступ к серверу для программирования для запуска собственных скриптов и программ. Предоставление людям возможности запускать веб-программы, например CGI-скрипты, имеет потенциал негативного влияния на веб-сервер и других пользователей. Избегайте разрешать людям запускать свои собственные CGI по умолчанию. Если вы должны разрешить такое использование, воспользуйтесь средствами операционной системы, которые ограничивают потребление программами ресурсов, чтобы не позволить нестандартной программе привести к ухудшению обслуживания других пользователей.

Если вы не тот редкий системный администратор, у которого не очень много работы, то вы, скорее всего, не захотите отвечать за поддержание актуальности содержимого веб-сайта. Мы настоятельно рекомендуем вам создать процесс, в котором либо запрашивающие люди, либо люди, назначенные ими, смогут обновлять содержимое нового веб-сервера. Иногда это просто означает открытие общего доступа к то́му, содержащему веб-контент; для внешних сайтов это может означать создание методов безопасного доступа пользователей для обновления сайта. Еще более удачным решением для сайтов, уже использующих базы данных для хранения некоторых видов данных, которые им нужно публиковать на веб-страницах, будет веб-сайт на основе базы данных. Тогда существующие процессы обновления базы данных будут управлять веб-контентом. Если база данных еще не используется, это может стать подходящим моментом для ее создания в качестве элемента установки веб-сервера и сайта.

29.1.9.2. Внутренний сайт

Для внутреннего сайта обычно достаточно простой модели публикации. Создайте корневой каталог документов в разделе, к которому можно открыть общий доступ, и дайте внутренним группам доступ с правами на чтение и запись своих поддиректорий в этом разделе. Таким образом они смогут управлять своим собственным внутренним контентом.

Если внутренним пользователям нужно изменять сам веб-сервер, добавляя модули или директивы конфигурации, которые могут затронуть другие группы пользователей, мы рекомендуем пользоваться отдельным, возможно виртуальным, сервером. Этот подход не нужно применять для каждой поддерживаемой группы, но некоторым группам он понадобится с большей вероятностью. Например, группе разработчиков, которая хочет установить средства управления исходным кодом третьих сторон, часто требуется изменять веб-сайт при помощи материала из скриптов установки разработчика этих средств. Факультет университета, предоставляющий дистанционное обучение, может создать свою программу управления курсом, которая потребует тесной интеграции с веб-сайтом или связи аутентификации с чем-то помимо основной директории комплекса.

29.1.9.3. Внешний сайт

Сайты, видимые извне, должны настраиваться в соответствии с хорошими методами обеспечения безопасности, такими как блокировка неиспользуемых портов или расположение за брандмауэром. Если в вашей организации нет внешнего веб-сайта и сервер, который вы создаете, будет первым, важно спросить, согласует ли заказчик создание этого сайта с соответствующими сторонами в организации. Сайт будет необходимо структурировать для поддержки общей схемы, и время всех участников процесса будет тратиться более эффективно, если выполнить предварительное планирование.

Создание веб-сайта включает четыре отдельных, независимых друг от друга компонента: регистрация домена, интернет-хостинг DNS, веб-хостинг и веб-контент.

Первый элемент – это регистрация домена в глобальном реестре. Существуют провайдеры, или регистраторы, которые делают это для вас. Точное описание этого процесса не входит в задачи данной книги.

Второй элемент – это хостинг DNS. Служба регистрации выделяет имя, но не предоставляет службу DNS, которая принимает DNS-запросы и отправляет DNS-ответы. Некоторые службы регистрации объединяют хостинг DNS с регистрацией DNS.

Третий элемент, веб-хостинг, означает наличие веб-сервера по адресу, выданному DNS для вашего сайта. Это сервер, который вы только что установили.

Четвертый и последний элемент – это веб-контент. Веб-страницы и скрипты – это просто файлы, которые нужно создать и загрузить на веб-сервер.

29.1.9.4. Процесс создания материалов веб-сайта

Если планируемый веб-сайт требуется для хорошо заметного и, главным образом, статического контента, например веб-представительства новой компании,

мы рекомендуем установить какой-нибудь процесс введения в эксплуатацию новых версий веб-сайта. Стандартный процесс, который очень хорошо работает для многих сайтов, – это установить три идентичных сервера, один для каждого этапа процесса ввода в эксплуатацию.

Первый сервер считается «черновиком» и используется для редактирования или загрузки образцов из программ редактирования веб-страниц на рабочих станциях. Второй сервер – это сервер контроля качества. Когда объект готов к публикации, его *переносят* на сервер контроля качества для проверки, корректировки и, в случае наличия скриптов и веб-приложений, стандартного тестирования программ. Последний сервер – это «действующий», или рабочий, сервер. Если объект проходит контроль качества, он переносится на рабочий сервер.

Для сайтов, сильно загруженных скриптами и/или имеющих особенно строгие требования к контенту, в процесс часто вводится еще один сервер. Этот дополнительный сервер, часто известный как *эталонный* сервер, функционально идентичен рабочему серверу, но либо заблокирован от внешнего использования, либо скрыт за специальным брандмауэром или VPN. Обычно назначение эталонного сайта – это проверка или интеграция и тестирование отдельных приложений либо процессов, которые должны без сбоев взаимодействовать с рабочим веб-сервером. Сайт контроля качества может вести себя странно из-за самого тестирования для контроля качества, поэтому эталонный сайт позволяет проводить тестирование интеграции на сайте, который должен вести себя идентично рабочему, но не будет затрагивать внешних пользователей, если с тестом что-то пойдет неправильно. Кроме того, он предоставляет дополнительный этап проверки, который позволяет публиковать контент внутри организации, а затем передавать его другой группе, возможно, отвечающей за размещение материала на внешнем сайте. Обычно доступ на эталонный сайт разрешен только внутренним пользователям или определенным сторонним партнерам.

29.2. Тонкости

До сих пор мы рассматривали самостоятельные решения. Тонкости представляют собой способы максимально эффективного использования других служб, чтобы системные администраторы не заботились о таком количестве мелких деталей.

29.2.1. Веб–хостинг третьих сторон

Компании по веб-хостингу (веб-хостеры) предоставляют веб-серверы для использования другими. Пользователи загружают контент и публикуют его. Существует конкуренция, кто предоставит больше функций, большее время безотказной работы, меньшую стоимость. **Управляемый хостинг** касается хостеров, которые предоставляют дополнительные услуги, например мониторинг.

Крупные компании часто содержат собственную службу управляемого хостинга, чтобы не приходилось начинать отдельные проекты с нуля каждый раз, когда нужно создать новую веб-службу.

Большинство материала данной главы будет полезно системным администраторам, которые обеспечивают работу веб-сайтов или служб хостинга; данный раздел касается пользования такими службами.

29.2.1.1. Преимущества передачи веб-служб сторонним исполнителям

Интеграция является более мощной, чем изобретение. При пользовании услугами хостинга не нужно устанавливать локальные программы, все это находится в ведении провайдера. Вместо того чтобы быть экспертом в области сетей, установки серверов, проектирования информационных центров, питания и охлаждения, инженерных процессов и многих других аспектов, можно просто сосредоточиться на предоставляемых веб-службах.

Хостеры часто создают сетевую «панель управления», которую можно загрузить для управления и настройки размещенной службы. Все данные хранятся на серверах хостера, что может показаться *недостатком*. На самом деле, если вы не работаете в крупной организации или не имеете в своем распоряжении необычных ресурсов, большая часть размещаемых служб обладает лучшей комбинацией надежности и безопасности, чем может обеспечить отдельная организация. Они выигрывают за счет экономии масштаба и могут выделить больше резервирования, пропускной способности и ресурсов системных администраторов, чем отдельная организация.

Внешний хостинг определенных веб-приложений или служб может помочь организации более эффективно использовать труд своих системных администраторов и минимизировать расходы на оборудование и ресурсы сети. Это особенно справедливо, когда желаемые услуги потребовали бы сильной индивидуализации или значительного обучения части имеющегося персонала и ресурсов, представляющих собой «отраслевой стандарт» дополнительных служб, используемых с веб-службой. При разумном использовании услуги управляемого веб-хостинга могут также быть элементом плана аварийного восстановления и предоставлять дополнительную гибкость при расширении.

Небольшие сайты проще всего создать при помощи службы веб-хостинга. Экономическое преимущество вызвано тем, что хостер обычно объединяет десятки небольших сайтов на каждом сервере. Оплата может изменяться от 5 долларов в месяц для сайтов, которые получают очень мало трафика, до нескольких тысяч долларов в месяц для сайтов, использующих большую пропускную способность.

29.2.1.2. Недостатки передачи веб-служб сторонним исполнителям

Недостатки сводятся к беспокойству о данных, трудностям перехода и опасениям, не приведет ли передача хостинга к передаче системного администрирования. Что касается первого, во многих случаях данные можно экспортировать с размещенного сайта таким образом, что их можно сохранить локально. Многие хостеры также предлагают резервное копирование на своих ресурсах, а некоторые предоставляют услуги резервного копирования, которые включают периодическое дублирование данных, поэтому копия может быть отправлена непосредственно вам.

Что касается двух других проблем, многим системным администраторам очень тяжело избавиться от привычки делать все самим, даже если они перегружены работой. Сохранение ответственности за выполнение всех остальных служебных обязанностей системного администратора – одна из лучших форм обеспечения гарантий занятости, поэтому решения, которые снижают вашу загруженность, обычно полезны для вашей работы.

29.2.1.3. Унифицированный вход в систему: управление профилями

В большинстве случаев очень желательно иметь унифицированный, или последовательно организованный, вход во все приложения и системы организации. Лучше, чтобы все приложения имели доступ к единой системе паролей, чем требовать у людей наличия пароля для каждого приложения. Когда у людей слишком много паролей, они начинают записывать их на бумажках под клавиатурой или приклеивать к мониторам, что делает пароли бессмысленными. Когда вы приобретаете или создаете веб-приложение, убедитесь, что его можно настроить для запроса вашей существующей системы аутентификации.

При работе с веб-серверами и приложениями комбинация имени пользователя и пароля и дополнительная информация для доступа или индивидуальной настройки обычно называется *профилем*. Управление профилями на веб-серверах обычно представляет собой наиболее серьезную проблему. К счастью, мы уже знаем, как управлять такой информацией на нескольких серверах (см. главу 8). Хуже, что методы управления профилями для веб-приложений нестандартизированы вообще и многие современные веб-приложения используют внутреннее управление профилями.

Стандартное веб-приложение либо включает собственный веб-сервер, либо работает под уже существующим. Большинство веб-серверов не предоставляют средств централизованного управления профилями. Вместо этого в каждой директории есть правила профилей, установленные в управляющем файле веб-сервера. Теоретически каждое приложение может работать в директории и подчиняться правилам контроля доступа, установленным для этой директории. На практике это обычно игнорируется.

Есть несколько стандартных методов, при помощи которых веб-серверы и приложения управляют данными о профилях, например файлы .htaccess и .htpasswd в Apache, применение запросов LDAP или Active Directory, запросы системного уровня к подключаемому модулю аутентификации (Pluggable Authentication Module – PAM) или SQL-запросы во внешнюю базу данных. Любое конкретное приложение может поддерживать либо какую-то их часть, либо иметь полностью собственный внутренний метод. Все чаще приложения просто запускаются в виде скрипта на веб-сервере, а управление профилями находится под непосредственным контролем приложения, часто через серверную базу данных этого приложения. В некоторых случаях это делает централизованное управление профилями особенно трудным. Установите приоритет выбора продуктов, которые хорошо интегрируются с вашей системой аутентификации.

При использовании методов аутентификации, встроенных в программное обеспечение вашего веб-сервера, все вопросы аутентификации разбираются до того, как система CGI получает контроль. Например, в Apache, вне зависимости от того, выполняется ли аутентификация при помощи локальных текстовых файлов для хранения информации об именах пользователей и паролях или используется что-то более сложное, например модуль аутентификации LDAP, запрос на ввод имени пользователя и пароля обрабатывается на уровне веб-сервера. CGI-скрипт запускается только после успешного входа в систему, и ему через переменную среды сообщается, что имя пользователя прошло аутентификацию. Для большей гибкости в большинстве CGI-приложений есть какая-либо собственная система аутентификации, которая имеет свою систему имен пользователей и паролей. Однако хорошо организованные системы можно настроить

таким образом, чтобы отключить эту функцию и просто пользоваться предварительно прошедшим аутентификацию именем пользователя, переданным веб-сервером Apache. Приложение может допустить, что вход в систему был завершен, и использовать имя пользователя в качестве ключа для получения профиля приложения для этого пользователя.

29.2.2. Гибридные приложения

Один из побочных эффектов стандартных форматов обмена данными между веб-приложениями – это явление, называемое *гибридными* приложениями. Они могут привести к значительным проблемам расширения.

Гибрид – это веб-сайт, который использует данные и API других веб-сайтов для создания нового приложения[1]. Гибридные приложения просто берут хорошо структурированные выходные данные одной веб-службы, разбирают данные в соответствии со схемой и вставляют их в свое новое приложение. Комбинации часто являются гениальными, разносторонними и очень полезными. Разработчики приложений создают очень сложные XML-схемы для данных своих приложений.

Прекрасным примером гибридного приложения, которое использует данные таким образом, является HousingMaps (*http://www.housingmaps.com*), которое показывает интерактивные карты, используя данные Google Maps с информацией о недвижимости с популярного сайта Craigslist.

Гибридное приложение содержит два элемента, поэтому расширять надо их оба. Первая часть – это компонент гибридного приложения, написанный автором для объединения использованных служб. Вторая часть – это сами использованные службы.

Обычно блок объединения является легким, и его расширение – вопрос применения ранее рассмотренных методов. Однако нужно иметь в виду, что, если гибрид является действительно оригинальным и инновационным, приложение может за короткое время стать очень популярным и вызвать неожиданную нагрузку на инфраструктуру вашего веб-сервера.

Самая большая проблема – это службы, на которые полагается гибрид. Обычно они выполняют тяжелую работу. Для системных администраторов, которые обеспечивают работу такой службы, внезапная популярность гибридного приложения может вызвать неожиданный поток запросов. Таким образом, хороший API предполагает ограничение и управление. Например, большинство API требуют, чтобы любой пользователь зарегистрировался для получения идентификационного ключа, передаваемого в каждом запросе. Ключи обычно легко получить, а их подтверждение является мгновенным и автоматизированным. Однако каждый ключ позволяет сделать определенное количество запросов в секунду и максимальное количество запросов в заданный 24-часовой период. Эти ограничения на уровень запросов должны быть указаны в SLA, которое нужно показывать в момент запроса пользователем ключа, и ограничения должны соблюдаться в программе, которая предоставляет услугу.

Когда пользователь превышает лимит, это является признаком злонамеренного использования или неожиданно успешного приложения. Более умные ком-

[1] По крайней мере один безработный дизайнер написал гибридное приложение для демонстрации своих навыков, пытаясь быть замеченным и нанятым компанией, которая создала использованный им API.

пании не предполагают злонамеренного использования по умолчанию, а некоторые из них даже поддерживают в сообществе хорошую репутацию, предоставляя временное послабление ограничений, чтобы помочь приложениям с высокой популярностью.

Так как все запросы привязаны к ключу пользователя, можно отслеживать тенденции и смотреть, какие приложения являются наиболее популярными. Эти данные могут быть полезны для маркетинговых целей или для выявления подходящих кандидатур на приобретение.

Когда лимит количества запросов превышен, первый шаг – определить, гарантируется ли ответ. Если изучение логов вашего сервера показывает последовательную, но неподдерживаемую запись сославшегося URL, возможно, вам стоит проверить приложение, чтобы посмотреть, в чем дело, и привлечь к этому внимание своей веб-группы и соответствующего руководства.

Гибридное приложение представляет собой важнейшую возможность для обучения вашей организации. Существование такого приложения, особенно используемого так, что оно влияет на ваши нормальные веб-службы, показывает, что у вас есть ценные данные. Какой-нибудь другой источник данных каким-то образом повышает его ценность, и ответственные за управление бизнес-процессами люди из вашей организации могут получить из этого много жизненно важной информации. Поэтому мы всегда рекомендуем, чтобы любая попытка немедленно ограничить доступ гибридного приложения шла по вашим стандартным каналам.

Если использование ваших данных представляет собой шанс, а не неудобство для вашей организации, вас могут попросить соответствующим образом расширить свои веб-службы или установить контакт с авторами гибридного приложения, чтобы вашу организацию в явном виде указывали рядом с данными.

Если принимается решение заблокировать использование ваших веб-служб гибридным приложением, то можно применить стандартные методы блокировки, поддерживаемые вашей сетевой инфраструктурой. Можно деактивировать ключ API. Перед тем как выполнить любую блокировку, имеет смысл проконсультироваться с юридическим и маркетинговым отделами, наличие уже имеющейся политики повысит возможность быстрого реагирования.

29.3. Заключение

Сеть все быстрее становится универсальной системой предоставления услуг в организации, а клиент веб-броузера может обеспечить общий интерфейс нескольким приложениям. Веб-службы должны проектироваться с учетом основных приложений, чтобы их можно было расширять, добавляя копии (горизонтально) или перераспределяя нагрузку между различными уровнями службы (вертикально). Создать простой веб-сайт в качестве базы для различных применений относительно легко, но обеспечить, чтобы системных администраторов в конечном итоге не заставили обслуживать содержимое, труднее. Формирование комиссии из заинтересованных в веб-службе лиц, в идеальном случае с выделенной группой веб-мастеров, может решить эту проблему и обеспечить возможность расширения по мере роста пользования веб-службами в организации. Другой вариант расширения – передача сторонним исполнителям служб, которые достаточно просты или требовательны к ресурсам, чтобы системные администраторы тратили время на что-то другое.

Задания

1. Какие факторы должны рассматриваться по-разному при предоставлении внешних и внутренних веб-служб в вашей организации?
2. Сколько криптографических сертификатов используется в вашей организации? Как они управляются? Какие усовершенствования вы внесли бы в управление ими?
3. Какие методы используются в вашей организации для создания нескольких веб-сайтов на одной машине?
4. Приведите пример характерного для веб-служб ведения логов и применения этой информации.
5. Выберите веб-службу своей организации и разработайте план ее расширения, предполагая, что она будет получать в пять раз больше запросов. В сто раз больше запросов.
6. Размещается ли внешний веб-сайт вашей организации у стороннего хостера? Почему да или почему нет? Оцените достоинства и недостатки перехода на внешний или внутренний хостинг.

Часть V

Методы управления

Глава 30

Организационная структура

То, какую структуру имеет группа системного администрирования, и то, как эта структура встроена в большую организацию, – это решающие факторы успеха или неудачи данной группы. В данной главе рассмотрены некоторые вопросы, которые каждая компания должна учитывать при создании группы системного администрирования, а также показаны результаты наших наблюдений во множестве разнообразных компаний. Глава завершается несколькими примерами организационных структур для различных компаний.

Общение – это область, которая находится под сильным влиянием организационной структуры как группы системного администрирования, так и компании в целом. Структура организации определяет главные связующие пути как между самими системными администраторами, так и между системными администраторами и их пользователями[1]. Оба канала общения – это ключ к успех группы системного администрирования. Системным администраторам в компании необходимо сотрудничать, чтобы построить надежную, последовательную компьютерную инфраструктуру для работы остальной части компании. Однако они также должны учитывать интересы пользователей и предоставлять им надежную поддержку и хорошее обслуживание.

Руководству и отдельным работникам нужно постараться избежать ситуации «они против нас», независимо от того, какую структуру имеет организация. Некоторые организационные структуры могут больше способствовать развитию этой ситуации, чем другие, но слабые каналы общения всегда являются корнем таких проблем.

30.1. Основы

Создание эффективной организации системного администрирования, в которой отсутствуют как внутренние конфликты, так и конфликты с пользовательской базой, – это сложная задача. Правильное определение размера и финансирование отдела системного администрирования, чтобы группа могла предоставлять хороший уровень обслуживания и при этом не была финансовым грузом компании, – это еще одна непростая задача. Мы также рассмотрим, какое влияние на эту проблему может оказать руководство.

Идеальная группа системных администраторов – это такая группа, которая может предоставить нужный уровень обслуживания за наименьшую возможную

[1] Связь между системными администраторами и их руководством также очень важна и может как сплотить, так и разрушить команду. Эта тема подробно обсуждается в главах 33 и 34.

цену. Отчасти предоставлять хорошее обслуживания для вашей компании – значит удерживать ваши расходы на максимально низком уровне, не затрагивая при этом качество обслуживания. Для этого вам понадобятся хорошие системные администраторы с необходимым набором навыков, которые занимаются нужными делами. Привлечение большего количества людей в группу системного администрирования не так эффективно, как привлечение в группу правильных людей. Хорошая группа системного администрирования имеет обширный набор технических навыков, и ее составляют люди, обладающие достаточными навыками общения и сработавшиеся со всеми остальными.

Маленьким группам системного администрирования необходимы всесторонне образованные системные администраторы с обширным набором навыков. Мы укажем, какие функции должны предоставляться центральной группой, а какие лучше выполняются маленькими распределенными группами системных администраторов. Мы объясним отличия механизмов централизованных моделей от децентрализованных применительно к системному администрированию, а также опишем преимущества и недостатки каждого подхода.

30.1.1. Определение размеров

Правильно определить размер вашей группы системного администрирования довольно сложно; если она слишком маленькая, это будет неэффективно и остальная часть компании станет страдать от ненадежной инфраструктуры и плохой службы поддержки пользователей. Если группа слишком большая, компания будет нести ненужные расходы и общение между системными администраторами станет более сложным. На практике в группах системного администрирования чаще бывает недобор персонала, нежели перебор. Слишком большое количество служащих, как правило, связано с отсутствием необходимого набора навыков в организации. Если у группы системного администрирования есть проблемы с поддержкой пользователей или с предоставлением нужного уровня обслуживания и надежности, простое увеличение количества персонала может и не быть выходом из сложившейся ситуации. Задумайтесь над приобретением отсутствующих навыков посредством тренингов или консультаций, прежде чем набирать новых людей.

Решая вопрос о размере группы системного администрирования, руководство организации должно учитывать несколько факторов: количество и разнообразие людей и машин в компании, сложность окружающей обстановки, тип работы, которой занимается компания, уровни обслуживания, необходимые различным группам, а также насколько критична стабильность работы различных компьютерных служб. Хорошей мыслью будет опросить системных администраторов, чтобы приблизительно определить, сколько времени каждый из них уделяет поддержке пользователей и машин в различных группах, а также обслуживанию машин центральной инфраструктуры.

В идеале ваша система уведомлений о неисправностях должна быстро предоставлять вам эту информацию за заданный период времени. Если она не способна это делать, вы можете попросить каждого системного администратора заполнить короткую форму, показанную на рис. 30.1, приблизительными числами. Эта информация даст основу для определения темпа роста группы системного администрирования, что позволит оставить уровни обслуживания почти неизменными. Также это даст вам правильное представление об областях, которые потребляют большое количество времени системных администраторов, и позволит найти пути уменьшения расходов на поддержку.

Укажите приблизительную долю времени, уделяемого каждой категории.
Пожалуйста, убедитесь, что в сумме они дают 100%.

	Доля		Количество
• Поддержка пользователей/настольных систем		• Количество пользователей	
• Поддержка серверов пользователей		• Количество пользовательских серверов	
• Поддержка инфраструктуры		• Количество машин инфраструктуры	

Рис. 30.1. *Краткая форма для сбора приблизительных чисел с целью прогнозирования темпа роста*

Пример: высокие расходы на поддержку

Когда в Synopsys проводили опрос, на что системные администраторы тратят свое время, руководители обнаружили, что системные администраторы тратили большое количество времени на поддержку старого, находящегося в плохом состоянии оборудования, которое также имело высокую стоимость ремонта в соответствии с контрактом. Замена оборудования на более новое и быстрое помогла бы сэкономить затрачиваемую рабочую силу и место в серверной. Руководители использовали эту информацию, чтобы убедить владеющую данным оборудованием группу списать его и заменить новыми машинами. Это дало системным администраторам возможность эффективнее использовать свое время и предоставлять лучшее обслуживание пользователям.

Не существует магического соотношения между пользователями и системными администраторами, которое работало бы для каждой компании, так как у разных клиентов различные потребности. Например, в студенческом городке может быть 500 или 1000 пользователей на каждого системного администратора, потому что бóльшая часть этих пользователей работает на своих машинах круглосуточно каждый день, довольно спокойно относится к небольшим перебоям и обычно не доводит свою технику до предела. Напротив, в высокотехнологичных сферах, таких как проектирование аппаратного обеспечения или расшифровка генов, больше требуется от IT-служб и они могут нуждаться в соотношении, близком к 60:1 или даже 20:1. При разработке программного обеспечения диапазон даже шире: мы видели системных администраторов, обслуживающих и 50 пользователей, и 5. В нетехнологичной корпоративной среде может потребоваться так же много системных администраторов, как и в технологичной, но с большим упором на систему поддержки пользователей, пользовательский интерфейс и обучение работе в среде. Независимо от их типа, во всех организациях должно быть как минимум два системных администратора или, по меньшей мере, подходящая замена для своего единственного системного администратора, если этот человек заболеет или уйдет в отпуск.

Сами машины также требуют времени на обслуживание, независимо от непосредственных запросов от пользователей. Серверы нуждаются в регулярном резервном копировании, обновлении программного обеспечения и операционной системы и установке патчей, мониторинге, а также обслуживании и обновлении аппаратного обеспечения. Что-то из вышеперечисленного может быть оптимизировано или автоматизировано с помощью методов, рассмотренных в других частях этой книги, но все-таки на обслуживание сервера тратится значительная часть времени. Даже если настольные системы – просто взаимозаменяемые копии, они все равно требуют времени на поддержку, хотя оно и минимально, так как вы можете просто поменять сломанную машину.

В любой достаточно большой организации некоторые люди проводят свое время, преимущественно обслуживая службы инфраструктуры, такие как электронная почта, печать, сеть, аутентификация и служба имен. Компаниям, предоставляющим своим пользователям услуги электронной коммерции или другие важные веб-ориентированные услуги, также будет требоваться группа для обслуживания соответствующих систем.

Все эти факторы должны учитываться при выборе размера организации. Определить соотношение между пользователями и системными администраторами – серьезный шаг, но это только полдела. Соберите реальные данные по вашей организации, чтобы определить, где системные администраторы проводят свое время. Используйте эти данные, чтобы определить, где можно улучшить автоматизацию и процессы, и чтобы выявить службы и системы, поддержку которых, возможно, вы больше не хотите осуществлять. Определите вместе с вашими пользователями SLA и применяйте эти SLA, чтобы грамотно рассчитать размер группы системного администрирования.

30.1.2. Модели финансирования

Деньги – главное в любом деле. То, как и кто финансирует системное администрирование, – решающий фактор для успеха или неудачи группы системного администрирования.

Основная причина, по которой подразделение системного администрирования, как правило, испытывает недостаток работников, заключается в том, что оно чаще рассматривается с точки зрения расходов, а не прибыли. Проще говоря, отдел системного администрирования не приносит реальных денег – он приносит расходы. Чтобы извлечь максимальную прибыль, предприятие должно минимизировать количество издержек, что зачастую ведет к сокращению размера и темпов роста группы системного администрирования.

Пример: контроль издержек

Компания среднего размера, занимающаяся разработкой программного обеспечения и вырастающая примерно на 30% в год, пыталась контролировать издержки и поэтому сократила рост бюджета группы системного администрирования. Руководство группы системного администрирования знало, что группа пострадает и что проблем в будущем будет еще

больше, но им было необходимо представить это в количественной форме высшему руководству компании.

Группа системного администрирования провела исследования, чтобы определить, как расходовался бюджет, и выделила факторы, которые она не могла контролировать, например затраты на поддержку отдельного пользователя или отдельного сервера. Однако группа не могла контролировать количество людей, нанятых другими группами, или количество серверов, купленных другими группами, поэтому она не могла контролировать свой бюджет на эти расходы. Если бы бюджет не соответствовал этим издержкам, уровни обслуживания упали бы.

Наиболее важным фактором было то, как обстояла работа с контрактами по обслуживанию. По прошествии первого года счета по контрактам на обслуживание машин согласно договору были предъявлены центральной группе системного администрирования, а не подразделениям, которые покупали и владели машинами. Основываясь на последних тенденциях, группа подсчитала темпы роста своего бюджета и определила, что через 5 лет весь бюджет системного администрирования будет целиком поглощен одними только контрактами на обслуживание. Не останется денег даже на зарплаты. Последний выходит, тушите свет (и подпишите контракт об обслуживании)!

Как только руководитель отдела системного администрирования смог привести цифры и объяснить проблемы финансирования группы, финансовый директор и его команда разработали новую модель финансирования, чтобы решить проблемы, возложив ответственность за расходы по системному администрированию на то подразделение, которое их вызвало.

Вы должны быть готовы объяснить и подтвердить денежные затраты на системное администрирование, если хотите избежать недостаточного финансирования.

Довольно сложно показать, как группа системного администрирования экономит деньги компании, когда все идет гладко. К сожалению, гораздо легче показать, где компания теряет деньги на набор сотрудников в группу системного администрирования, после того как инфраструктура и поддержка ухудшились до такой степени, что люди, работающие в структурных подразделениях, тратят значительное количество времени на решение компьютерных и сетевых проблем. Если компания достигает такой стадии, то восстановить порядок вещей полностью практически невозможно. Группа системного администрирования потеряет доверие и сотрудничество с клиентской базой, которые будет крайне трудно восстановить, независимо от качества финансирования.

Вам требуется избежать такого состояния, то есть изучить такие модели финансирования, которые работают. Вам необходимо уметь отвечать на следующие вопросы. Кто платит? Как это соизмеряется? Что пользователи получают за их деньги?

Проектирование модели финансирования также влияет и на организационную структуру, потому что люди, которые платят, обычно хотят иметь в своих руках значительный контроль. Как правило, системные администраторы либо оплачиваются напрямую подразделениями бизнеса и предоставляют отчет этим

подразделениям, либо централизованно финансируются компанией и составляют собственное подразделение. Это и есть соответственно *децентрализованная* и *централизованная* модели. Очень странно наблюдать, как компании переходят от одной модели к другой и обратно каждые несколько лет, так как у каждой модели есть свои сильные и слабые стороны.

Когда компания переходит от одной модели к другой, это всегда тяжело для системных администраторов. Для руководства очень важно проводить откровенные, открытые встречи с системными администраторами. Им необходимо услышать мнение руководства о сильных сторонах существующей структуры и проблемах, с которыми группе придется столкнуться для обеспечения поддержки этих сильных сторон. Также им нужно честно сказать, какие слабые стороны имеет действующая структура и как новая структура затронет эти слабости. Системным администраторам необходимо дать возможность высказывать свое мнение, задавать вопросы и предлагать решения. Кроме того, системные администраторы могут иметь значимые для руководства предположения о том, как можно сохранить существующие сильные стороны. Если системные администраторы вовлечены в процесс, у него будет гораздо больше шансов на успех. Представители пользователей также должны быть вовлечены в этот в процесс. Для достижения успеха необходимы общие усилия.

Основная мотивация децентрализованной модели – предоставить отдельным подразделениям лучшее или более адаптированное обслуживание за счет лучших отношений с их системными администраторами и бóльшими возможностями по контролю их действий. Для централизованной модели главное – контролировать издержки, отслеживая их централизованно, уменьшать их количество за счет устранения излишков, а также используя преимущества экономики масштабирования.

Когда компания переходит к централизованной организации системного администрирования, она испытывает необходимость в стандартизации и сокращении дублирования служб. Однако отдельные подразделения будут очень чувствительны к потере контроля и их хорошо адаптированных служб, опасаясь малейших неудач и спадов производительности после централизации, и не будут сразу доверять центральной группе. Вместо того чтобы работать совместно с центральной группой и попробовать решить проблемы, некоторые подразделения могут даже подпольно нанимать системных администраторов, чтобы предоставить поддержку, которая была раньше, лишая смысла процесс централизации и скрывая реальные расходы компании на системное администрирование.

Смена модели с одной на другую тяжела как для системных администраторов, так и для их пользователей. Гораздо лучше выбрать модель правильно с самого начала или работать над постоянными улучшениями, чем надеяться на то, что радикальные перемены помогут решить все проблемы, не создавая новых.

Финансирование группы системного администрирования должно быть в значительной степени децентрализовано, чтобы не стать черной дырой, в которой исчезают огромные суммы денег. Децентрализованное финансирование может помочь подразделениям бизнеса избежать затрат на поддержку старого оборудования и другой подобной траты времени. Также это позволит каждому подразделению бизнеса держать уровень поддержки в своих руках и иметь уровень, отличный от других подразделений. Отделу, который хочет лучшую поддержку, нужно будет либо содействовать системным администраторам в процессе автоматизации задач, либо финансировать расширение штата системных администраторов. Однако, когда у подразделения бизнеса всего один системный администратор, удвоение штата вряд ли будет большим шагом вперед.

Проведя временной анализ работы системных администраторов и каждого предварительно определенного SLA, возможно создать такую модель финансирования, при которой каждое подразделение бизнеса будет платить за каждого отдельного человека и каждый отдельный сервер, в зависимости от выбранного уровня обслуживания. Такие выплаты объединяют стоимость инфраструктуры для поддержки этих людей и машин с прямыми издержками. Такой подход децентрализует издержки и имеет то преимущество, что подразделениям бизнеса не приходится расширять штат системных администраторов целыми отделами. Он требует жестких процедур проверки – получают ли группы более высокий уровень обслуживания, за который они платят.

В идеале лица, пользующиеся обслуживанием, должны платить только за то обслуживание, которое они получают. Системы с фиксированной оплатой подвержены неправильной эксплуатации, когда пользователи начинают пытаться выжать из служб, за которые они платят, все, что только возможно, – это, как правило, приводит к сильному росту издержек. Тем не менее отслеживание расходов и тарификация могут добавить столько издержек, что дешевле будет терпеть небольшие злоупотребления службами. Комбинированный метод, при котором часть нагрузки переводится на более высокий уровень либо группы по достижении определенных лимитов ответственны за дополнительные расходы, может оказаться работоспособным. Например, мы можете разделить расходы по предоставлению удаленного доступа соразмерно по отделам, вместо того чтобы предоставлять счета на уровне отдельных пользователей. Группы, которые превышают предварительно определенный уровень на человека, также оплачивают все дополнительные расходы.

Естественно, по соображениям планирования бюджета и удержания контроля, руководство хочет либо точно знать, какими будут расходы, либо, по меньшей мере, иметь хорошую оценку. В этом случае они могут быть уверены, что не выйдут за пределы бюджета из-за непредвиденного роста расходов на системное администрирование. Один из способов решить этот вопрос – ежемесячные финансовые отчеты вместо «сюрприза» в конце года.

30.1.3. Влияние цепи управления

Цепь управления может существенно влиять на то, как работает организация системного администрирования. По большей части в быстро развивающихся компаниях информационные технологии могут находиться в ведении главного технического директора, на котором, кроме того, лежит ответственность за инженерные и исследовательские отделы, а также отдел разработки. В других компаниях системное администрирование подчиняется хозяйственному отделу и отчитывается перед главным исполнительным директором либо перед главным финансовым директором. Такое отличие имеет последствия. Если ваш информационный директор отчитывается вашему техническому директору, компания может смотреть на IT как на нечто, во что можно вкладывать деньги для извлечения доходов. Если же ваш информационный директор отчитывается вашему финансовому директору, компания может смотреть на IT как на расходы, которые необходимо сократить.

Когда отдел системного администрирования отчитывается перед техническим директором или перед инженерной организацией, возникают некоторые полезные эффекты и потенциальные проблемы. Самые требовательные пользователи бывают обычно именно в этих организациях, поэтому у них, как правило, наиболее близкие отношения с системными администраторами. Эта группа обычно хорошо финансируется, потому что является частью структурного подраз-

деления, где можно напрямую увидеть результаты инвестирования в системное администрирование. Однако другие части компании могут пострадать, потому что люди, устанавливающие приоритеты системных администраторов, будут отдавать приоритет проектам инженерной группы. По мере роста компании инженерный отдел будет разбит на несколько отделов, каждый со своим вице-президентом. К этому времени отдел системного администрирования также будет разбит на несколько групп, которые будут поддерживать различные подразделения бизнеса или отчитываться перед какой-нибудь другой частью компании, так как они не являются частью отдельной «инженерной» иерархии.

> В качестве грустного контрпримера можно привести случай, когда Том встретился с техническим директором, который не разбирался в информационных технологиях до такой степени, что считал, что высокотехнологичной компании не нужно IT-подразделение, так как «все должны быть настолько технически грамотными, чтобы самим следить за собственными машинами».

Напротив, отчетность через исполнительного или финансового директора будет означать, что отдел системного администрирования приносит сплошные расходы и никакой прибыли. Люди, перед которыми отчитываются системные администраторы, обычно имеют лишь слабое представление о том, что делает данная группа и какие затраты для этого необходимы. Тем не менее исполнительный или финансовый директор обычно имеет более широкий взгляд на компанию в целом и поэтому более беспристрастен при распределении ресурсов группы системного администрирования. Преимущество такой отчетной системы в том, что сильная группа руководителей имеет налаженную связь с высшим руководством для обсуждения бюджета, обязанностей и приоритетов группы. Может быть полезно отчитываться перед финансовым директором, так как бюджетные запросы группы системного администрирования можно обсудить и подтвердить, а позиция финансового директора заключается в определении лучшего для компании способа оплаты работы группы.

Аналогично, если группы системного администрирования отчитываются напрямую перед подразделениями бизнеса, которые их финансируют, подразделения обычно будут инвестировать в IT ровно столько денег, сколько им необходимо, хотя качество может быть различным в разных частях компании. Каждая структура отчетности имеет свои преимущества и недостатки. Не существует единого решения для всех организаций. Преимущества и недостатки также зависят от точек зрения и личностей людей, вовлеченных в эти процессы.

Руководство группы системного администрирования должно быть в курсе, как их структура отчетности влияет на группу системного администрирования, и использовать сильные стороны, по возможности избегая слабых сторон имеющейся структуры.

Друзья на высоких постах

Хотя близость к техническому директору в инновационных компаниях часто полезна, в одной компании, которая не была технически направленной, Том наблюдал обратное. Когда он устроился на работу, он беспо-

коился, что придется отчитываться перед исполнительным директором, а не техническим, что ему было удобнее.

В этой компании исполнительный директор отвечал за систему производства, которая делала для компании деньги: представьте себе высокотехнологичный конвейер, производящий вместо автомобилей и других материальных товаров финансовые транзакции для других компаний, с плотным ежемесячным графиком. Офис технического директора был недавно образованным отделом, который должен был привнести некоторые инновации в работу компании. Однако офис технического директора еще не был кредитоспособен.

Лучшей возможностью для IT-подразделения Тома было стать частью организации исполнительного директора. Исполнительный директор держала бóльшую часть денег в компании, так как ее часть компании зарабатывала деньги, на которые существовала остальная организация. Как часть ее организации, IT-группа могла совместно работать с исполнительным директором не только для лучшего финансирования всех обновлений, которые требовались в производственной части компании. Это также давало возможность влиять на организацию технического директора, играя роль пользователя того, что создает технический директор.

Когда исполнительному директору было что-то необходимо, у нее были на это средства. Когда Тому было что-то нужно, у него были способы влияния на исполнительного директора. Когда технический директор и Том в чем-то не соглашались, у Тома была возможность повлиять на человека, который контролировал все финансирование.

30.1.4. Подбор навыков

При создании группы системного администрирования менеджерам по персоналу необходимо собрать самодостаточную группу с разнообразными наборами навыков и должностями. Различные роли, которые могут играть системные администраторы, более подробно рассмотрены в приложении А.

Обязанности системных администраторов можно разделить на четыре основные группы. К первой относятся *техническое обслуживание* и *поддержка клиентов*, что включает в себя службу поддержки клиентов (глава 13), обслуживание серверов, службу поддержки второго уровня и специализированную поддержку для особых групп пользователей.

Ко второй группе относится *внедрение* новых служб. Этим представителям необходимо сосредоточиться на своих текущих проектах, поэтому их не должны затрагивать срочные пользовательские запросы, которые могут затянуть окончание проекта.

К третьей группе относится *проектирование* архитектуры новых служб. Группа проектирования состоит из системных *архитекторов*, которые исследуют новые технологии, проектируют и создают прототипы новых служб для пользователей и других системных администраторов. Группа проектирования

должна знать о нуждах пользователей от других групп системных администраторов и брать на себя ответственность за то, что новые службы будут спланированы и построены до того, как они понадобятся пользователям.

Если вы разделяете группы системных администраторов по ответственности за сети, базы данных и безопасность и т. д., каждая из этих групп должна иметь персонал, который будет справляться со всеми направлениями, охватываемыми администрированием. Должны быть люди для проектирования, внедрения и обслуживания в каждой поддерживаемой области.

Наконец, группа системного администрирования очень много выиграет от наличия *специалистов широкого профиля*, которые имеют глубокое понимание того, как работают и взаимодействуют практически все компоненты. Эти системные администраторы могут решать сложные, сквозные проблемы, которые могут быть не под силу системным администраторам, специализирующимся только в одной или двух областях. Специалистов широкого профиля часто называют *специалистами по интеграции*, потому что они эффективно объединяют различные технологии для создания наилучших систем и служб.

Часто эти группы пересекаются, особенно в маленьких компаниях, в которых одному или двум системным администраторам приходится исполнять все эти роли на определенном уровне. В больших компаниях эти должности обычно разделены. Младших системных администраторов обычно нанимают для работы в службе поддержки. По мере того как они набираются опыта, они могут перейти к поддержке второго уровня, а в дальнейшем выполнять обязанности по внедрению, ежедневной поддержке подразделений бизнеса или обслуживанию инфраструктуры. Самые высокие по должности системные администраторы, как правило, занимаются проектированием или являются специалистами широкого профиля.

В больших компаниях ищут способы предоставить системным администраторам шанс поработать иногда в других областях, в других группах, что способствует их профессиональному росту и обучению, а также помогает им обучать остальную команду на основе своего опыта и знаний.

Проводить всех системных администраторов через службу поддержки может быть полезным – это даст им важное понимание наиболее распространенных проблем, часть которых им придется решать постоянно. Также это может дать возможность обучения младших системных администраторов и более быстрого выполнения некоторых сложных запросов. Работников службы поддержки можно менять, чтобы дать им отдохнуть и провести неделю, обучаясь более серьезной работе с пользователями или конструкторами.

Аналогично, вовлечение конструкторов в работу по непосредственной поддержке пользователей поможет им понять потребности пользователей и то, насколько хорошо работают их службы. Привлечение конструкторов в работы по проектированию даст им особые знания и позволит улучшить взаимодействие с проектировщиками.

Системные администраторы на должностях, которые обычно не предполагают значительного общения с пользователями, таких как обслуживание серверов, проектирование, конструкторские должности, могут утратить верное представление о потребностях пользователей. Чередуя их деятельность с задачами, требующими значительного общения с пользователями, можно держать их в курсе направления работы компании.

Когда дела совсем плохи, наймите кого-нибудь получше

Иметь возможность нанимать персонал с различными навыками и уровнем – это привилегия компаний, у которых все очень неплохо. Когда дела идут хорошо, возможно нанять неопытного системного администратора, которого научит и подготовит более опытный коллега. Возможность продвижения собственных сотрудников снижает затраты на наем нового персонала, служит наградой для лучших сотрудников и аккумулирует внутренний интеллектуальный потенциал компании.

Однако, если у группы системного администрирования не все хорошо – системы регулярно дают сбои, пользователи недовольны, низкий моральный дух и т. д., – в этом случае требуется другая тактика. Когда дела идут плохо, необходимо нанять людей, ориентированных на реформы. Хорошо обученные люди с опытом работы в успешных компаниях как раз подходят на роль реформаторов.

При реформировании неблагополучной компании или даже при обновлении организации, у которой все неплохо, но требуются улучшения, начните с найма нескольких очень опытных людей, умеющих работать в команде. Когда ситуация начнет стабилизироваться, предоставьте им свободу действий по реорганизации группы – дайте им возможность использовать больше неопытных сотрудников так, как подсказывает им их опыт, или попросите нанять новых неопытных сотрудников, как описано в истории в разделе 2.1.5.3. Хорошие люди тянутся к хорошим людям; их профессиональные контакты помогут им найти нужных сотрудников.

Том любит говорить: «Когда дела совсем плохи, наймите кого-нибудь получше».

30.1.5. Группы инфраструктуры

По мере роста компании потребуются люди, занимающиеся исключительно поддержкой инфраструктуры. Группа инфраструктуры будет следить за такими централизованными службами, как аутентификация, печать, электронная почта, служба имен, календарная служба, сети, удаленный доступ, службы директорий и безопасность. Эта команда также обычно ответственна за автоматизированные службы для системных администраторов, такие как автоматическая загрузка, конфигурация и установка патчей на новые машины (глава 3).

Группа инфраструктуры должна быть сплоченным подразделением, даже если она распределена по нескольким местам. Инфраструктура компании должна быть целостной и непрерывной во всех подразделениях. Если различные группы управляют разными частями инфраструктуры, они смогут не прийти к согласию в вопросах использования протоколов и интерфейсов между компонентами, что приведет к нежелательным результатам.

Пример: поддержка распределенной сети

Крупная транснациональная компания по производству компьютеров создала средства распределенного управления сетями и компьютерами. Обязанности были распределены между IT-группами: центральный IT-отдел занимался WAN, удаленные подразделения имели локальные группы системного администрирования, а у каждого отдела из главного офиса была собственная IT-группа, занимающаяся системным и сетевым администрированием. На тот период средства удаленного администрирования, привычные для нас сегодня, отсутствовали.

Поначалу, с 20 подразделениями, казалось довольно легко выделять каждому подразделению поддомен, сеть класса C и предоставлять системным администраторам средства для простой генерации файлов зон DNS. Однако, когда у компании было уже 200 подразделений с разными администраторами, которые хотели управлять своими поддоменами совсем по-другому, всякий раз, когда администратор покидал компанию, группа системного администрирования испытывала проблемы с обучением персонала. Кроме того, многие конфликты оставались неразрешенными, так как во многих случаях цепи управления конфликтующих сторон пересекались только на уровне генерального директора. Никто не мог взять на себя обязанность судьи и решить, что должно быть сделано.

Такое количество поддоменов также увеличило объем работ, который приходилось выполнять системным администраторам, когда кто-либо переходил в другое подразделение. Приходилось перемещать почтовые ящики, псевдонимы электронных адресов, внутренние списки рассылки и переделывать карты NIS, различные серверы модемной аутентификации необходимо было обновить и т. д. С лучшей, централизованно управляемой системой пришлось бы всего лишь переместить почтовый ящик с единственным псевдонимом. Но при таком огромном количестве необходимых изменений что-то неизбежно пропускалось и возникали ошибки.

Отсутствие центральной структуры управления системным администрированием обходилось дорого для компании и по другим причинам: многочисленные группы системного администрирования не могли договориться о сетевой архитектуре и даже об используемом сетевом оборудовании. Перекрывающиеся дублирующие сети были построены на различном оборудовании. Несоответствие между аппаратной частью отражалось на сбоях в некоторых коммуникациях. Сеть, которая получалась в результате такого неконтролируемого, децентрализованного процесса, была ненадежна, и поддерживать ее не представлялось возможным, но каждое подразделение продолжало финансировать свою собственную группу администрирования и непреклонно защищало свою территорию.

Много лет спустя, когда все средства для централизации управления сетью, включая контроль пространств имен, сетевую адресацию и многие другие аспекты поддержки, стали доступными, компания все еще продолжала использовать свою устаревшую и неэффективную модель распределенного администрирования.

У каждого элемента инфраструктуры есть свой особый метод, согласно которому ее должны строить и поддерживать как самодостаточную единицу. Все службы инфраструктуры приходят в беспорядок, когда различные их части управляются разными группами, которые не взаимодействуют между собой. С точки зрения организации это значит, что желательно создать централизованную группу инфраструктуры и планировать ее рост по мере необходимости. Когда остальным частям потребуется их собственная инфраструктура системного администрирования, их системные администраторы должны отчитываться перед центральным руководством системного администрирования, а не местным.

Очень показательный в этом плане пример – электронная почта, которая является частью интерфейса между компанией с пользователями и остальным миром. Целостный образ – единый формат электронной почты, используемый по всей компании, сокрытие имен серверов и т. д. – придает компании профессиональный вид. А для системных администраторов единая архитектура электронной почты хороша тем, что ее легче отлаживать и администрировать. Использование выделенных точек, на которые приходит и откуда отправляется электронная почта компании, приводит к лучшей безопасности, так как фильтрация может быть более полной. Все это требует взаимодействия между группами инфраструктуры в глобальном масштабе.

Современные компьютерные инфраструктуры сильно зависят от сетей и сетевых служб. Если сетевая архитектура или архитектура сетевых служб либо неразумно спроектирована, либо плохо управляема, это увеличивает нагрузку системных администраторов, расходы и недовольство пользователей. Если каждому подразделению разрешен *творческий подход*, результатом будет кошмар для руководителей. Проектирование и конструирование сети должно быть совместным усилием, а там, где это невозможно, должны существовать четко определенные линии разграничения между зонами компании, которые имеют целостное внутреннее устройство.

Безопасность компании в целом сильна лишь настолько, насколько сильно слабейшее звено. Если у разных групп различные стандарты и подходы, определить уровень безопасности компании будет просто невозможно.

30.1.6. Поддержка пользователей

Поддержка пользователей – ключевой элемент функций системного администрирования. Поддерживать пользователей означает обеспечивать им возможность работать эффективно. Это, в свою очередь, означает, что все их компьютерные требования должны быть частью общего решения. Поддержка пользователей дает лучшие результаты при распределенной модели, в отличие от поддержки инфраструктуры.

Наличие выделенного персонала для поддержки пользователей помогает устанавливать соответствие вашего времени отклика с ожиданиями ваших пользователей. Как рассмотрено в разделе 31.1.3, наличие специализированного персонала для быстрого ответа на короткие запросы и передача больших запросов персоналу, не работающему с пользователями, устанавливает соответствие времени отклика со временем, ожидаемым пользователями.

Пользователям нравится, когда они лично знают тех людей, которые предоставляют им поддержку. Пользователи устанавливают отношения с этим человеком

и привыкают к его методу работы и стилю общения. Им гораздо комфортнее просить о помощи именно этого человека. Они имеют бóльшую уверенность в том, что их системный администратор знает, в какой обстановке они работают, какие службы и как использует их подразделение и чего можно ожидать от пользователей и среды.

Ранее мы указали, что выбор между централизованной и децентрализованной моделью для организации системного администрирования влияет на поддержку пользователей и на отношения как между самими системными администраторами, так и между системными администраторами и пользователями. При децентрализованной модели, где у каждого подразделения или группы есть своя собственная группа системного администрирования, связь с пользователями, как правило, сильная, но взаимодействие между системными администраторами зачастую слабое. У пользователей будут более близкие отношения с их системными администраторами, однако в конце концов они начнут страдать от отсутствия взаимодействия между самими системными администраторами. Например, если усилия системных администраторов не очень хорошо координируются, многие задачи не могут быть автоматизированы, не будет согласованных машин, операционных систем, единого уровня установленных патчей и дополнений во всей компании и некоторые службы, которые должны быть централизованы, будут реализованы несколько раз. Все это выльется в неэффективность и отсутствие надежности, что будет очень вредно для обслуживания, предоставляемого пользователям.

При централизованной модели связь между системными администраторами, как правило, сильная, а взаимодействие с пользовательской базой, напротив, слабое. Централизованная модель может привести к ситуации «мы против них» с обеих сторон. С другой стороны, это, как правило, компенсируется сильной инфраструктурой и более целостной и надежной организацией. Однако пользователям может показаться, что им не уделяют достаточно внимания, и проекты для отдельных подразделений могут неприемлемо задерживаться из-за проектов инфраструктуры или других подразделений. Каждое подразделение будет страдать от отсутствия собственного системного администратора для своих специфических нужд.

Централизованная модель поддержки может привести к тому, что пользователь, звоня в службу поддержки, будет каждый раз говорить с новым человеком. Так как системные администраторы обслуживают такое большое количество людей, системный администратор, отвечающий на звонок, может и не знать хорошо подразделение и самого пользователя. Это не та модель поддержки, которая устраивала бы пользователей. Группу пользователей должна поддерживать команда максимум из пяти системных администраторов. Пользователи должны знать своих системных администраторов и быть уверенными, что системные администраторы знакомы со структурой и требованиями их подразделения. Если в группу по работе с пользователями входит больше пяти человек, разбейте ее так, чтобы ее половина работала с половиной этой группы пользователей. Другой подход заключается в поиске путей сокращения количества системных администраторов, непосредственно предоставляющих поддержку пользователям данной группы, переводя некоторых системных администраторов на внутреннюю работу.

Некоторые компании используют комбинированные модели, при которых каждый отдел или подразделение бизнеса имеет несколько выделенных системных администраторов, которые отчитываются перед центральной организаци-

ей системного администрирования. Эта модель также неидеальна, так как системные администраторы некоторых подразделений бизнеса могут быть более красноречивыми, чем остальные, а это приведет к тому, что некоторые потребности одних подразделений не будут должным образом удовлетворяться централизованной автоматизацией и стандартизацией в пользу других подразделений. У комбинированных моделей большой потенциал, но они также могут иметь худшие стороны централизованной и децентрализованной моделей одновременно.

Какую бы модель вы ни выбрали, опасайтесь этих недостатков и пытайтесь делать все возможное для их нейтрализации.

30.1.7. Служба поддержки

Первый уровень службы поддержки пользователей – это уровень, который лучше всего работает при централизованном подходе. Это организация, которая получает первоначальные сообщения о проблемах и разрешает базовые вопросы, в противном случае отправляя запрос в соответствующую область. Пользователям нужен единый телефон, адрес электронной почты и веб-страница для отправки запросов в службу поддержки. Пользователи не хотят ни запоминать, какое конкретно подразделение занимается данной проблемой, ни рисковать тем, что их запрос затеряется между подразделениями, потому что тот, кто принял запрос, не знает, кто должен его выполнить.

Крупным компаниям требуются хорошо согласованные региональные службы поддержки, чтобы каждое достаточно большое подразделение имело собственную службу. При наличии нескольких служб поддержки процедуры передачи запроса на более высокий уровень и процедуры передачи управления становятся очень важными, так как некоторые запросы будут пересекать границы регионов. Крупным компаниям необходимо найти баланс между хорошо управляемой центральной службой поддержки, которая сама сможет принимать все звонки, и маленькими распределенными, которые не могут обработать все звонки, однако способны предоставить услуги системного администрирования в более дружелюбной и человечной манере. В главе 13 подробно рассмотрены создание служб поддержки и управление ими.

30.1.8. Аутсорсинг

Передача функции системного администрирования сторонним организациям может показаться приемлемым решением для некоторых организаций, потому что область системного администрирования, как правило, находится вне основной деятельности компании. Если системное администрирование не является ключевой частью бизнеса компании, компания может предпочесть привлечь стороннюю компанию для выполнения всех его функций. В этом случае компании необходимо лишь подписать контракт и не беспокоиться о найме системных администраторов, заработной плате, удержании сотрудников и всех других проблемах, связанных с наемными рабочими.

Для некоторых компаний привлечение сторонних исполнителей имеет смысл. Если компания действительно маленькая и имеет базовые компьютерные потребности, подписание контракта будет проще найма системного администратора, когда в компании нет никого, кто бы мог оценить уровень знаний и производительность этого системного администратора. Если компания не будет

удовлетворена организацией, предоставляющей услуги системного администрирования, она может расторгнуть контракт или выбрать более сложный путь замены этой организации на новую. Изменить или расторгнуть договор о найме не так уж и просто.

Компаниям иного типа не следует передавать IT-функции другим компаниям или нужно делать это крайне осторожно. Для компаний, занимающихся электронной коммерцией, IT и системное администрирование – основные части бизнеса. Компании, которые полагаются на устойчивые к отказам компьютерные системы, обнаружат, что договоры о найме становятся невероятно дорогими, когда учитываются их требования к надежности. Организациям, зависящим от передовых технологий, часто бывает необходимо иметь также и собственные системы, так как компании, предоставляющие услуги, имеют собственные технологические стандарты, на которые сложно повлиять отдельным пользователям. В сложных ситуациях избавиться от плохо выполняющего свои обязанности поставщика услуг труднее. Нелегко переключиться от одной группы системного администрирования к другой без больших потерь качества обслуживания и перебоев на то время, пока новая группа адаптируется к данной организации.

Безопасность – другая проблема при привлечении сторонних компаний. Если для компании важна безопасность, особенно в областях защиты информации и обработки конфиденциальной информации пользователей, юридический отдел должен потребовать строго конфиденциальных соглашений и сведений о том, с какими компаниями, кроме вашей, поставщик услуг безопасности работал, работает и будет работать. Если бреши в системе безопасности могут привести к потере доверия клиентов или каким-то другим серьезным образом затронут прибыль компании, обеспечение безопасности должно быть одним из ключевых направлений работы компании. Внутренний штат сотрудников службы безопасности заинтересован в успехах компании, тогда как заинтересованность стороннего поставщика будет ограничена условиями контракта.

В компаниях, для которых присутствие в Интернете или сайт электронной коммерции – основной источник дохода, функция системного администрирования по обслуживанию данного сайта – одна из основных областей их бизнеса. Поэтому многие компании не хотят привлекать сторонних исполнителей в эту область их бизнеса. Они хотят, чтобы люди, ответственные за поддержку высокой доступности, были заинтересованы в общем деле. Компании, для которых присутствие в Интернете не является основным источником дохода и которым не требуются компьютерные системы высокой доступности, могут не захотеть содержать дорогостоящую группу системного администрирования для круглосуточного обслуживания, поскольку привлечение сторонних организаций в этом случае будет финансово более выгодным.

Многие компании частично решают вопрос своего присутствия в Интернете с помощью аутсорсинга, помещая машины своих интернет-служб в аппаратном центре провайдера. Главное преимущество такого подхода в том, что поставщик услуг имеет широкополосные интернет-соединения высокой степени избыточности, а также системы электропитания и охлаждения высокой надежности, которые слишком дорого было бы содержать большинству компаний. Располагать свои машины в аппаратной провайдера лучше при крупном масштабе производства. Некоторые высококлассные компании-поставщики услуг также обеспечивают поддержку и аппаратной части, и запущенного на ней программного обеспечения. Другие могут предоставлять включение и выключение

питания по запросу. Как и в других случаях привлечения сторонних исполнителей, важно определить уровни обслуживания в контракте, с денежными взысканиями, если они не будут предоставлены. Уровни обслуживания должны включать гарантированную пропускную способность, время отклика на служебные запросы, питание и охлаждение, время непрерывной работы, физическую безопасность, а также гарантии доступности сети.

Привлечение сторонних исполнителей – сложный вопрос, на который у многих людей есть твердые взгляды. Мы попытались представить некоторые доводы «за» и «против» для различных ситуаций. Более подробно эта тема рассмотрена в разделе 21.2.2.

30.2. Тонкости

Тонкости организации системного администрирования заключаются в возможности использования консультантов и подрядчиков, чтобы помочь вашей группе расти и строить новые службы и инфраструктуру, сохраняя при этом приемлемые уровни обслуживания. Правильно используемые консультанты и специалисты могут предоставить персоналу компании возможность профессионального роста и извлечения опыта. Неправильное их использование может вызывать раздражение, приводить в уныние и отчуждать группу системного администрирования.

Мы проводим различие между консультантами и подрядчиками по их уровню навыков и работе, которой они занимаются. Консультант привносит особые новые и глубокие знания, обычно в специализированные проекты. Подрядчик привносит навыки, которыми компания уже может располагать, и фактически дублирует работу внутренней группы системного администрирования компании.

30.2.1. Консультанты и подрядчики

Консультанты, которые являются экспертами в своих областях, могут быть полезным временным дополнением к группе системного администрирования. Консультант должен быть вовлечен в особый проект, например проектирование и построение новой службы, которая должна быть быстро расширена на всю компанию и в которой системные администраторы компании могут на данный момент не иметь опыта.

Благоприятные отношения с консультантом вовлекут в проект, над которым трудится консультант, системных администраторов, особенно архитекторов и конструкторов. Консультант должен стремиться делиться идеями, решать проблему сообща и работать совместно с группой, а не диктовать им, что и как делать. Хороший консультант может вносить необходимые специализированные знания и опыт в новые начинания, что приведет к лучшему проектированию и увеличению знаний собственных системных администраторов компании.

С другой стороны, для морального духа и успешности команды системного администрирования не очень хорошо нанимать консультантов для новых и интересных проектов, в то время как собственные системные администраторы будут заниматься ежедневной рутинной поддержкой и обслуживанием. Новая служба будет не так хорошо поддерживаться, как в том случае, если бы

собственные системные администраторы участвовали в проекте и понимали принципы его разработки. Она также может не учитывать местные особенности или быть не так хорошо интегрированной с другими системами, как в том случае, если бы при проектировании использовался собственный опыт. Собственные системные администраторы не получат возможности профессионального роста и обучения новым навыкам и будут крайне недовольны своим положением, что приведет к высокой текучести кадров и неприемлемым уровням поддержки пользователей.

Если нужно конструировать новые решения, но у собственных системных администраторов нет времени на участие в них, необходимо нанять подрядчиков, которые выполняли бы ежедневную работу собственных системных администраторов, необязательно для создания новой службы. Обычно проект будет более успешным с точки зрения бюджета, возможностей и последующей поддержки и обслуживания, если в нем участвуют собственные системные администраторы, чем когда он был полностью отдан группе извне. Помощь системным администраторам в виде их освобождения от ежедневных обязанностей и предоставления возможности принимать участие в новых проектах также приведет к созданию более сильной и позитивно настроенной группы системных администраторов.

Чередование собственных системных администраторов, которые принимают участие в интересных проектах, так, чтобы все они имели шанс поучаствовать в проекте, также усиливает группу.

Контракт на отдельные задачи

Установка коммерческих систем резервного копирования/восстановления данных обычно довольно сложна. На третий или четвертый раз это уже гораздо проще, но большинство системных администраторов никогда не достигают в этом достаточного уровня мастерства. Новая система резервного копирования устанавливается каждые несколько лет.

Вместо этого будет гораздо дешевле нанять кого-нибудь, чтобы провести установку. Найдите кого-нибудь, кто уже три или четыре раза устанавливал именно эту систему.

Большинство компаний, создающих программное обеспечение для резервного копирования, имеют профессиональные сервисные группы, которые проведут установку за вас. На наш взгляд, такие команды бесценны. Они настраивают все надлежащим образом и обучают имеющийся персонал деталям, необходимым для ежедневной работы.

Однажды Том видел, как системный администратор устанавливал такую систему на протяжении 6 месяцев. Его постоянно прерывали работой над другим проектом, что растягивало и откладывало проект. Компания была довольна, что ей не пришлось заплатить 10 000 долларов за контракт с профессиональной службой. Том считал, что лучше бы она их заплатила.

Многие подобные задачи выигрывают от привлечения специалиста с опытом.

30.3. Примеры организационных структур

Как различные роли и обязанности должны распределяться в разных по размеру компаниях? Чем в компаниях электронной коммерции отличается организация подразделений системного администрирования? Чем отличаются учебная и некоммерческая организации? Мы рассмотрим, как должна выглядеть организация системного администрирования в малых, средних и крупных компаниях, организациях электронной коммерции и университете/некоммерческой организации. В этих примерах предполагается, что малая организация насчитывает от 20 до 200 сотрудников, компания среднего размера – от 200 до 1000 сотрудников; а крупная – больше 1000 сотрудников. Это приблизительные цифры; у малой компании с множеством участков есть много потребностей большой компании.

30.3.1. Малая компания

У малой компании будет один или два системных администратора, от которых ожидается удовлетворение всех основных потребностей бизнеса. Не будет официальной службы поддержки, хотя запросы должны будут проходить через систему электронной помощи. Системные администраторы будут вовлечены в поддержку пользователей и обслуживание инфраструктуры. Однако только один из системных администраторов будет привлекаться к проектированию и конструированию новых служб по мере их необходимости.

Когда штат малой компании превысит 200 сотрудников и она начнет становиться компанией среднего размера, будет формироваться и ее организация системного администрирования. Это промежуточное время, когда высшему руководству компании предстоит принять важные решения о том, как организовать и финансировать системное администрирование. На переходных этапах будет сформирована официальная служба поддержки, которая изначально будет состоять из системных администраторов, чередующих друг друга на должностях поддержки пользователей.

30.3.2. Компания среднего размера

В компании среднего размера системные администраторы начинают специализироваться несколько активнее. Прежде чем штат компании дорастет до 1000 человек, должна быть сформирована группа службы поддержки с выделенным персоналом. Предполагается, что служба поддержки будет решать достаточно сложные задачи. Системные администраторы на должностях поддержки пользователей все еще могут чередоваться, чтобы расширить выделенный штат. Некоторые системные администраторы будут специализироваться на конкретных операционных системах; другие займутся сетями и безопасностью, сначала работая по совместительству, а затем, по мере роста компании, на полную ставку. Архитекторы большей частью будут и конструкторами и, в идеале, должны уметь решать комплексные проблемы, связанные с несколькими различными технологиями. Штат службы поддержки пользователей также может привлекаться к задачам по проектированию и конструированию, выделяя дни для работы над проектом или с пользователями.

30.3.3. Крупная компания

В крупной компании будет высокая степень специализации в группе системного администрирования, хорошо организованная служба поддержки, с четко определенной группой поддержки второго уровня для более сложных проблем, небольшие группы по работе с пользователями, специализированные группы по различным отделам или подразделениям бизнеса, а также центральные группы поддержки инфраструктуры и безопасности. Кроме того, в крупной компании будет по крайней мере один архитектор и команда разработчиков на каждое технологическое направление. У компании могут быть региональные организации системного администрирования или организации системного администрирования, ориентированные на филиалы либо большие подразделения бизнеса. Эти организации системного администрирования будут нуждаться в официальных каналах связи для координации их работы и четко определенных областях ответственности. По возможности они должны подчиняться тем же самым политикам компании.

30.3.4. Компания электронной коммерции

Компания электронной коммерции отличается от других организаций тем, что у нее есть две группы компьютеров, сетей и служб, которые требуют различных уровней доступности и направлены на решение разных задач. Проблемы системы, ориентированной на внешних клиентов компании, всегда будут иметь высший приоритет по сравнению с внутренними пользовательскими запросами о поддержке, так как первые всегда напрямую связаны с прибылью компании.

Чтобы избежать данного конфликта интересов, компании с крупным подразделением электронной коммерции необходимо выделить две группы системного администрирования: одну – для поддержки присутствия в Интернете, а другую – только для обслуживания корпоративных систем (этого также часто требует соблюдение закона Сарбейнса–Оксли). Должно быть четкое разделение между оборудованием, используемым для каждой системы, так как у них различные требования к доступности и вообще разные назначения. Организации, в которых элементы интернет-служб зависят от элементов корпоративной инфраструктуры, неминуемо сталкиваются с проблемами. При четком делении также легче выполнять обслуживание, если за каждую область ответственны различные группы системных администраторов.

Состав корпоративной группы системных администраторов зависит от размера компании. Состав интернет-службы серьезно отличается. В ней может быть служба поддержки, которая является частью организации поддержки пользователей[1]. Хотя эта служба может и включать поддержку второго уровня, на который перенаправляются запросы, у нее не будет маленьких внутренних групп поддержки пользователей, обслуживающих каждое подразделение. Будут лишь системные администраторы, ответственные за поддержку и обслуживание интернет-службы, а также архитекторы и разработчики, которые проектируют

[1] Служба поддержки, которая обеспечивает поддержку внешних пользователей компании, в противоположность внутренним пользователям, обслуживаемым корпоративной группой системного администрирования.

и внедряют усовершенствования службы, расширяют службу, чтобы удовлетворить требования пользователей.

Две IT-группы Google

В Google есть две различные IT-группы. Группа системных операций обслуживает внутренние IT-системы. Ответственная за сайт инженерная группа обслуживает системы, используемые в веб-проектах. Изначально была одна группа, но ее разделение позволило системным администраторам лучше удовлетворять требования бизнеса и создало среду, в которой отсутствуют конфликты из-за приоритетов.

30.3.5. Университеты и некоммерческие организации

Для некоммерческих организаций важно держать под контролем текущие расходы. Как правило, у них очень ограниченный бюджет, поэтому крайне важно использовать имеющиеся на компьютерные системы средства должным образом, чтобы при этом все отделы и подразделения работали совместно в общих интересах. Однако в университетах часто образуются сферы интересов вокруг того финансирования, которое получают отдельные исследовательские группы или профессора. В интересах университета или некоммерческой компании имеет смысл максимально все централизовать и работать как одна команда. Это потребует от руководителя организации сильных навыков управления, а также хорошего обслуживания центральной группы системного администрирования.

Пример: мудро используйте ограниченные ресурсы

Вот пример того, что может произойти, если отсутствует бюджет для централизованных служб. У факультета университета были ограниченные средства, выделенные на оборудование. Несколько исследовательских групп из этого подразделения получали дополнительные деньги на оборудование от своих исследовательских проектов. Оборудование, которое больше не использовалось в исследовательской группе, отдавалось факультету, чтобы помочь удовлетворить потребности студентов и инфраструктуры. У факультета было несколько важных потребностей, которые он не имел возможности финансировать. Систему резервного копирования возможно было применять только для машин, которыми пользовались студенты. Для компьютеров исследовательской группы не было службы резервного копирования. Серверы, которые предоставляли данному факультету службы электронной почты, печати, базу программного обеспечения, а также службы домашних директорий, были двумя ненадежными машинами, спроектированными для использования в качестве рабочих станций и работавшими уже 7 лет.

Тем не менее согласование вопросов, как лучше использовать деньги с исследовательских договоров, в отделе не проводилось. У одного профессора было достаточно денег, полученных с исследований, чтобы купить четыре или пять современных компьютеров, с достаточным диско-

вым пространством, мониторами и подходящими графическими картами. Вместо этого он решил купить два самых дорогих компьютера, с эффектными, но совершенно бесполезными аппаратными излишествами, и дополнительные процессоры, которые были несовместимы с вычислительным кодом, запускаемым на данной машине. Оба компьютера были отданы некоему аспиранту, доктору философии, у которого уже и так имелся высококлассный компьютер. По большей части они простаивали. Факультет не получил ни одной машины, как и не было достигнуто соглашение о заказе сервера резервного копирования для исследовательского общества факультета.

Профессора имели право тратить свои собственные деньги, как им вздумается, и никто из них не горел желанием расходовать их на то, что могло принести выгоду людям за пределами их группы в дополнение к их собственной. Вместо этого деньги были явно выброшены на ветер, отчего пострадало все отделение. В конечном итоге глава факультета был ответственен за то, что не смог мотивировать профессоров факультета работать как одна команда.

30.4. Заключение

Размер и расходы группы системного администрирования – области, за которыми часто следят очень внимательно. Если организация системного администрирования отчитывается на уровне вице-президента, это может иметь существенное влияние на две упомянутые области. Компания, как правило, хочет оптимизировать свои расходы на системное администрирование, поэтому для него часто устанавливается наименьший возможный бюджет, чтобы не пострадали другие люди в компании. Группа системного администрирования в общем и ее руководство в частности обязаны помочь компании выбрать правильное соотношение. Оптимизация группы системного администрирования таким образом, чтобы она имела правильный набор навыков и должностей, – один из способов, которыми может помочь организация системного администрирования. Предоставлять данные о том, как и почему расходы других групп влияют на расходы группы системного администрирования, полезно, как и предложение и участие в таких моделях финансирования, которые повысят непосредственную ответственность других подразделений за расходы на системное администрирование, что, в свою очередь, сделает анализ расходов/доходов структурного подразделения более точным.

Другая важная область организации системного администрирования – это выбор между централизованным и децентрализованным системным администрированием. Подразделения инфраструктуры должны быть централизованны для предоставления отлаженного, надежного сервиса. Исключением является подразделение службы поддержки – более прямая поддержка пользователей может выиграть от меньшей централизации, но есть множество подводных камней, которых следует избегать. Взаимодействие между системными администраторами должно поддерживаться на высоком уровне, группам необходимо работать сообща, а разрешение конфликтов должно происходить на более низком уровне цепи руководства, чем уровень генерального директора.

Консультантов и подрядчиков можно эффективно использовать как краткосрочные ресурсы для продвижения особых проектов, которым иначе пришлось бы подождать. Однако они должны использоваться так, чтобы предоставить собственным системным администраторам возможность участвовать в интересных проектах, учиться и улучшать свои навыки. Использование исключительно кратковременных ресурсов для построения систем, а собственных системных администраторов лишь для поддержки – не лучшее решение.

По мере роста компаний системные администраторы стремятся стать более специализированными, сконцентрированными на конкретных областях, вместо того чтобы решать все возникающие проблемы. Системные администраторы встречаются с проблемами масштаба в областях, которые не возникают в компаниях меньшего размера. Крупным компаниям нужны архитекторы для различных технологических направлений, чтобы иметь общую картину и вести группу в правильном направлении. Также очень большое преимущество крупной компании принесет наличие нескольких специалистов широкого профиля для решения комплексных задач.

Компаниям, которые в основном предоставляют обслуживание через Интернет, как правило, нужны две отдельные группы системного администрирования для поддержки двух разных частей инфраструктуры. Кроме того, группе, поддерживающей интернет-службу, необходим набор навыков, отличный от необходимого обычной внутренней группе системного администрирования.

Задания

1. Является ли ваша группа системного администрирования централизованной или децентрализованной?
2. Есть ли у вашей группы системного администрирования децентрализованные части, которые могли бы работать эффективнее, будучи централизованными? Какие проблемы, по-вашему, решит централизация этих групп? Какие проблемы она может создать?
3. Есть ли у вашей группы системного администрирования централизованные части, которые могли бы работать эффективнее, будучи децентрализованными? Какие проблемы, по-вашему, решит децентрализация этих групп? Какие проблемы она может создать?
4. Каким образом вашей организацией были эффективно наняты консультанты или подрядчики?
5. Каким образом вашей организацией были неэффективно наняты консультанты или подрядчики?
6. Как финансируется ваша организация системного администрирования? Какие у вашей модели финансирования имеются недостатки и преимущества? Вы можете предложить пути ее улучшения? Какие данные вам придется представить высшему руководству для одобрения ваших идей?
7. Каковы отношения между различными частями вашей организации системного администрирования? Вы размышляли о способах, при помощи которых можно периодически привлекать ваших системных администраторов для работы в других областях? Какие преимущества и недостатки получит группа от воплощения этой идеи?

Глава 31

Восприятие и заметность

При правильном выполнении системное администрирование похоже на хороший театр: аудитория видит прекрасное представление и никогда не задумывается о том, сколько месяцев планирования потребовалось для его создания или какой объем работ выполнялся во время представления за кулисами. Бóльшая часть работы, необходимой для представления, невидима для аудитории. Системные администраторы обычно работают за кулисами. Это все так, но аудитория ценит представление *больше*, если понимает, чего стоило его создание. Аудитория больше способствует успеху театра, если чувствует какую-то связь с его сотрудниками.

Восприятие – это то, каким люди вас видят, это мера качества. **Заметность** – это сколько люди вас видят, это мера количества. Эта глава о том, каким пользователи вас видят и как улучшить их восприятие. Вы великий человек[1], и мы надеемся, что эта глава поможет вам показать себя с лучшей стороны.

Ощущения пользователей – это ваш образ в их реальности. Если вы работаете усердно, но это не выглядит таковым, люди будут считать, что вы не работаете усердно. Если они не знают, что вы существуете, вас не существует. Если они знают, что вы существуете, но не имеют представления о том, что вы делаете, они будут допускать худшее. Такова действительность.

Многие системные администраторы считают, что если они будут хорошо выполнять техническую часть работы, то создадут хорошее впечатление и будут видимыми. Это неправда. Многие системные администраторы считают, что настоящих системных администраторов касаются только технические проблемы, а восприятие и заметность – это не их забота. Это либо забота их руководителя, либо у них нет времени интересоваться тем, как другие люди воспринимают их, либо все это вообще ерунда. Мы надеемся изменить ваше мнение. Для этого мы пытались сделать наши примеры настолько реальными и земными, насколько это возможно.

31.1. Основы

Этот раздел о восприятии. Мы уже установили, что вы хороший человек. Правильно ли люди вас воспринимают? Основы этой главы касаются улучшения

---

[1] Наш издатель уверяет нас, что эта книга будет читаться только такими же замечательными людьми, как вы.

того, как вас воспринимают, и создания вашего положительного образа. Каждое ваше взаимодействие с другими – это шанс улучшить их восприятие. Первое впечатление, которое вы производите на пользователей, будет определяющим при дальнейшем взаимодействии с ними. У вас должно быть положительное отношение к людям, которых вы поддерживаете, потому что они будут воспринимать вас по этому отношению.

Пользователи оценивают эффективность работы не по тому, как усердно вы работаете, а по тому, как быстро выполняются их запросы. Поэтому мы рассмотрим подход, который позволит вам установить ваши приоритеты в соответствии с ожиданиями пользователей по времени выполнения работы. Мы завершим этот раздел обсуждением темы, которую мы называем «Быть системным адвокатом», – заблаговременного удовлетворения потребностей пользователей.

Вы ответственны за то, как вас воспринимают – позитивно или негативно. Возьмите на себя ответственность по улучшению того, как вас воспринимают. Никто не сделает это за вас.

Ниже рассмотрено несколько ключевых элементов, которыми должен овладеть каждый системный администратор, чтобы добиться положительного восприятия. Некоторые из них больше подходят для инициативы руководства, но другими нужно овладеть на личном уровне. После этого мы рассмотрим приемы, которыми могут воспользоваться системные администраторы для повышения уровня своей заметности.

31.1.1. Хорошее первое впечатление

Важно произвести на ваших пользователей хорошее первое впечатление. Если вы неправильно начнете, трудно будет снова завоевать их доверие. Однако, если вы произведете хорошее первое впечатление, возможная ошибка будет воспринята как случайность.

Попытайтесь вспомнить первый день учебного года в начальной школе. Ребенок, который в этот день попадал в неприятности, считался «плохим ребенком» весь оставшийся год. За ним пристально следили, ему редко доверяли, и у него никогда не было презумпции невиновности. Если что-то шло не так, то в этом подозревали его. С другой стороны, некоторые ученики вели себя хорошо первую неделю в школе. Их поведение было образцовым, и они очень старались понравиться учителю. В течение всего года им могли сойти с рук небольшие нарушения либо они могли спросить и получить разрешение нарушить правила.

Подумайте о впечатлении, которое вы производите, как о счете в банке с хорошей репутацией. Каждый хороший поступок, который вы сделали, записывается на этот счет. Если вам повезет, вы можете позволить себе сделать один плохой поступок на каждые пять хороших поступков на счету. Хорошее первое впечатление начинает этот банковский счет с положительным балансом.

Если ваше первое взаимодействие с пользователем – это встреча, то вы можете многое сделать, чтобы произвести хорошее первое впечатление: придите вовремя или раньше, будьте вежливым, дружелюбным и внимательным. Люди – это существа, воспринимающие мир визуально, поэтому внешность и выражение лица они замечают в первую очередь. Улыбайтесь.

Волосы другого цвета

Одеться так, чтобы произвести хорошее первое впечатление, в различных компаниях может означать разное. Одна женщина-системный администратор, которую мы знаем, носит мешковатые комбинезоны и красит свои волосы в ярко-розовый цвет по современной моде рейверов. Она очень сильно выделяется! Какое-то время она была системным администратором одной из крупнейших компаний Силиконовой долины. Когда ее назначили для прямой поддержки веб-фермы небольшой группы людей, они относились к ней с большим уважением и энтузиазмом. Однажды коллега сказал ей, что причина, по которой ее так быстро приняли пользователи, заключалась в том, что они решили, что любой, кто так одевается и не получает за это замечаний, должен быть отличным техническим специалистом.

Уделяйте внимание своей одежде. В различных компаниях подходящая одежда понимается по-разному – в одних компаниях уважают костюм, а в других над ним смеются. Если нам неважно, как мы одеваемся, это не означает, что другие люди такие же.

Когда я впервые тебя увидел

Том случайно встретил человека, которого не видел несколько лет. Этот парень мимоходом упомянул: «Я до сих пор помню глупую футболку, которая была на тебе, когда я впервые тебя увидел!» Первые впечатления – это продолжительные впечатления. Каждый день может стать днем, когда вы можете произвести первое впечатление.

Ваше выражение лица также важно. Дружелюбный, спокойный вид – это величайший актив, который может иметь системный администратор. Улыбайтесь тут и там, иначе люди запомнят вас «сердитым».

Не кричите. Не кричите в споре или из-за того, что кто-то раздражает вас в ситуации, которая иначе была бы спокойной. Кричать на людей плохо. Правда, плохо. Настолько плохо, что за это людей понижают в должности, увольняют или даже хуже. В ярости или раздражении почти невозможно найти и сказать что-то вежливое, а если вы скажете что-то вежливое, это прозвучит иначе. Лучше всего просто исключить себя из этой ситуации. Если вы так раздражены, что боитесь сорваться и на кого-то закричать, скажите, что вам нужно выйти в туалет. Это всегда работает. Необходимость выйти в туалет является социально приемлемым оправданием, даже если вы на важном собрании, разговариваете по телефону или стоите перед неработающим сервером, а в спину вам дышит генеральный директор. Это удобная причина сделать перерыв и расслабиться. Все понимают, что это значит и почему требуются немедленные действия.

У вас уже сформировалась базовая репутация среди ваших нынешних пользователей, но очень важно производить хорошее первое впечатление на каждого нового человека, которого нанимают. В конце концов, эти «новые люди» будут боль-

шинством ваших пользователей. Произведение хорошего первого впечатления на новых сотрудников начинается до их первого дня на работе. Вам нужно обеспечить, чтобы, когда они придут, они нашли свои компьютеры у себя в офисах, настроенные, с созданными учетными записями, и чтобы все работало правильно.

В первый рабочий день человек может быть нервным и бояться своего нового окружения. Наличие обустроенного рабочего места создает у него чувство теплоты и гостеприимства, которое влияет на его впечатление не только о системных администраторах, но и обо всей компании. У системных администраторов есть возможность приобрести репутацию людей организованных, компетентных и учитывающих потребности своих пользователей.

Компании понимают, что первый рабочий день нового сотрудника задает настрой всему периоду его работы в компании. Человек, который приходит в первый рабочий день, обычно имеет очень высокую мотивацию. Для поддержания этой мотивации его работа сразу должна быть производительной. Каждый день, который отделяет человека от производительной работы, снижает мотивацию. Если вам нужна высокая производительность, убедитесь, что новые сотрудники сразу могут начать работать.

М-е-д-л-е-н-н-а-я доставка компьютеров

Одна программистка из Нью-Джерси рассказала нам, что, когда она начала работать в большой страховой компании, у нее не было компьютера в течение первого месяца. Это может быть приемлемо для нетехнических специальностей, но она была программисткой! Сотрудники ее группы очень удивились, что это ее расстраивало, потому что для установки компьютеров в их подразделении это считалось нормальным. Первый месяц ей платили ни за что, и все считали это «нормальным». Это была пустая трата ресурсов компании. Тот факт, что коллеги привыкли к такой медленной реакции, показывает, что системные администраторы этой компании работали так не впечатляюще уже давно.

Гораздо лучше относиться к установке новых компьютеров как ко времени для создания положительного образа

Доставка компьютеров

В Нью-Йоркском технологическом институте доставка новых компьютеров студентам и персоналу представляет собой очень занятный ритуал. Компьютеры привозят на тележке, украшенной бубенчиками.

Все знают: звук бубенчиков означает, что кто-то получает новый компьютер. По мере того как тележка едет по коридору, собирается толпа желающих посмотреть, кому везут компьютер. Наконец тележка достигает пункта назначения. Все смотрят, как компьютер вынимают из тележки и ставят на стол человека. Возгласы «Ооооо» и «Аааaа» звучат как при открывании подарков во время праздника по поводу рождения ребенка. Иногда люди даже аплодируют. Конечно, компьютер был предварительно настроен и проверен, чтобы сейчас его можно было просто включить и использовать. Репетиции делают совершенным все.

Чтобы убедиться в том, что в первый рабочий день у людей есть все необходимое, вы должны создать процесс совместно с другим административным персоналом, часто не входящим в группу системного администрирования. У секретарей обычно есть контрольный список встреч со всеми новыми сотрудниками. Очень важно убедиться, что компьютерные потребности входят в этот список: выяснение того, какой компьютер нужен человеку, заказ компьютера, размещение сетевых разъемов, выяснение предпочтительного для человека имени учетной записи, определение внутренних списков рассылки, на которые человеку нужно подписаться, выяснение, какие нужны программы, создание учетных записей и т. д. Если существует стандартная конфигурация настольного компьютера, заранее настроенные машины должны быть под рукой, готовые к установке. Иначе должен существовать процесс, в соответствии с которым с новым сотрудником связываются заблаговременно за несколько недель, чтобы согласовать нужное оборудование, заказать, установить и проверить его.

В первый рабочий день сотрудника наиболее дружелюбный сотрудник вашей группы системных администраторов должен встретиться с человеком для личного инструктажа, ответа на вопросы и персональной доставки напечатанного руководства «Добро пожаловать в нашу сеть». Процесс инструктажа представляет группу системных администраторов в лучшем виде. Это обнадеживает пользователя. Пользователям не нравятся безликие организации. Проще рассердиться на человека, которого вы никогда не видели. Инструктаж – это вложение, которое окупается более тесной связью в будущем.

Пример: собрания для инструктажа

Если системные администраторы не будут встречаться с новыми сотрудниками для инструктажа, это будет делать кто-то еще. В одной компании посчитали, что такой инструктаж был бы для системных администраторов пустой тратой времени, а для новых сотрудников – раздражающим фактором. Вместо этого коллега рассказывал человеку о том, как войти в систему, ругая в это время группу системных администраторов или вспоминая последнее незапланированное отключение системы. Прошло довольно много времени, прежде чем системные администраторы поняли, что происходит, и еще больше, прежде чем они смогли переломить ситуацию и восстановить свою репутацию.

31.1.2. Отношение, восприятие и пользователи

То, как люди вас воспринимают, непосредственно связано с отношением, которое вы показываете. Иметь положительное отношение очень важно, потому что люди очень быстро улавливают ваше настроение.

Проблема отношения номер один среди системных администраторов – это вопиющее неуважение к людям, для обслуживания которых они наняты. Удивительно, насколько часто нам приходится напоминать системным администраторам, что их пользователи – это не «лузеры» или «юзвери». Они являются причиной, по которой у системных администраторов есть работа. Системные администраторы находятся здесь, чтобы обслуживать, а также, что более важно, защищать этих людей. Системные администраторы и пользователи компьютеров находятся по одну сторону баррикад.

Мы призываем к тому, чтобы системные администраторы перестали использовать понятие *«юзеры»* и заменили его на термин *«пользователи»* (Smallwood 1992). Это будет напоминанием того, что системные администраторы работают в сфере обслуживания, поддерживая потребности этих людей, а не «паразитов», которые весь день делают запросы. Это может значительно изменить отношение системных администраторов.

Работа в качестве консультанта очень просвещает, пользователи напрямую платят вам за вашу работу по системному администрированию и заменят вас, если вы не будете соответствовать их требованиям. Она помогает вам понять, насколько лучше все работает, когда вы относитесь к «юзерам» как к пользователям и действительно заботитесь о том, что им нужно.

С другой стороны, системный администратор может попасть в неприятности, если он будет руководствоваться принципом «пользователь всегда прав». Это другая крайность. Часть работы системного администратора состоит в том, чтобы (вежливо) сказать «нет», когда это нужно. Системный администратор может, в конце концов, начать делать работу пользователя, если будет выполнять *все*, что пользователь попросит. Вместо этого системный администратор не должен забывать содействовать пользователю в том, чтобы он сам себе помогал. Это поиск равновесия. Руководство группы системного администрирования должно четко определить, где провести границу (см. раздел 13.1.5). Кроме того, это помогает принять принцип «то, что я *могу* это сделать, не означает, что я *должен*». Научите пользователей, как делать что-то самостоятельно, предоставьте документацию, обеспечьте, чтобы они стали хорошими пользователями, которые не будут постоянно спрашивать, как что-то сделать. Кроме того, обязанность системных администраторов – вежливо отклонять просьбы, которые противоречат политике.

По мере того как системный администратор переходит от поддержки пользователей на более высокие должности, такие как проектировщик систем, связь с «пользователем» часто предоставляет возможность для большего сотрудничества, при котором системный администратор и пользователь вместе работают в команде. Когда это происходит, вы пытаетесь развить отношения «деловых партнеров». Вы работаете вместе, чтобы сделать лучше для компании, и определяете «сферы деятельности», которые разграничивают, что должны делать системные администраторы, а что – пользователи, но между вами по-прежнему должны сохраняться отношения как между пользователями и системными администраторами.

Мы постарались смоделировать такой язык в этой книге. Мы всегда называем людей, которых обслуживаем, «пользователями», используя понятие «юзер», только когда имеем в виду, что человек пользуется лишь конкретным устройством или службой.

Другая проблема с отношением, которая может возникнуть у системных администраторов, – это раздражение системных администраторов из-за того, что пользователи ничего не делают, но лишь создают для них проблемы. Системные администраторы могут развить неприязнь к пользователям и начать избегать их или жаловаться каждый раз, когда пользователи приходят к ним в офис. Это плохо. Мы слышали такие высказывания: «О, здорово! Пришла еще одна проблема». Это забавная ситуация, потому что ваша работа как системного адми-

нистратора – устранять проблемы. Если вас раздражает постоянный поток проблем, возможно, вам нужен отпуск (см. раздел 32.2.2.8). Более позитивное отношение – рассматривать каждую «проблему» как загадку, решение которой – это интересный вызов.

С этой ситуацией связано раздражение из-за того, что «все мои юзеры тупые» или «почему эти люди постоянно звонят в службу поддержки с глупыми вопросами?». Наш ответ: они бы не звонили, если бы знали ответ, и вас бы не наняли, если бы вы не знали об этом больше, чем они. «Мои юзеры – идиоты! Они практически ничего не знают о компьютерах!» Наш ответ: они знают достаточно, чтобы работать на компанию, у которой хватает ума, чтобы нанять кого-то вроде вас, кто может отвечать на их вопросы, и об областях своей деятельности они знают гораздо больше, чем вы.

Создавайте возможность такого взаимодействия с пользователями, при котором они не будут приходить к вам с проблемами. Проявите инициативу периодического их посещения. Мы приведем несколько предложений далее в этой главе.

Высказывания о пользователях

Один системный администратор перестал уважать своих пользователей и вскоре был уволен после того, как он во всеуслышание жаловался на них в кафетерии компании. Он жаловался на то, что, хотя пользователи много знали в областях, не касающихся компьютеров, их подход к компьютерам, по его мнению, был идиотским. Он без конца жаловался на них в обед и объяснял, что помогать им было ниже его достоинства. Одной из его ошибок было то, что он называл их *идиотами* (и даже хуже). Другой его ошибкой было непонимание знаков, которые его коллеги подавали ему жестами, пытаясь объяснить, что люди, о которых он говорил, и их директор сидели за столом позади него. Как вы можете догадаться, вопрос был решен руководством на очень высоком уровне.

Если ваши пользователи вас раздражают, пожалуйтесь своему руководителю лично и работайте над конструктивными решениями. Не жалуйтесь на них на людях и помните, что сообщения электронной почты можно переслать, в окна чатов легко подсмотреть, а разговоры без труда прослушиваются через стены офисных помещений. Высказаться – это необходимая форма избавления от стресса, найдите для этого правильное место.

Вы должны развить предусмотрительное отношение к сообщениям о проблемах. Запросы от пользователей могут представлять собой интересные вызовы и возможность выполнить фантастическую работу, которой вы сможете гордиться. Когда вы внесете такое отношение в свою жизнь, пользователи заметят перемену в обслуживании, которое вы предоставляете. Отвечая на заявку пользователя, закончите искренней благодарностью за сообщение о проблеме: «Спасибо, что сообщили об этом. Это помогло нам исправить проблему и найти пути предотвратить ее в будущем». Это может создать совершенно другое ощущение. Ваше отношение видно во всем, что вы делаете.

31.1.3. Приоритеты, установленные в соответствии с ожиданиями пользователей

То, как вы определяете приоритеты своих задач, влияет на восприятие пользователями вашей эффективности. Вы можете сделать пользователей гораздо счастливее, если ваши приоритеты будут соответствовать их ожиданиям[1].

Пользователи ожидают, что небольшие задачи будут выполняться быстро, а крупные проблемы потребуют значительного количества времени. Определения *«небольшие»* и *«крупные»* – это выражение их ощущений, которые основаны на их восприятии вашей работы. Например, смена пароля, которая воспринимается как требующая одной-двух минут, должна выполняться быстро. Установка нового компьютера воспринимается как более объемный процесс, и оправданно тратить на него день или два. Когда отключается критический сервер, пользователи ожидают, что вы все бросите и будете устранять эту экстренную проблему[2]. Следовательно, вы можете сделать пользователей гораздо счастливее, если установите приоритет запросов таким образом, что сначала будут урегулироваться экстренные вопросы, затем – проблемы, которые решаются быстро, а после этого – запросы, на которые требуется больше времени.

В каждый конкретный день ваша группа может выполнить 100, 500 или 5000 000 запросов. Если вы будете выполнять их в порядке поступления, ваши пользователи не будут особенно рады вашей работе, даже несмотря на выполнение их запросов. Вместо этого вы можете выполнять в день тот же объем работы, но в другом порядке, и пользователи будут довольны, потому что это соответствует их ожиданиям.

Пользователь расстроится, если ему сказать, что его небольшой просьбе придется подождать, пока вы не выполните более крупный запрос, например установку нового компьютера. Представьте, как бы вы расстроились, если бы вам пришлось ждать печати одной страницы, потому что кто-то печатает 400-страничный отчет, который был в очереди перед вами. Это очень похоже. Однако важно обеспечить, чтобы крупные задачи не откладывались из-за небольших задач бесконечно.

Кроме того, задержка выполнения таких задач, как смена пароля, воспринимается негативно из-за цепного эффекта. Невозможность войти в систему задерживает другие задачи. Человек, который не способен войти в систему, не может выполнять другую работу. Однако замена старого компьютера на новый вряд ли будет восприниматься так же, потому что у человека уже есть компьютер.

Часто быстрые запросы легко автоматизировать, чтобы перевести на самообслуживание. Вы можете создать веб-страницу, которая выполняет задание для пользователя. Могут существовать способы, при помощи которых люди смогут сменить идентификатор, чтобы автоматически получить другой пароль. Вместо личной выдачи IP-адресов системный администратор может настроить DHCP-сервер, чтобы IP-адреса предоставлялись в реальном времени, удовлетворяя

---

[1] Спасибо Ральфу Лоуре (Ralph Loura) за этот подход.

[2] Консольные серверы позволяют вам выполнять задачи в консоли сервера с вашего рабочего места. Однако у пользователей может сложиться впечатление, что машина вас не волнует, потому что вы не в серверной. Может быть полезно объяснить им, что виртуально вы работаете в серверной, возможно, пригласив их посмотреть на ваш экран.

ожидания пользователей и не требуя никакой работы со стороны системных администраторов. Однако некоторые устройства не могут использовать DHCP, в таких случаях нам приходится проявить больше изобретательности. Создание веб-страницы, которая позволяет пользователям устанавливать свои IP-адреса, может не стоить затраченных на это сил. Вместо этого вы можете повесить список следующих десяти доступных IP-адресов на своей двери. Люди могут отрывать IP-адрес, которым они хотят воспользоваться, если они напечатают свои имена в нужном месте, чтобы в дальнейшем вы могли обновить свой список. Такие творческие решения может быть интересно создавать. Иногда решение является очень простым, например разместить запасные картриджи рядом с принтером, чтобы время на их смену не включало лишние 15 мин, необходимые для того, чтобы дойти до удаленной комнаты с расходными материалами.

Используя такой подход лично для себя, вы также можете применять его в масштабах организации. Вы можете разделить группу системных администраторов таким образом, чтобы сотрудники службы поддержки нижнего уровня обслуживали запросы, которые, в соответствии с ожиданиями пользователей, должны быть выполнены срочно. Требования, выполнение которых займет больше времени, можно передавать персоналу более высокого уровня. Старшие системные администраторы могут отвечать за более крупные проекты, например создание служб. Такое разделение труда позволяет вам обеспечить соответствие ваших приоритетов ожиданиям пользователей и защищает людей, которые работают над долгосрочными проектами, от постоянных прерываний (см. раздел 32.1.2.1). На первый взгляд это может себе позволить только большая группа системных администраторов, но от такого подхода может выиграть даже группа из двух системных администраторов. Один системный администратор может защищать другого от прерываний в первой половине дня, а во второй – наоборот. Это называется подходом взаимной защиты от прерываний (Limoncelli 2005).

31.1.4. Системный адвокат

Пользователи воспринимают вас как нечто среднее между клерком, который выполняет черную работу по мере ее поступления, и адвокатом, который заблаговременно решает их проблемы и отстаивает их интересы. Этот раздел о том, как стать адвокатом, – такую позицию мы считаем лучшей.

На одной стороне находится то, что мы называем системным клерком, который скорее реагирует на проблемы, чем предупреждает их. Ему точно указывают, что делать, и он не участвует в планировании своей работы. Иногда расходы на оплату труда клерка идут из нетехнических бюджетов. Системный клерк может проводить свой день, устанавливая программы, выполняя резервное копирование, создавая учетные записи путем ручного ввода необходимых команд и т. д.

С другой стороны – системный адвокат, который заблаговременно разбирается с техническими потребностями своих пользователей, доводит эти потребности до руководства, автоматизирует рутинные задачи, которые его просят выполнить, и участвует в процессе планирования проектов, которые его затрагивают. Ранее мы рассматривали установку машин и создание учетных записей пользователей за день до их выхода на работу. Чтобы достичь этой цели, системные администраторы должны участвовать в процессе найма. Вовлечение в процесс – это одна из заблаговременных мер, которые может предпринять адвокат.

Между клерком и адвокатом есть бесконечное количество градаций. Постарайтесь осознать, где вы находитесь и что можете сделать, чтобы двигаться в сторону адвоката.

Переход к адвокату – это медленная эволюция. Она начинается с одного проекта, направленного на опережение событий. Опережающий подход – это вложение, которое может с лихвой окупиться в будущем. Вы тратите время сейчас, чтобы экономить его в будущем. Вам может быть трудно выделить время для заблаговременной работы, если вы не умеете держать голову над водой. Выберите какой-нибудь аспект, улучшение которого, по вашему мнению, принесет значительную пользу, и посоветуйтесь об этом со своим руководителем. Если ваш руководитель поверит в целесообразность вашего проекта, он может захотеть перераспределить ваше рабочее время для выполнения этого проекта.

Есть много преимуществ в том, чтобы быть адвокатом, а не клерком. Это лучше для вашей компании, поскольку означает, что вы согласуете свои приоритеты с приоритетами своих пользователей. Это переводит ваш взгляд на то, как вы можете лучше обслуживать людей, которые оценивают вас и наблюдают за вами. Это лучше для вас, потому что поддерживает вашу репутацию как исполнительного человека. У людей с такой репутацией выше шансы при наличии возможностей повышения. Когда все преимущества оцениваются, это, конечно, помогает заслужить репутацию самого полезного человека в группе.

В большой группе обычно будет весь спектр сотрудников – от клерков до адвокатов. Клерки – это важная часть группы. С роли клерка системные администраторы начинают работать и учиться у других, они предоставляют адвокатам полезную поддержку. Однако даже самый неопытный системный администратор должен развить отношение заблаговременного исполнения и работать в направлении адвоката. Есть значительная разница между клерком, управляемым системными администраторами, и клерком, управляемым пользователями. Работа под управлением системных администраторов означает указания по правильным способам выполнения задач и возможность расти и учиться. Клерк, которым управляют пользователи, не имеет возможности учиться у экспертов в своей области и может чувствовать себя изолированным.

Самое большое преимущество достигается за счет применения исполнительного подхода во всей группе системных администраторов. Группа становится активной, позитивной движущей силой, направленной на изменения в организации. Ее начинают ценить как целое. Многим компаниям жизненно важно наличие подходящей IT-инфраструктуры для выполнения своих деловых задач. Будьте частью этой инфраструктуры.

Ниже приведено несколько примеров, иллюстрирующих различие в поведении клерка и адвоката в разных ситуациях.

31.1.4.1. Установка программ

Возможно, вы считаете, что устанавливать программы довольно просто, но в этом процессе есть много подпроцессов. Например, клерк может получить программу для установки от пользователя, который ее купил. Пользователь мог заказать ее несколько недель назад и с нетерпением ждать установки. Часто в такой ситуации что-то идет не так. Пользователь не знал, что есть сетевой сервер лицензий, и приобрел лицензию только для своей рабочей станции. Это нарушает стратегию наличия небольшого количества хорошо организованных и наблюдаемых серверов лицензий. Чаще установка не удается из-за какой-то простой причины, для устранения которой требуется долгое время. Например, пользователь рассчитывал, что программа будет установлена на машину, которая оказалась перегруженной и на которую нельзя ставить новые приложения;

приложение лицензировано для узла, который скоро выводится из эксплуатации; либо системе не хватает дискового пространства. Устранение таких препятствий, чтобы вторая попытка установки стала успешной, может потребовать много времени.

Пока клерк поздравляет себя с выполнением установки после преодоления такого большого количества препятствий, пользователь жалуется начальнику системного администратора, что ему потребовалось ждать установки программы несколько недель. Пользователь не понимает, что установка нового диска должна планироваться. Он также не понимает, что добавление нового сервера лицензий требует дополнительного мониторинга и планирования надежности и что, если не полагаться на запланированную инфраструктуру, дальнейшая работа потребует от системных администраторов больших усилий. Никто не подсчитывает реальные расходы на программу, которые должны включать стоимость дискового пространства, ресурсов процессора и тот факт, что установка выполнялась два раза, потому что первая попытка не удалась из-за недостаточного дискового пространства. Усилия по установке в течение нескольких недель не соответствовали ожиданию пользователем быстрой установки после получения носителя. Как было рассмотрено в разделе 31.1.3, соответствие ожиданиям пользователя критически важно.

Системный адвокат находился бы в положении, которое позволило бы сделать процесс более плавным. Пользователи знали бы, что системный администратор должен быть вовлечен в процесс с его начала. Адвокат опросил бы пользователя, чтобы понять назначение программы, и выполнил бы планирование емкости для выделения необходимых ресурсов диска, процессора и сети. График, согласованный всеми участвующими сторонами, позволил бы избежать непонимания. Закупка включала бы программу – возможно, заказанную системным администратором для обеспечения правильного лицензирования, – а также дополнительные ресурсы диска, процессора и сети. Проблемы, например недостаток дискового пространства, могли быть решены во время ожидания доставки программы.

Такое планирование устанавливает соответствие программы имеющимся ресурсам диска, процессора и сети и предоставляет пользователю лучшее понимание процессов системного администрирования, а системному администратору – лучшее понимание потребностей пользователя. Люди ценят то, что они понимают, и недооценивают то, чего не понимают. Благодаря этому процессору обе стороны больше ценят друг друга.

31.1.4.2. Решение проблемы быстродействия

Пользователь жалуется на низкое быстродействие системы. Клерка могут попросить установить на машину пользователя более быструю сетевую карту, поскольку все пользователи полагают, что системы всегда «тормозят» из-за медленных сетей[1]. После установки мало что улучшается, и пользователь не удовлетворен результатом. Не была проведена правильная диагностика проблемы. На самом деле мы много раз сталкивались с тем, что в такой ситуации быстродействие становилось хуже. Теперь у компьютера была более быстрая сетевая карта, чем у сервера, и он перегружал сервер потоком трафика. Проблему исправила бы модернизация сервера.

[1] Историческая справка: до сетевой компьютеризации было принято винить в этом недостаток памяти.

Адвокат принял бы более активное участие в наблюдении проблемы – в идеальном случае до того, как пользователь заметил это, если есть хорошая система мониторинга, – применяя различные средства диагностики проблемы и предлагая те или иные решения. Адвокат уделил бы время объяснению проблемы и различных потенциальных решений, чтобы они с пользователем могли вместе выбрать наилучшее. Предложение представляется руководству пользователем, который теперь может прояснить все вопросы. Системный администратор находится рядом, чтобы поддержать пользователя, если тот ошибется. После того как руководство одобрит закупку и проблема решится, пользователь будет очень счастлив.

Результатом таких совместных действий станет сообщество пользователей, которое проявляет больше заинтересованности в развитие сети.

31.1.4.3. Простая автоматизация

Адвокат планирует работу (см. главу 32), чтобы выделить время на проекты, которые будут предотвращать проблемы. Кроме того, он выделяет себе в течение рабочего дня дополнительное время, автоматизируя свои задачи, которые выполняются дольше других. Автоматизация открывает лучшие пути выполнения задач.

Клерк может предпочесть отложить все запросы на создание учетных записей до определенного дня в неделю, а затем выполнить их все сразу. Пользователи сталкиваются с очень плохим графиком выполнения. Адвокат автоматизирует задачу, поэтому создание учетных записей становится простым и он может выполнять его по первому требованию.

Автоматизация задачи необязательно должна быть очень сложной. Не погружайтесь с головой в создание совершенной системы. Простой скрипт, который помогает вам с наиболее распространенным случаем, может быть ценнее, чем крупная система, которая автоматизирует все возможные аспекты задачи. Например, автоматизация создания учетной записи является простой, за исключением особых случаев, например учетных записей администраторов. Автоматизируйте 80%, для которых это возможно, и оставьте эти особые случаи для следующих версий программы. Документируйте случаи, которые требуют ручной обработки. Для данных случаев документация особенно важна, потому что процесс выполняется гораздо реже, поэтому проще забыть нюансы. Кроме того, автоматизация скрывает, как выполняются нормальные задачи, поэтому у сотрудников, выполняющих особые задачи, нет базового уровня, с которым они могут сравнить свою работу.

Вместо скрипта, который что-то автоматизирует, можно написать скрипт, выдающий команды, которые выполняют задачу. Системный администратор может проверять команды на правильность, редактировать их для особых случаев и затем вставлять их в командную строку. Написание таких скриптов обычно проще, чем автоматизация всего процесса, и может быть этапом к дальнейшей автоматизации процесса.

Ручная установка ОС на машину также может быть долгим процессом, особенно если нужно сделать ряд индивидуальных изменений по памяти. Разработчики ОС предоставляют средства автоматизации установки, которые также автоматизируют индивидуализацию, как рассмотрено в главе 3. Адвокат пользуется этими средствами, клерк продолжает устанавливать ОС вручную.

Автоматизация часто выполняется только для точного повторения процессов и предотвращения ошибок, не обеспечивая других способов ускорения выполнения задачи. Простая последовательность команд, включающих имена файлов, в которых легко ошибиться, является подходящим для автоматизации процессом, если это сэкономит немного времени. Экономия времени вызвана отсутствием необходимости исправлять ошибки.

31.1.4.4. Полная автоматизация

Самое важное, что нужно запомнить при автоматизации процесса, – сначала выполнить весь процесс вручную, а затем точно автоматизировать эти шаги. После этого вы можете импровизировать, вводить новые возможности или написать небольшую программу и даже сделать ее элементом более крупной структуры. Но сначала вы должны выполнить процесс сами и автоматизировать свои шаги.

Мы знаем это из своего опыта. Мы видели много неопытных системных администраторов, которые неделями пытались автоматизировать процесс только для того, чтобы обнаружить, что пытаются выполнить то, о работе чего *они* не имеют точного представления! Легко попасть в эту ловушку. На теоретическом уровне люди думают, что знают, как это выполняется. Это звучит просто, почему автоматизация должна быть сложной? Почему бы не начать просто с написания кода для этого? В результате много времени тратится впустую, потому что вы не знаете, можете ли что-то сделать, пока вы это не сделаете.

По мере выполнения процесса вручную записывайте, что вы делайте. Выполняйте процесс, а не просто продумывайте ваш путь. У вас не так хорошо получается симулировать компьютер, как у компьютера. Например, если вы автоматизируете создание учетных записей пользователей, записывайте все шаги по мере ручного выполнения процесса. Теперь проверьте учетную запись, чтобы убедиться, что она работает. Вы можете обнаружить, что что-то забыли, и это потребует от вас повторить процесс.

После того как шаги будут записаны, подумайте, как автоматизировать каждый из них. Есть ли команда, которая выполняет эту функцию? Что происходит «за кулисами», когда вы щелкаете по этой кнопке? Изменяет ли это параметры реестра? Запускает программу? Обновляет файл?

Теперь напишите код для автоматизации одного шага. Не ждите, пока весь код будет написан, чтобы начать тестирование. Тестируйте каждый шаг по отдельности, прежде чем добавить его к вашей основной программе. Тестируйте основную программу после добавления каждого этапа автоматизации. Нахождение ошибок на раннем этапе – ключ к написанию надежного кода. Это предотвращает ситуацию, в которой вы обнаруживаете, что ошибка на первом этапе сделала остальной ваш код бесполезным. Еще хуже обнаружить, что исправление ошибки на первом этапе затронуло все остальные этапы. Что если переменная, определенная на первом этапе, теперь должна стать массивом переменных? Нужно изменить все этапы, на которых использовалась эта переменная. Что если вы случайно не поменяли ее везде? Что если это кардинально изменит алгоритмы, используемые на следующих этапах? Если эти шаги уже написаны, то вам придется изменять код в соответствии с переменной, а не писать его нормально с первого раза. В силу этих причин автоматизация и тестирование по одному шагу приведут к созданию лучшей системы.

Книга *«The Practice of Programming»* Кернигана и Пайка (Kernighan and Pike 1999) дает прекрасные советы по такой постепенной разработке и тестированию ваших программ. *«Programming Pearls»* Бентли (Bentley 1999) – отличная книга для ознакомления, если вам потребуется разрабатывать более сложные алгоритмы.

31.2. Тонкости

До сих пор в данной главе рассматривались способы улучшения того, как вас воспринимают. Следующий уровень – расширить вашу заметность. Мы говорили о качестве, теперь мы говорим о количестве.

Парадокс заметности системного администратора заключается в том, что системных администраторов замечают только тогда, когда что-то ломается. Достижение нескольких месяцев 100-процентной безотказной работы требует значительного объема закулисного труда и самоотдачи. У руководства может сложиться впечатление, что системные администраторы не нужны, потому что оно не видит объема выполняемой работы. Затем каждый час начинает происходить сбой сервера, пока не будет заменен контролер. Системный администратор вдруг становится ценным. Он герой. Он важен. Это не очень хорошее положение вещей, поскольку у людей формируется впечатление, что 95% времени системные администраторы ничего не делают, так как люди не видят важной закулисной работы, которую выполняют системные администраторы.

Один из вариантов – поддерживать нестабильную систему, чтобы системные администраторы всегда требовались и их всегда замечали. Это плохая идея. Лучше найти тонкие пути обеспечения понимания пользователями ценности того, что делают системные администраторы.

Вы ответственны за то, какую заметность имеете. Возьмите на себя ответственность за это достижение. Никто не покажет вас, кроме вас самих.

Не стоит пытаться применять ни один из описанных ниже подходов, если вы не предоставляете своим пользователем хорошее обслуживание. Основа хорошей заметности – выполнение хорошей работы. Бессмысленно рекламировать плохой продукт.

31.2.1. Веб-страница состояния системы

Хороший способ быть заметным для своих пользователей – создать веб-страницу, на которой отражается состояние вашей сети. Системные администраторы должны иметь возможность легко обновлять сообщение о состоянии, чтобы в случае сбоев они могли без труда о них сообщить. Когда сбоев нет, это должно быть указано. Состояние должно иметь метки даты и времени, чтобы люди знали, насколько свежими являются данные. На этой странице должна быть информация о том, как сообщить о проблемах, ссылки на ваши системы мониторинга и новости о недавних серьезных изменениях.

Большинство людей хотя бы раз в день запускают веб-броузер. Если домашняя страница – это ваша страница состояния, у вас есть возможность довольно часто появляться в их поле зрения. Так как пользователи могут изменять домашнюю страницу своего броузера, важно включать содержимое, которое интересно пользователям, каждый день, чтобы они не захотели сменить страницу.

Ссылки на сайты о местной погоде, новости и корпоративные услуги могут отбить у людей желание менять домашнюю страницу.

Веб-страница состояния информирует пользователей о вашей постоянной заинтересованности. Если сообщается о сбое, это говорит пользователям, что вы работаете над проблемой, и снижает количество избыточных телефонных звонков с жалобами на прерывание обслуживания.

Сообщение о состоянии должно быть простым и убеждать людей в том, что над проблемой работают. «Сервер `sinclair` отключен, мы работаем над ним». При отсутствии этой информации люди часто предполагают, что вы ушли обедать, игнорируете проблему или некомпетентны в данной проблеме. Затрата десяти секунд на сообщение о состоянии создает желательный для вас положительный образ.

По мере того как пользователи привыкнут проверять эту веб-страницу, вас будут меньше отрывать от работы по устранению проблемы. Нет ничего хуже, чем задержка работы над проблемой из-за того, что вы заняты ответами на телефонные звонки людей, которые хотят помочь вам, сообщая о проблеме. У людей не разовьется привычка проверять эту страницу, пока вы не будете постоянно обновлять ее.

Это может быть простая веб-страница или сложный веб-портал, на котором есть другие новости и функции. Коммерческие и бесплатные программы создания порталов имеют различную функциональность и сложность.

Решения без применения высоких технологий также эффективно работают. В одной компании просто повесили доску объявлений перед входом в серверную, и системные администраторы вывешивали сообщения о состоянии на ней. Если метод позволяет распространить сообщение, то он является хорошим решением. Такой подход будет хорошо работать только в небольших компаниях, где серверная расположена удобно для пользователей. В некоторых компаниях на доску объявлений направлена веб-камера, чтобы на нее было еще удобнее смотреть.

31.2.2. Встречи с руководством

Несмотря на то что полезно быть заметным всем пользователям, уместен и более дифференцированный подход. Регулярные персональные встречи с главой каждой группы пользователей могут быть очень ценными. Часто каждому системному администратору назначается одна или две группы пользователей. 30-минутная встреча с руководителем каждой группы раз в две недели может держать его в курсе проектов, выполняемых для его сотрудников. Руководитель может быть в курсе того, какая работа запрашивается его персоналом, и помогать устанавливать приоритеты этих проектов. Время от времени вы будете обнаруживать, что руководитель устраняет некоторые запросы. Дополнительная задача таких встреч – рассказывать руководителю об инфраструктурных изменениях, которые выполняются для улучшения сети, хотя и являются незаметными. Этот процесс имеет большое значение в освещении невидимых сторон вашей работы.

31.2.3. Физическая заметность

При рассмотрении своей заметности учитывайте свою физическую заметность. Место, где вы сидите, может вывести вас из поля зрения и памяти людей. Если

ваш офис скрыт за физическим барьером, вы создаете образ недоступности и недружелюбия. Если ваш офис у всех на виду, то вы под микроскопом. Каждый перерыв в вашей деятельности будет казаться снижением темпа работы. Люди не понимают, что работа системного администратора включает периоды действий и бездействия.

Хорошо найти равновесия между физической заметностью и незаметностью. Стратегический подход к этому – обеспечить хорошее распределение заметности в вашей группе. Люди, ответственные за непосредственное взаимодействие с пользователями и их обслуживание, должны быть более заметны, а служебные программисты и разработчики архитектуры – менее заметны.

Размещение офиса и заметность

Когда Том работал в Bell Labs, после завершения ремонта появилась возможность переехать в новые офисы. Его начальник решил переместить системных администраторов, работающих с пользователями, в офисы в коридорах, по которым ходило много народу. Старшие системные администраторы, больше ориентированные на работу по проектам, получили офисы в конце тупиковых коридоров, где было меньше прохожих. Физическое размещение вызвало большую заметность людей, которые должны были быть видны, и спрятало тех, кого обычно не стоило прерывать.

Размещение стола и заметность

Когда Том пришел в Cibernet, его попросили устранить проблему в лондонском офисе, где люди беспокоили старшего системного администратора тривиальными вопросами, которые могли быть решены младшими системными администраторами. Когда он приехал в офис, он сразу же увидел проблему.

Офис был размещен в открытом пространстве, во многом аналогично центру обработки вызовов, а группа системных администраторов находилась в дальнем конце. Из-за размещения рабочих мест пользователь, который шел к системным администраторам, физически достигал старшего системного администратора первым. Люди обращались со своими проблемами к первому системному администратору, до которого они доходили.

Том изменил места размещения людей, и это существенно улучшило ситуацию.

31.2.4. Общие собрания

Другой способ расширить ваш положительный образ – проводить регулярные собрания, открытые для всех пользователей. Такие собрания могут быть прекрасным местом для двустороннего общения. Но также они могут стать катастрофой, если вы не подготовитесь. Планирование – это самое главное.

В некоторых организациях проводятся ежегодные общие собрания, которые обычно включают представление руководителем высокого уровня «состояния сети», когда рассматриваются достижения прошлого года и ставятся задачи на следующий год. Обычно это представляет собой презентацию со слайдами. Один из способов показать, что в вашей группе системных администраторов есть разделение труда и структура, – организовать, чтобы главы различных областей кратко представляли свои направления, а не один человек вел всю презентацию. После каждой презентации должны следовать ответы на вопросы. При отсутствии нормального планирования такие собрания могут затянуться навечно. Важно, чтобы все выступающие встретились для планирования того, сколько времени каждый из них будет говорить и что скажет. Создайте сценарий, с которым ознакомятся все выступающие. Убедитесь, что у вас нет избыточности и все соблюдают график. Пусть кто-нибудь представляет людей и сигнализирует им, когда их время истекло.

В некоторых организациях проводятся ежемесячные или ежеквартальные собрания. Эти собрания групп пользователей часто представляют собой комбинацию развлечения (чтобы втянуть людей в процесс) и двустороннего общения. Первая половина может быть презентацией или выступлением. Вы можете попросить разработчика рассказать о чем-нибудь интересном, например о перспективной линейке продуктов или о новом продукте. Избегайте торговых презентаций. Системные администраторы должны представить новое, привлекательное для пользователей средство и создать заинтересованность, представляя планы основных обновлений сети, информацию по актуальной тематике, например как избегать спама, и т. д. Это отличное место для проведения генеральной репетиции презентации статей, которые системные администраторы, возможно, будут проводить на будущих конференциях, например LISA. Это также показывает пользователям, что персонал системного администрирования получает всеобщее признание своей хорошей работы и профессионализма. Вторая половина – это двустороннее общение, например ответы на вопросы или обсуждение конкретной темы. Кроме того, такие собрания являются хорошей возможностью объявить о запланированных изменениях и объяснить, зачем они нужны. Далее мы приведем формат, который используется в одной организации для ежеквартальных собраний пользовательских групп.

1. *Приветствие* (2 мин): поприветствовать группу и поблагодарить людей за то, что они пришли. Хорошая мысль – разместить на доске объявлений повестку собрания, чтобы люди знали, чего ожидать.
2. *Представление* (5 мин): участники представляются. Если коллектив большой, попросите каждую группу или другое подразделение поднять руки.
3. *Общение* (20 мин): общение с пользователями – это одновременно и искусство, и наука. Вам нужно, чтобы люди сосредоточились на своих потребностях, а не на том, как эти потребности должны быть выполнены. Попробуйте пройти курс проведения собраний, если вы чувствуете себя плохо подготовленным в данной области. Задавайте открытые вопросы, например: «Если что-то одно может быть улучшено, то это...», «Наихудший элемент нашей компьютерной среды – это...», «Моя работа была бы проще, если бы...».

   Записывайте предложения участников. Лучше всего использовать большой лист бумаги на подставке, чтобы все видели, что записывается. Не записывайте полные предложения, только ключевые фразы, например «быстрее устанавливать новые версии C++» или «server5, добавить процессо-

ры». Когда лист будет заполнен, повесьте его на стену и перейдите к следующему.

Не отклоняйте никакие требования и не отговаривайтесь от них. Просто записывайте, что говорят люди. Чтобы получить лучшие ответы, люди должны чувствовать себя комфортно. Люди не будут чувствовать себя комфортно – и перестанут говорить, – если на каждое их предложение вы будете приводить причину, почему это невозможно или слишком дорого. Однако ясно дайте понять, что запись идеи не гарантирует ее реализацию.

Остерегайтесь позволить одному слишком активному человеку перетянуть на себя весь разговор. Если это произошло, вам может потребоваться использовать такие фразы, как «Давайте послушаем тех, кто еще не высказался». В крайнем случае вы можете пройти по комнате и по очереди выслушать ответ каждого человека на вопрос, не позволяя другим перебивать его.

Не затягивайте собрание. Если вы превысили отведенное время, вежливо прервите дискуссию и переходите к следующим вопросам. У людей загруженные графики, и им нужно вернуться к работе.

4. *Обзор* (10 мин): проведите обзор того, что вы записали, прочитав это вслух. После этого просмотрите списки вместе со своим руководством, чтобы установить приоритеты задач (или отклонить их).
5. *Представление и рассказ* (30 мин): это самое интересное. Люди хотят, чтобы им было интересно, но разным людям интересны разные темы. Лучший способ заинтересовать людей технических специальностей – позволить им узнать что-то новое. Далекие от техники люди могут захотеть узнать о каком-нибудь таинственном элементе системы. Попросите разработчика предоставить какую-либо информацию о продукте, своего сотрудника – рассказать о чем-то полезном, что он делает или узнал, или обратите внимание на новую возможность вашей сети. Это может быть хорошей возможностью рассказать о предстоящем серьезном изменении либо описать сетевую топологию или какой-нибудь аспект системы, который часто не понимают ваши пользователи.
6. *Обзор собрания* (5 мин): пусть каждый по очереди кратко оценит собрание (менее чем в одном предложении). На больших собраниях может быть лучше, если люди скажут по одному слову или просто поднимут руки, если захотят что-то сказать.
7. *Закрытие* (2 мин): для начала попросите поднять руки тех, кто считает, что собрание было полезным. Напомните им, что с вами можно связаться, если они захотят зайти и обсудить вопросы в дальнейшем. Затем, и это важно, поблагодарите людей за то, что они нашли время в своем загруженном графике.

31.2.5. Информационные бюллетени

Многие крупные организации системного администрирования выпускают ежемесячный или ежеквартальный новостной бюллетень. Иногда такие бюллетени очень хороши и полезны для пользователей, но мы часто сталкиваемся с тем, что они игнорируются либо на них отвечают обвинением, что ваша группа больше занимается рекламой, чем решением проблем.

Мы считаем, что если у вас есть информационный бюллетень, то он должен быть простым и полезным: простая структура, легко читать. Содержимое должно быть интересным для целевой аудитории, например часто задаваемые вопросы или колонка «Спросите системных администраторов», в которой подробно объясняется один вопрос на выпуск.

Если вы наняли человека, который не занимается ничем другим, кроме подготовки информационного бюллетеня, то у вас нет простого информационного бюллетеня.

31.2.6. Рассылка для всех пользователей

Перед серьезными изменениями, например такими, которые могут быть реализованы во время технического перерыва (глава 20), отправляйте всем пользователям по электронной почте краткое сообщение, информирующее их об отключении и о том, какие улучшения ждут их после него. Отправка полезных массовых рассылок – это искусство. Сделайте сообщение очень кратким и содержательным. Самая важная информация должна быть в первом предложении. Дополнительная информация для тех, кто заинтересуется, должна содержаться в нескольких дополнительных кратких абзацах.

Включите в строку темы текст «ТРЕБУЕТСЯ ПРИНЯТИЕ МЕР», если требуется принять меры. Затем четко изложите эти меры в сообщении и объясните, что случится, если они не будут приняты.

Например, хорошее сообщение для массовой рассылки о техническом обслуживании системы может выглядеть следующим образом:

> Тема: Отключение службы печати в зданиях 1 и 2 В СУББОТУ УТРОМ
>
> Служба печати в зданиях 1 и 2 не будет работать в субботу, 24 июня, с 8 до 11 часов из-за технического обслуживания системы.
>
> Если в связи с этим у вас возникнут проблемы, пожалуйста, сообщите об этом Джону Смиту по добавочному номеру 54321 в кратчайшие сроки.
>
> Срок эксплуатации серверов печати в этих зданиях подходит к концу, и мы полагаем, что через несколько месяцев они станут менее надежными. В настоящее время мы заменяем их на новое оборудование, чтобы избежать проблем с надежностью в будущем. Если у вас возникнут вопросы, пожалуйста, свяжитесь с нами по адресу print-team@company.com.

Более многословное сообщение (традиционное письмо), напротив, менее полезно. Например, следующее сообщение не доводит важную информацию быстро:

> Дорогие пользователи!
>
> Чтобы улучшить обслуживание, группа системного администрирования отслеживает все компоненты системы. Мы прилагаем усилия для предупреждения проблем и их устранения до того, как они возникнут. Для этого нам нужно время от времени планировать отключение некоторых компонентов системы, чтобы выполнять техническое обслуживание. Мы делаем все возможное, чтобы запланировать технический перерыв на время, которое не позволит негативно затронуть никакую срочную работу в других частях компании.
>
> Мы обнаружили потенциальную проблему с серверами печати в зданиях 1 и 2. Мы предполагаем, что эти серверы печати через несколько месяцев станут менее надежными и будут вызывать в этих зданиях проблемы с печатью. Из-за этого в субботу, 24 июня, с 8 до 11 часов утра мы запланировали заменить эти серверы на новые, надежные машины. В это время вы не сможете пользоваться службой печати в зданиях 1 и 2.

> Если время этого технического перерыва будет пересекаться с какой-либо срочной работой, пожалуйста, сообщите нам об этом в кратчайшие сроки и мы перенесем его на другое время. По вопросам планирования можно связаться с Джоном Смитом, добавочный номер 54321.
>
> Как и всегда, мы рады ответить на любые вопросы об этом мероприятии, которые могут у вас возникнуть. Вопросы можно задать непосредственно людям, работающим над этим проектом, отправив сообщение по адресу print-team@company.com, как обычно. Все остальные вопросы можно задавать по адресу helpdesk@company.com, как обычно.
>
> Спасибо за ваше сотрудничество с нашей программой регулярного техобслуживания.
>
> Группа системного администрирования

В таком сообщении всегда должно быть указано два способа связи с системными администраторами: чтобы задать вопросы или на случай, если у кого-то есть проблема из-за объявленного мероприятия. Очень важно, чтобы эта контактная информация была точной. Мы сталкивались с большим количеством жалоб от людей, которые получали такое сообщение, но в силу различных причин не смогли связаться с адресатом. Важно, чтобы указанные контакты были двумя разными средствами связи (электронная почта и телефон, факс и телефон и т. д.), а не просто, например, два адреса электронной почты. Убедитесь, что вы не говорите людям: «Если ваша электронная почта не работает, пожалуйста, отправьте в нашу службу поддержки сообщение по электронной почте, чтобы вашу проблему устранили».

Массовая рассылка должна использоваться только время от времени и для важных изменений. Слишком большое количество сообщений массовой рассылки или слишком многословные сообщения приводят к пустой трате времени пользователей и выглядят занудными.

Кому нужно это прочесть?

Частью культуры Google является требование, чтобы все сообщения массовой рассылки начинались с утверждения, сообщающего, кому не нужно читать нижеследующее сообщение. Вот несколько реальных примеров:

- «Если вы не пользуетесь [URL внутренней службы], вы можете не читать это сообщение».
- «Если вы не пишете код на C++ под Linux, вы можете не читать это сообщение».
- «Если вы не пользуетесь GFS или не знаете, что это такое, вы можете не читать это сообщение».
- «Если в течение последних 12 месяцев у вас не было дня рождения, вы можете не читать это сообщение».

Рекламируйте услуги в неожиданных местах

Лес Ллойд (Les Lloyd) в колледже Роллинз использует подпись в сообщениях электронной почты для объявления о новых возможностях, ближайших занятиях и основных запланированных отключениях.

31.2.7. Обеденный перерыв

Проводить свой обеденный перерыв вместе с пользователями – прекрасный способ быть на виду. Обед с различными пользователями каждый день или раз в неделю – это замечательный, дружелюбный и ненавязчивый способ поддерживать связь.

Бесплатный обед

Томми Рейнгольд (Tommy Reingold) из Bell Labs просматривает серийные номера заявок на устранение неполадок. Создатель каждой 10 000-й заявки приглашается на обед. Том оплачивает обед сам из-за ценного опыта, который получает. Это простой и недорогой способ для системных администраторов приобрести репутацию веселой и интересной группы. Этот «конкурс» не афишируется, и для пользователей бывает приятной неожиданностью, когда они выигрывают приз. Забавно бывает наблюдать за тем, как люди отправляют одну-две дополнительные заявки, чтобы увеличить свои шансы на победу.

31.3. Заключение

Не оставляйте восприятие и заметность на волю случая. Активно участвуйте в управлении ими. При отсутствии управления они станут катастрофой. Когда мы осознаем эти принципы, мы быстро находим много способов улучшить их.

Восприятие – это категория качества: как люди смотрят на вас. Формирование хорошего первого впечатления – это технический вопрос, который требует значительного планирования. Создание процессов, в соответствии с которыми новые пользователи получают компьютеры и учетные записи в день выхода на работу, требует координации между многими различными подразделениями. Важно, чтобы новые пользователи получали какой-нибудь инструктаж, помогающий им освоиться в сети, а также необходимую начальную документацию.

Мы выяснили, что, называя «юзеров» «пользователями», мы изменяем свое отношение к ним. Это сосредоточивает наше внимание на том, что мы их обслуживанием. Важно уважительно относиться к вашим пользователям. Не бывает «глупых» вопросов.

Мы рассмотрели теорию массового обслуживания, принципы изменения порядка запросов, которые вы получаете, чтобы время их выполнения было согласовано с ожиданиями пользователей.

Мы рассмотрели философию «системного адвоката» в системном администрировании. Системный адвокат – это системный администратор, который проявляет инициативу в решении проблем до того, как они возникают. Переход от роли клерка к роли системного адвоката – это изменение в отношении и стиле работы, которое может значительно улучшить обслуживание, предоставляемое вами пользователям. Это нелегко, это требует усердной работы и затрат времени сейчас для получения отдачи в будущем.

Заметность – это категория количества: как часто люди вас видят. Мы рассмотрели много способов повышения заметности. Создание веб-страницы состояния системы позволяет вам каждый день появляться перед глазами пользователей. Встречи с руководителями помогают им понимать, что вы делаете, а вам – поддерживать максимальное внимание к их наивысшим приоритетам.

Расположение офисов каждого сотрудника вашей группы влияет на ее заметность. Люди, которые работают с пользователями, должны находиться в более посещаемых местах. Нужно проводить общие собрания и собрания групп пользователей. Информационные бюллетени часто создаются группами системного администрирования, но редко читаются пользователями. Их создание требует больших усилий, а проигнорировать их очень легко. Обед и общение с пользователями – это простой способ поддерживать взаимодействие.

Контроль над вашим восприятием и заметностью требуется для создания положительного образа вашей группы и лично вас. Умелое управление этими аспектами повышает вашу способность эффективной работы с пользователями, расширяет ваши возможности по лучшему обслуживанию пользователей и имеет значительный потенциал для развития вашей карьеры.

Задания

1. Какое первое впечатление вы производите на своих новых пользователей? Является ли оно положительным или отрицательным? Что вы можете сделать, чтобы его улучшить?
2. Спросите трех пользователей, что они помнят о том, как общались с вашей группой системного администрирования впервые. Что нового вы узнали из этого?
3. Кто инструктирует новых сотрудников в первый день работы в вашей организации?
4. Используют ли сотрудники вашей группы слово «юзер» или «пользователь»? Какое поведение вы показываете личным примером другим?
5. С кем и где вы говорите, когда вам нужно пожаловаться на пользователя?
6. Выберите десять типичных запросов пользователей и оцените их ожидания относительно сроков выполнения. Опросите трех пользователей об их ожиданиях. Как вы справились со своей задачей? Что нового вы узнали?
7. Как ваша организационная структура содействует или препятствует попыткам соответствовать ожиданиям пользователей по времени выполнения запросов? Как это можно улучшить? Что делаете в этом направлении лично вы и что вы можете сделать, чтобы улучшить ситуацию?
8. Каков ваш уровень по шкале от одного (клерк) до семи баллов (адвокат)? Почему? Как вы определили свою оценку? Какие меры вы можете принять для движения в сторону адвоката?
9. Сталкиваетесь ли вы с парадоксом заметности системного администратора, рассмотренным в разделе 31.2? Приведите несколько примеров. Что вы можете сделать, чтобы переломить ситуацию?
10. Какой из следующих проектов имел бы наибольшее положительное влияние на заметность вашей организации: веб-страница состояния системы, регулярные встречи с основными руководителями, реорганизация место-

положения вашего офиса и офисов вашей группы, общие собрания, собрания пользователей, информационный бюллетень или периодические обеды с вашими пользователями?

11. Выпускает ли ваша группа информационный бюллетень для пользователей? Спросите пятерых пользователей, читают ли они его, и если да, что полезного они там находят. Что нового вы узнали?
12. Кто в вашей группе лучше всего подготовлен для проведения общего собрания?
13. Обсудите со своим руководителем следующий вопрос: что требует большего развития, ваше восприятие или ваша заметность? А как насчет вашей группы?

Глава 32

Быть счастливым

Эта глава – о том, как быть счастливым системным администратором. Разные люди понимают счастье по-разному. Счастливый системный администратор хорошо справляется со стрессом и бесконечным потоком нагрузки, с радостью ходит на работу каждый день и имеет хорошие отношения с пользователями, коллегами и руководителями. Счастье – это ощущение достаточного контроля над своей трудовой жизнью и хорошая общественная и семейная жизнь. Оно предполагает чувство выполнения чего-то и получение удовлетворения от своей работы. Оно предполагает хорошие отношения с вашими коллегами и вышестоящим руководством.

Так как счастье каждый понимает по-своему, различные методы из данной главы для некоторых читателей могут подходить лучше, чем для других. Мы постарались отразить главным образом то, что работало для нас. Например, из сотен книг по планированию времени мы попытались выбрать 10% таких работ, которые применимы для ситуаций, с которыми сталкиваются системные администраторы. Если вы считаете, что книги по управлению временем на 90% являются мусором, мы надеемся, что здесь упомянули оставшиеся 10%.

Счастливых системных администраторов, которых мы встречали, объединяют определенные привычки: хорошие профессиональные навыки, хорошие навыки общения, психология личности и методы управления их руководителями. Мы употребили слово «*привычки*», поскольку имели в виду то, что люди делают неосознанно, как, например, постукивают пальцами, когда слышат песню по радио.

Некоторые люди от природы владеют этими чертами, но другим этому надо учиться. Эти методы можно изучить при помощи книг, лекций, занятий, конференций и даже тренировочных лагерей. Достаточно удивительно, что счастье создается набором навыков, которые можно развить при помощи тренировки! Нелегко сделать какой-то подход привычкой. Не ждите мгновенного успеха. Если вы будете пытаться еще и еще, это будет становиться проще и проще. Общее практическое правило – привычка может сформироваться, если вы ведете себя так в течение месяца. Начните сегодня.

Задача данной главы – показать вам эти приемы и навыки, а затем указать ресурсы для более полного ознакомления с данной темой.

32.1. Основы

Основы включают организованность и возможность правильно общаться. Доведение до конца – важная задача, она обеспечивается организованностью и требует хорошего планирования времени. Профессиональное развитие также

важно. Эти базовые навыки являются основой, на которой вы можете построить успешную карьеру.

32.1.1. Доведение до конца

Доведение до конца означает завершение того, что вам поручено сделать. Счастливые системные администраторы поддерживают организованность при помощи письменных или электронных записных книжек либо КПК, в которых записаны их списки дел и календари встреч. Организация – важный этап в обеспечении доведения работы до конца. Ничто не раздражает пользователей больше, чем проигнорированные запросы или встречи. Вы будете счастливее, если разовьете к себе уважение, основанное на репутации человека, безупречно доводящего работу до конца. Это одна из причин, по которым во всей книге мы уделяем так много внимания использованию программ для отслеживания заявок. Такие программы дают нам уверенность, что обещания не были забыты.

В вашем мозге есть только ограниченное пространство для хранения информации, поэтому не перегружайте его тем, что лучше записать в свою записную книжку. По слухам, Альберт Эйнштейн так беспокоился о том, чтобы обеспечить 100-процентное использование своего мозга для физики, что он не «тратил» его на такие глупые вещи, как выбор одежды, – у него было семь костюмов, все одинаковые, по одному на каждый день недели, – или свой домашний адрес и телефон – он записывал их на карточке в своем кошельке. Когда люди спрашивали у него его телефон, он советовал им посмотреть его в справочнике. Он его не помнил.

Ваша память несовершенна. Ваша записная книжка, напротив, не может случайно упустить действие или перепутать две встречи. У вас должна быть одна записная книжка, чтобы вся эта информация была в одном месте. Это лучше, чем иметь миллион бумажек, приклеенных к монитору. Объедините свои рабочий и общий календари, чтобы не возникало конфликтов. Вы бы не хотели пропустить важный день рождения, юбилей или встречу с пользователем. Поддерживать различные календари дома и на работе – значит нарываться на неприятности. Их синхронизация нарушится.

Комбинированная записная книжка должна включать ваши личные события, юбилеи, приемы врача, списки дел, не связанных с работой, и напоминания о регулярных событиях, например даты вашего следующего ежегодного медосмотра и очередного техосмотра вашей машины. Пользуйтесь своей записной книжкой для напоминания о регулярных, повторяющихся событиях. Включите напоминания о том, чтобы делать перерывы, делать что-то приятное для себя и близких вам людей. Используйте свою записную книжку для записи названий фильмов, которые вы хотите посмотреть, чтобы в следующий раз, когда вы зайдете в салон видеопроката, вам не приходилось раздраженно вспоминать тот классный фильм, который рекомендовали коллеги. Ничто из этого не должно быть упущено в куче бумажек, приклеенных к вашему столу или в вашем беспорядочном и несовершенном мозге.

Пример: динамические списки задач

Пытаясь достичь идеального доведения до конца, Том составляет 365 списков задач в год. Он заканчивает каждый день, переписывая невыполненные задачи из сегодняшнего списка в завтрашний. На завтрашней стра-

нице уже были задачи, которые он ранее назначил на этот день. Если день перегружен, то Том может переписать незавершенные задачи даже еще дальше на будущее.

Утром он читает сегодняшний список и отмечает каждую задачу, которую обязательно нужно выполнить сегодня. Сначала он работает над этими задачами. После того как они будут выполнены и вычеркнуты, он работает над остатком списка. Раньше он думал, что системному администратору невозможно устанавливать приоритеты, теперь он может делать это каждое утро.

При появлении новой задачи он записывает ее на первый день, когда сможет над ней работать. Обычно это сегодняшний список, но иногда он может быть через несколько дней или даже месяцев. Раньше он думал, что системный администратор не способен планировать так далеко вперед, теперь он может планировать работу, а не ощущать постоянное беспокойное желание сделать ее прямо сейчас или пока не забудет.

Перед окончанием рабочего дня он может посмотреть, что не было выполнено. Если оказывается, что он не укладывается в срок, который обещал пользователю, он может позвать этого человека, чтобы узнать, сможет ли задача подождать до следующего утра или она настолько важна, что ему нужно задержаться и поработать над ней. Раньше он всегда чувствовал давление, которое вынуждало его задерживаться допоздна каждый вечер, или вину за каждое несоблюдение срока. Теперь он может позвать людей и изменить сроки.

В конце дня необходимость переписывать невыполненные задачи дает ему стимул не допускать их затягивания, так как в этом случае ему придется чаще их переписывать. В конце дня он так или иначе обрабатывает каждую запись. Задача либо выполнена и вычеркивается, либо перенесена на будущую дату и тоже вычеркивается. Он чувствует выполнение работы и завершение, потому что «справился» с каждой задачей. Раньше чувства завершения не было, потому что каждый день он оставлял работу с чувством, что работе не было видно конца, поскольку у него было так много незавершенных задач. Теперь он может лучше спать, зная, что сделал важные дела, а об остальных не стоит беспокоиться до утра.

При написании ежемесячных или ежегодных отчетов он пользуется выполненными списками задач для справки, а не пытается с трудом вспомнить, что он сделал.

Существуют программы, КПК и даже веб-порталы, которые автоматизируют этот процесс. Однако Том предпочитает пользоваться бумажной системой, потому что в ней проще делать заметки на полях и у нее нулевое время перезагрузки. Том рисует много схем, а это проще делать на бумаге. Физическая папка, которой он пользуется, достаточно велика, чтобы вмещать ручки и листы бумаги, которые всегда удобно иметь при себе.

Наличие системы любого типа лучше, чем полное ее отсутствие. Мы так сильно в это верим, что призываем работодателей оплачивать сотрудникам КПК или старомодные бумажные записные книжки, даже если они используются как

для личной, так и для рабочей информации. Нам все равно, какой системой вы пользуетесь, нас беспокоит лишь то, чтобы вы пользовались хоть какой-нибудь системой.

После некоторого времени пользования записной книжкой вы обнаружите, что можете лучше сосредотачиваться и концентрироваться. Вы сможете лучше сосредоточиться на том, что делаете, когда вы не пытаетесь одновременно помнить, что вам нужно делать потом, на следующей неделе, и будет ли встреча с пользователем в следующую среду или через среду. Вы можете как бы намеренно забывать то, что записали в свою записную книжку. Каждое утро вы можете просматривать сегодняшние задачи и определять основные приоритеты на день. Пусть ваша записная книжка работает за вас, не дублируйте ее работу.

32.1.2. Управление временем

Управление временем предполагает его разумное использование. Вместо того чтобы повышать производительность, работая больше времени, вы можете сделать больше за то же время при помощи нескольких приемов и небольшого планирования.

Работайте умнее, а не больше. Пользователи не видят, насколько усердно вы работаете. Они видят, что вы можете выполнить. Смиритесь с этим аспектом действительности. Усердно работать могут все, и мы уверены, что на это способны все читатели данной книги. Успешные системные администраторы уделяют основное внимание достигнутым результатам, а не затраченным усилиям.

32.1.2.1. Сложность управления временем

Управление временем очень сложно для системных администраторов, потому что работа системного администратора обычно сопряжена с прерываниями. Люди или какие-то внешние события прерывают вашу работу своими запросами. Поэтому, вместо того чтобы работать над своими задачами высокого приоритета, вы проводите время, отвечая на запросы других людей, которые основаны на их приоритетах. Представьте себе, как вы вели бы автобус из Нью-Джерси в Сан-Франциско, если бы останавливались каждый раз, когда пассажир вас об этом просит. Вы бы могли вообще не достичь пункта назначения! Несмотря на то что остановки в этих местах могут быть интересны, вашей задачей было доставить автобус и пассажиров в Сан-Франциско. Критический шаг к хорошему планированию времени системных администраторов – разорвать этот круг.

Как было рассмотрено в разделе 31.1.3, вы можете разделить свой рабочий день, например, работая над проектами в первую половину дня и отвечая на заявки во вторую. Если пользователи будут знать, что у вас такой рабочий процесс, они будут учитывать это и беспокоить вас утром только в экстренных случаях. Если они не знают об этом, вы можете вежливо записать их запросы и сказать им, что разберетесь с ними после обеда. В качестве альтернативы вы можете договориться с коллегой, чтобы кто-то всегда заботился о прерываниях. Либо вы можете просто приходить очень рано утром, когда другие еще не пришли и не могут вас прервать.

Когда вас прерывают, вы можете отклонить прерывание, записав запрос в свой личный список задач и сказав человеку, что вы вернетесь к просьбе позже. Иногда у вас может не быть возможности записать запрос. Например, вы идете

по коридору, когда Синди Лу обращается к вам со своей просьбой. В данном случае лучше всего может быть прямо сказать: «Я не запомню вашу просьбу, потому что не могу сейчас ее записать. Не могли бы вы написать мне по электронной почте?» Люди оценят честность, если вы не будете выглядеть грубым или возмущенным. В такой ситуации очень легко показаться грубым, поэтому мы рекомендуем вам быть особенно любезным. Если для управления вашим списком задач используется система заявок, например аналогичная рассмотренным в разделе 13.1.10, может быть эффективно попросить человека подать заявку. Это обучает пользователей применять каналы, которые были созданы специально для них. Возможно, имеет смысл показать пользователям, что вы воспринимаете их всерьез, выслушав их и затем конкретно объяснив, как подать заявку в системе заявок. Вы можете сказать: «Не могли бы вы создать заявку, в которой указано: “Исправьте проблему DNS на сервере 5; Джон[1] знает, что я имею в виду”». Пользователь оценит отсутствие необходимости тратить много времени на создание сообщения. Ключ к эффективному отклонению – не казаться грубым и помогать пользователю получить помощь.

32.1.2.2. Определение целей

Распространенная проблема – чувствовать, что вы буксуете, усердно работая месяц за месяцем, но не получая никаких результатов. Вы тратите так много усилий, вытирая пол, что у вас нет времени устранить течь. Вы можете разорвать этот круг, только изменив свое поведение. Мы предлагаем *определение целей*. Уделите немного времени определению целей на следующий месяц. Запишите все, что придет в голову, в любом порядке. Затем установите приоритеты и уберите задачи с низким приоритетом. Запланируйте, какие элементарные меры требуются для выполнения оставшихся целей. Определите приоритеты задач, которые приблизят вас к этим целям, и прекратите делать то, что вас к ним не приблизит.

Планирование на год вперед может показаться фантастикой, особенно если вы работаете в среде, где все быстро меняется. Вы можете полагать, что в начинающей компании неразумно планировать больше чем на 6 месяцев вперед, но не вынуждайте себя иметь только жесткие «деловые» цели. Даже в начинающей компании, где квартальные цели неточны, у вас могут быть долгосрочные цели: исправить или заменить четыре наименее надежных сервера, чаще приходить на встречи вовремя, выполнять в срок месячные планы, заставить себя тратить на себя время, получить повышение, накопить на первоначальный взнос за дом.

Один из полезных подходов – тратить час первого дня месяца, просматривая свои достижения за предыдущий месяц, чтобы оценить, насколько они вас приблизили к более крупным задачам. Затем запланируйте, что вы хотите выполнить в следующем месяце, возможно, проверив свои задачи на год. Можно начинать каждую неделю, проверяя свое состояние. Это дает эффект постоянного поддержания своих задач в мыслях. Сколько раз вы приближались к предельному сроку и думали: «Черт возьми, я не верю, что забыл над этим поработать!»? Доверьтесь процессу. Он работает.

---

[1] Только если вас зовут Джон.

32.1.2.3. Ежедневное планирование

И снова, планирование – это ключ к успешному управлению временем. Вы должны начинать каждый рабочий день, просматривая свой список задач, устанавливая их приоритеты и встраивая их в график рабочего дня. Такое вложение пяти минут времени имеет огромную отдачу.

Пример: все объединить

Если говорить о работе рано утром, Том считает, что за первый час рабочего дня он может сделать больше, чем за весь остальной день вместе взятый, потому что его не прерывают. Люди не прерывают его, потому что они еще не пришли на работу или слишком заняты проверкой своей почты, подготовкой к работе и т. д. Раньше он проводил свой первый час, читая электронную почту и посещая различные веб-сайты (Adams 2000). Однако как-то раз он понял, что было бы лучше тратить этот самый продуктивный час на что-нибудь более сто́ящее. Теперь он начинает с проверки системы мониторинга на любые экстренные предупреждения, а затем просматривает в своем почтовом ящике сообщения, отмеченные как «срочные», не поддаваясь соблазну прочитать все остальные[1]. Он тратит пять минут на планирование своего рабочего дня: сначала он просматривает, редактирует и устанавливает приоритет своих задач, возможно, переводя некоторые из них на завтра, если на них не будет времени. Затем он составляет график на день с точностью до одного часа. Он выделяет время на встречи, на которые он должен прийти, и пару часов на задачи по запросам. Остальное время он распределяет на свои проекты с наивысшим приоритетом. Остаток первого часа тратится на работу над одной задачей с самым высоким приоритетом. Он даже не отвечает на телефонные звонки. Этот первый час обеспечивает то, что самому важному проекту каждый день уделяется по крайней мере небольшое внимание. Самый продуктивный час тратится на самые важные задачи. Он не делает это каждый день, но он всегда старается успеть это выполнить. Когда он пропускает этот шаг, важные задачи забываются, встречи пропускаются, а графики сдвигаются.

Может быть, вам и не стоит разбивать свой день по часам. Возможно, для вас будет удобнее разбивка по полчаса, или, наоборот, такой вариант окажется еще хуже. Может быть, для вас лучше разбивка по полдня. Поэкспериментируйте немного и решите, что работает лучше.

Несмотря на то что первый час рабочего дня может быть очень продуктивным из-за отсутствия прерываний, вы, возможно, найдете другое время, которое будет особенно продуктивным из-за ваших биологических часов. У некоторых людей наиболее продуктивное время бывает в середине дня, или в 6 ч вечера,

[1] На самом деле его системы мониторинга и электронной почты отправляют срочные сообщения ему на пейджер, поэтому он может полностью исключить этот этап.

или даже в 2 ч ночи. Для этого не существует никаких объективных причин или общих ритмов, это просто физиологические особенности людей. Вне зависимости от того, каким это время будет у вас, планируйте ваш график на его основе. Назначайте на этот час работу, которая требует больше всего мыслей, внимания к деталям или энергии. Возможно, у вас и не получится сходу определить ваш наиболее продуктивный час. Кроме того, он может изменяться с возрастом, примерно так же, как с возрастом меняется ваше время сна. Единственный способ найти свои пики производительности – это успокоиться и внимательно прислушиваться к своему организму.

После прочтения предыдущего примера вы, скорее всего, подумали, что Том – «жаворонок». Удивительно, но это не так. Начало дня с работы над графиком пробуждает в нем видение того, что ему нужно сделать в этот день. Он считает первый час таким продуктивным из-за отсутствия прерываний, а не потому, что его биологические часы определяют утро как наилучшее время для работы. Его пиковый час – 7 ч вечера, особенно если в 5 ч вечера он поужинал.

32.1.2.4. Обрабатывайте документы один раз

В книгах по управлению временем также рекомендуется несколько других приемов, которые заслуживают повторения здесь, потому что они полезны для системных администраторов. Один из таких приемов – «касаться каждого листа бумаги только один раз». Полностью обрабатывайте всю корреспонденцию, а не сортируйте ее по группам для дальнейшей обработки. Когда вы берете в руки бумагу, изучите ее и решите, нужно ли вам выбросить ее, не читая, прочитать и выбросить, исполнить и выбросить, ответить на нее и выбросить или подшить в папку. Иногда исполнение документа означает его запись в ваш список задач. В других случаях вы можете записать свой ответ на полях и отправить письмо обратно тому, кто его прислал. Наихудшее, что вы можете сделать, – прочитать документ, а затем положить его в кучу, чтобы исполнить потом: это означает, что вам придется прочитать его дважды, что является пустой тратой времени. Помните: все, что вы подшиваете, создает вам дополнительную работу, когда нужно очищать папки, или делает усилия по поддержанию порядка в папке более значительными. Подшивайте минимум документов. Если сомневаетесь, выбрасывайте[1]. Если документ был действительно важным и позднее окажется, что он вам нужен, вы можете связаться с отправителем и получить его копию.

К электронной почте можно относиться так же. Если вы читаете каждое сообщение, а потом сохраняете его для дальнейшей обработки, фактически вы удваиваете объем обрабатываемой вами электронной почты. Вместо этого прочти-

[1] Люди, которые не являются системными администраторами, могут класть такие документы в папку «Выбросить через 30 дней», которая очищается раз в месяц. Однако обычно мы видим, что системные администраторы не получают важную информацию на бумаге. Системные администраторы получают важную информацию в электронном виде. Бумажные записки, которые получают системные администраторы, обычно создаются нетехническими сотрудниками компании, которым нужно только раздражать нас бесполезной информацией, например тем, что из-за ремонта в туалете на втором этаже нужно пользоваться туалетом на третьем этаже. Мы считаем, что системные администраторы, которые читают эту книгу, достаточно умны, чтобы пойти на третий этаж самостоятельно, когда они увидят, что туалеты на втором этаже ремонтируются.

те и удалите сообщение, сохраните его, скопируйте его в вашу систему списка задач и удалите оригинал или перешлите письмо кому-то еще и удалите оригинал. Если вы никогда не удаляете сообщения, потому что боитесь, что когда-нибудь они могут вам понадобиться, настройте свою систему так, чтобы она копировала каждое полученное вами сообщение в папку «Архив». Тогда вы не будете бояться удалять сообщения, потому что знаете, что всегда можете обратиться к архиву. Этот архив может обновляться, как файлы логов, сохраняя сообщения только за последние несколько месяцев для экономии дискового пространства.

Использовать автоматизированную систему, которая будет делать все это за вас, даже лучше, чем выполнять это самому. UNIX-системы имеют нескольких отличных средств обработки электронной почты, например, procmail (van den Berg 1990). Том руководствуется принципом: «Если вы не пользуетесь procmail, вы работаете слишком много». Такие системы, как procmail, позволяют вам устанавливать фильтры для предварительной сортировки своей электронной почты по различным критериям. У Тома есть папка для каждого списка рассылки, на который он подписан, и он использует procmail для фильтрации сообщений из рассылок в соответствующие папки. Это поддерживает его почтовый ящик относительно чистым. Если у него нет времени читать тот или иной список рассылки целую неделю, он просто удаляет содержимое папки: если бы там были сенсационные новости, он бы услышал их где-нибудь еще или сам увидел бы метеорит, падающий с неба. Кроме того, у фильтров есть возможность вызывать другие программы: procmail отсылает копию сообщения Тому на пейджер, если оно отправлено его начальником либо имеет слово «срочно» в названии темы или «обед» в тексте. Это обеспечивает немедленное внимание к трем его наивысшим приоритетам, при этом ему не нужно постоянно проверять новую электронную почту.

Том также пользуется фильтрами для сохранения всей входящей почты в папку, названную по текущим году и месяцу. В первый день каждого месяца запускается задача хрона, которая сжимает архивы старше трех месяцев. Время от времени он записывает эти архивы на CD и удаляет все архивы старше одного года. Это уравновешивает необходимость постоянного хранения и желание не тратить дисковое пространство зря.

Системы, архивирующие всю электронную почту

Служба gmail компании Google сохраняет все сообщения электронной почты по умолчанию и предоставляет прекрасные возможности поиска. Вместо того чтобы тратить время на удаление или сохранение сообщений, можно при необходимости просто искать сообщения в архиве.

32.1.2.5. Сохранение сосредоточенности

В книгах по управлению временем много говорится о том, как сохранять сосредоточенность. Общий принцип заключается в том, что беспорядок на рабочем столе создает много отвлекающих факторов, из-за которых мозгу становится труднее сосредоточиться. Распространение этого принципа на пользователей компьютеров означает также поддержание порядка в ящике электронной поч-

ты и на рабочем столе графического интерфейса. Чем больше значков на экране, тем выше риск отвлечься на что-то. Виртуальные экраны могут очень помочь сохранять концентрацию внимания, если отображают только ту информацию, на которой вы хотите сосредоточиться. Это может показать радикальной мерой, но вы также можете отключить любые системы, которые сообщают вам о получении новых сообщений, и вместо этого выделять каждый день несколько минут на чтение электронной почты. Электронная почта может стать одним из прерываний, которые не позволяют вам выполнять свою работу.

32.1.2.6. Ежедневные задачи

Если что-то нужно сделать сегодня, сделайте это в первую очередь. Это обеспечит выполнение задачи. Если есть задачи, которые вам нужно повторять *каждый* день, запланируйте их на начало рабочего дня.

Пример: эффективно планируйте ежедневные задачи

Раньше Тому приходилось каждый день менять ленты для резервного копирования. Это занимало около 15 мин, если все проходило нормально, и час, если нет. Его план, который, однако, не был эффективным, заключался в том, чтобы начать замену лент в 17:30 и успеть закончить ее к 18:00 – концу рабочего дня. Если он начинал в 17:30, но работа занимала только 15 мин, он тратил оставшиеся 15 мин впустую, потому что не хотел начинать новый проект прямо перед уходом. Так пропадало больше часа в неделю. Если он сильно увлекался работой над проектом и переставал следить за временем, оказывалось, что он начинал менять ленты, когда уже опаздывал туда, куда собирался после работы. Он опаздывал, был раздражен из-за этого и сердился, когда ему нужно было заменять ленты, потому что теперь он опаздывал еще сильнее, и приходил туда, куда собирался после работы, раздраженным и несчастным. Он пытался заменять ленты с самого утра, но это противоречило его стратегии тратить первый час на наиболее важные задачи. Наконец он остановился на замене лент сразу после обеда. Это работало хорошо и стало чем-то вроде ритуала, который возвращал его в рабочее состояние. Если что-то нужно делать каждый день, не назначайте это на конец дня.

32.1.2.7. Заблаговременное принятие решений

Эффективнее принять решение один раз, а не делать это снова и снова. Вот почему компилируемые языки обычно быстрее, чем интерпретируемые. Подумайте о том, что делает оптимизатор компилятора: он тратит немного дополнительного времени сейчас, чтобы сэкономить время в будущем. Например, если переменная складывается с константой, оптимизатор исключит это вычисление, если определит, что константа равна нулю. Интерпретатор, напротив, не может выполнять такую оптимизацию, потому что проверять перед каждым сложением, равна ли константа нулю, будет дольше, чем просто выполнить это сложение. Вы можете принимать решения заблаговременно аналогичным образом. Решите что-то сделать один раз и придерживайтесь этого принципа. Когда вы нарушаете свою старую привычку, ваш мозг может попытаться начать принимать

решение с нуля. В таком случае отвлеките его, заменив эти мысли установками, которые отражают ваши заранее определенные решения. Вот несколько установок, которые работали для нас.

- *Любое время подходит для сохранения работы.* За то время, пока вы думаете, является ли данный момент подходящим для сохранения работы, вы могли бы нажать клавиши, чтобы уже сделать это.
- *Всегда делайте резервные копии.* Всегда делайте резервную копию файла перед внесением изменения. Часто некоторые думают, что изменение настолько незначительно, что его можно будет потом исправить обратно вручную. Затем оказывается, что человек вносит значительное изменение. Лучше решить всегда делать резервные копии, чем тратить время на размышления, делать их или нет.
- *Записывайте запросы.* Вместо того чтобы пытаться запомнить запрос, запишите его: занесите его в КПК, подайте заявку в службу поддержки, напишите ее на руке. Любая запись лучше, чем пытаться что-то запомнить. Однако мы часто ловим себя на мысли: «Это настолько важно, что я не смогу об этом забыть». На самом деле, если это настолько важно, для этого стоит создать заявку.
- *Заменяйте ленты по понедельникам, средам и пятницам.* В разделе 26.1.6 мы рассматривали систему резервного копирования, в которой каждый день требовалось долго разбираться, чтобы решить, нужно ли менять ленты. Вместо этого было принято решение, что время ценнее, чем пустые ленты, и ленты просто заменялись, даже если в этом не было необходимости.
- *Возьмите КПК.* Том всегда пытался решить, нужно ли ему брать свой КПК с собой. Очевидно, что его надо было брать с собой на встречи, но нужен ли он был ему во время работы в офисе пользователя? Он обнаружил, что каждый раз, выходя из своего офиса, он задерживался, чтобы решить, потребуется ли ему КПК. Если он не брал КПК, но потом тот был ему нужен, ему приходилось записывать на клочках бумаги, которые неизбежно терялись. Кроме того, он терял КПК и всегда находил его потом в каком-нибудь офисе, в который он заходил, чтобы помочь пользователю. Когда он уходил домой вечером, он задерживался, чтобы решить, брать ли КПК с собой. Если он оставлял КПК в офисе, неизбежно оказывалось, что тот требовался ему дома. Если он брал КПК домой, на следующее утро он часто забывал его дома, потому что не помнил, взял ли он его домой предыдущим вечером. Решением всех этих проблем стало предварительное определение: «Том всегда будет брать КПК с собой, куда бы он ни пошел». В результате КПК всегда был у него, когда был нужен, вне зависимости от того, находился ли он дома или в офисе. Ему никогда не приходилось записывать на клочках бумаги. КПК никогда не оставался дома, потому что, когда Том уходил на работу, он знал, что нужно взять КПК с собой. Он больше не терял КПК, потому что у него вошло в привычку проверять, что он взял КПК, когда выходил из комнаты. Он стал более сосредоточенным, потому что его мозгу не требовалось отвлекаться на принятие отвлекающего решения, когда он начинал работу. Он экономил время, потому что не тратил его на постоянное принятие одного и того же решения.
- *Лучше раньше, чем позже.* Наш последний пример помогает предотвратить затягивание. Для небольших задач мы предлагаем использовать принцип «лучше раньше, чем позже». Например, Том часто откладывал небольшие

задачи, потому что, если задача была небольшая, он мог выполнить ее «в любое время». Однако «любое время» редко наступало. Например, когда он ехал поздно вечером домой, он мог заметить, что в его машине кончается бензин. Он мог бы решить, что может заправиться следующим утром по дороге на работу, особенно если не забудет выехать чуть пораньше. Как нарочно, на следующий день он рисковал опоздать и необходимость заправиться вынудила бы его опоздать еще больше. После принятия этой установки он стал заправляться вечером, когда обнаруживал, что в машине кончается бензин.

В жизни системного администратора есть много подобных ситуаций: сделать заказ сейчас, позвонить сейчас, начать процесс сейчас и т. д. Когда вы начинаете размышлять, подходящее ли сейчас время для выполнения этих задач, напомните себе, что «лучше раньше, чем позже».

Такие заблаговременные решения хорошо работают у нас. Вам надо уделить время тому, чтобы определить, какие решения вы принимаете постоянно, и выбрать одно или два для предварительного определения. Вы потеряете немного гибкости, но получите множество других преимуществ. Установки, которые вы разработаете, будут зависеть от вашего стиля жизни, манеры одеваться и, возможно, даже пола. Одной женщине было трудно всегда носить с собой записную книжку из-за стиля одежды. Вместо этого она всегда носила в сумочке один лист бумаги, на котором делала записи. Ее установка была следующей: «Когда я сяду за свой компьютер, я перенесу записи со своего листа». Подойдет все, что работает в вашей ситуации.

32.1.2.8. Нахождение свободного времени

Свободное время прячется повсюду, но, чтобы его найти, вам нужно хорошо поискать. Кроме того, вы можете создать свободное время, избавившись от бесполезной траты времени. Вот несколько простых мест, где можно поискать свободное время.

- Найдите «легкое» время в году. Компании по разработке программ, выпускающие новый продукт каждые 4 месяца, обычно имеют «период отдыха» продолжительностью 3–4 недели после каждого выпуска. В этот период у вас может быть свободное время, либо, наоборот, вы можете потратить его на то, чтобы заранее подготовить все необходимое для своих клиентов, чтобы впоследствии никто из них вас не беспокоил.
- Лучше убирайте, а не автоматизируйте. Будучи системными администраторами, мы склонны накапливать объекты, а затем тратить много времени на управление того, что мы накопили. Мы думаем, что улучшили свое положение, когда находим лучшие способы управления накопленными нами бесполезными задачами, и часто забываем, что сэкономили бы еще больше времени, если бы у нас было меньше объектов для управления.
- Перестаньте читать группы новостей Usenet. Точка.
- Удалите себя из двух самых активных списков рассылки, в которые вы входите. Повторяйте это раз в месяц.
- Воспользуйтесь преимуществами программ фильтрации электронной почты, например procmail.
- Воспользуйтесь преимуществами работы рано утром: приходите на час раньше.

- Сократите время вашей дороги на работу, избегая движения в часы пик. Работайте в нестандартное время. Определите «часы активности» вашего организма и измените свой график в соответствии с ними.
- Пройдите однодневный курс управления временем или поищите какие-нибудь книги по управлению временем специально для системных администраторов.
- Уделите внимание курсам или книгам, которые позволят вам автоматизировать задачи (писать код) за меньшее время. Если вы не знаете язык Perl и команду `make`, изучите их сегодня.
- Проводите еженедельные или ежемесячные встречи со своим главным пользователем – руководителем или главой подразделения – для определения приоритетов и устранения избыточных задач.
- Наймите помощника. Помощник, работающий неполный рабочий день, чтобы выполнять некоторые рутинные (тактические) задачи, может освободить вас для более важных (стратегических) обязанностей, и это может быть замечательным способом обучать кого-то работе системного администратора. Возможные кандидаты: местный старшеклассник или студент, секретарь с техническими способностями, человек, который заменяет вас, когда вас нет, временный сотрудник на летний период или заинтересованный программист. Студенты особенно полезны, потому что не требуют большой оплаты и ищут способы получить опыт.

32.1.2.9. Как справиться с людьми, заставляющими тратить время

Иногда оказывается, что вы работаете с людьми, не владеющими хорошими навыками управления временем, и их неэффективность влияет на вашу способность выполнять свою работу. Мы рекомендуем три меры. Последняя является крайней.

1. Обучайте этих людей. Помогите им увидеть, что не так в их процессах, и призывайте их обращаться за помощью. Делайте это тактично. Люди не любят, когда им говорят, что они неправы; направляйте их так, чтобы они поняли это сами. Спросите, можете ли вы как-нибудь им помочь сделать что-то быстрее.
2. Работайте с их руководством.
3. Если первые две меры невозможны – например, вы работаете с этим человеком лишь недолгое время или человек работает в другой части вашей компании (либо в другой компании!) и его обучение было бы неприемлемым и дерзким, – найдите способ управлять его временем. Это крайняя мера. Например, ваш проект задерживается из-за того, что вы ждете, пока что-то не будет выполнено кем-то еще. Этот человек никогда не выполнит ваших запросов, потому что его работа полна прерываниями. В этом случае убедитесь, что вы являетесь прерыванием самого высокого приоритета. Если нужно, стойте в его офисе, пока ваш запрос не будет выполнен. Как ни странно, но именно это вы *не* должны позволять никому делать по отношению к себе. Однако очевидно, что человек, с которым вы работаете в данной ситуации, не читал эту главу. Не позволяйте кому-то, погрязшему в плохом управлении временем, утянуть с собой вас (если вы заметили, что люди начали применять этот подход к вам, возможно, вам нужно перечитать всю эту главу).

32.1.2.10. Как справиться с медлительными бюрократами

Есть множество способов справиться с медлительными бюрократами. Мы бы хотели указать два наших любимых. Первый метод – подружиться с ними. Обычно эти люди имеют дело с бесконечным потоком безликих людей, которые рассержены и нетерпеливы. Станьте одним из приятных людей, с которыми они сегодня поговорили. Принесите им приятную перемену, показав себя как противоположность последних десяти человек, с которыми они работали. Тогда они будут работать для вас более охотно. Поговорите с ними о том, что им интересно, хотя для вас это может быть совершенно скучным. Разговаривайте так, как будто вы всегда были друзьями, но будьте искренни. Спросите их, как проходит их день, и выразите сочувствие, когда они скажут вам, как они перегружены. В разговоре по телефону спросите у них о погоде. Чтобы действительно раскрыть их лучшую сторону, спросите что-нибудь вроде «Что вы думаете о последнем решении нашего генерального директора/президента?». Несмотря на то что это может показаться пустой тратой времени, которая замедляет вашу деятельность, это вложение окупится лучшим обслуживанием.

Другой наш прием хорошо работает, когда постоянно приходится иметь дело с одним и тем же человеком. Когда бюрократ говорит нам, что выполнение запроса займет несколько недель, мы часто отступаем и сокращаем количество подаваемых запросов, чтобы не перегружать его. Это просто задерживает наши проекты. Вместо этого делайте все наоборот: давайте человеку сразу сотни запросов. Часто крупные запросы, требующие уйму времени для выполнения, передаются руководителям, у которых есть полномочия упорядочить процесс, пренебречь некоторыми формальностями или сделать особые исключения. Например, если каждый запрос требует индивидуального одобрения, руководитель сможет захотеть сгруппировать некоторые или все похожие запросы и провести их все разом. Работа бюрократов в том, чтобы поддерживать процессы, которые установили не они, и поэтому они не могут их оптимизировать. Если проблема в процессе, то какое-нибудь необычное действие выбивается из этого процесса. Тогда оно становится чем-то, что требует особого внимания бюрократа или его руководителя, и благодаря этому процесс может измениться.

32.1.2.11. Обучение

Обучение управлению временем может быть небольшим вложением со значительной отдачей. Оно очень недорого по сравнению с потенциальным ростом производительности. Многие внутренние корпоративные учебные центры проводят однодневные и двухдневные курсы по управлению временем. Воспользуйтесь этими внутренними курсами, особенно если ваше подразделение оплачивает их «внутренними», а не реальными деньгами. Большинство курсов дает десятки методов, и каждый обучаемый находит среди них различные полезные приемы для себя. Начинайте такое обучение без колебаний.

Этот раздел является лишь кратким введением в методы управления временем. Книги по работе над собой (см. Lakein 1996, Limoncelli 2005, MacKenzie 1997) могут помочь вам отработать ранее рассмотренные приемы и даже сделать гораздо большее. Когда вы хорошо управляете своим временем, вы получаете удовлетворение от чувства контроля над своим рабочим временем и ваша производительность повышается. Это делает вас более счастливым системным администратором.

32.1.3. Навыки общения

Научиться правильно общаться критически важно для того, чтобы быть счастливым и успешным в работе и в личной жизни. Все проблемы можно представить как проблемы общения. Если два человека в офисе не ладят друг с другом, они просто не взяли на себя труд научиться общению, при котором личные разногласия не становятся проблемой. Вам необязательно любить кого-то, чтобы работать с ним. Вам просто нужно умение общаться.

Даже технические проблемы являются проблемами общения: сломанный диск на сервере станет *проблемой* только в том случае, если никто не сказал, что сбой недопустим, или если заявка не была выслушана и обработана должным образом: например, чтобы вся система не выходила из строя из-за одиночных сбоев дисков, нужно было воспользоваться RAID.

Проблемы в жизни обычно принадлежат к одной из четырех категорий: мои проблемы, ваши проблемы, наши проблемы и проблемы других людей. Каждая из них решается с помощью различных наборов навыков общения.

1. *Мои проблемы:* когда у меня проблема, мне нужно обеспечить, чтобы меня услышали. Мы рассмотрим прием, называемый «я-утверждение».
2. *Ваши проблемы:* когда вы делитесь проблемой со мной, я должен убедиться, что понял вас правильно, чтобы я мог принять подходящие меры или помочь вам устранить неполадки. Мы рассмотрим прием, известный как «активное слушание».
3. *Наши проблемы:* когда у меня и у вас общая проблема, нам нужна возможность взаимодействовать друг с другом, чтобы мы могли согласовать определение проблемы и план действий. Если затем мы представим эту информацию другим людям, мы воспользуемся всеми навыками общения, описанными в этом разделе.
4. *Проблемы других людей:* когда проблемы у других людей, мне нужно быть сдержанным и не вмешиваться. Некоторые из нас тратят много времени, беспокоясь о проблемах других людей. Вместо этого мы должны сосредоточиться на своих проблемах. Навык общения, необходимый здесь, – это правило «не лезть не в свое дело».

32.1.3.1. Я–утверждение

Я-утверждение – это средство помочь вам выразить свою точку зрения, а также сообщить свои чувства. Ценность я-утверждения в том, что оно позволяет вам облегчить свою душу и побудить других сделать что-то конструктивное в отношении того, о чем вы сообщили. Вы сообщили им о проблеме, которую можно исправить. То, что происходит в результате, обычно позитивно. Когда мы раскрываем свои потребности, вселенная обычно заботится о нас.

Общая форма следующая: «Я чувствую [*эмоция*], когда вы [*действие*]». Это сообщает людям о влиянии их действий. Это гораздо эффективнее, чем просто говорить кому-то, что вам не нравится то или иное поведение.

Я-утверждение выражает мягкие эмоции – грусть или опасение, – а не жесткие эмоции – гнев. Говорят, что в основе каждой жесткой эмоции лежит мягкая эмоция. Поэтому, прежде чем выражать свое я-утверждение, выясните, какая это мягкая эмоция, и выразите *ее*. Обнаружив гнев, люди займут защитную

позицию и не пожелают услышать вас. Если люди будут слышать беспокойство или грусть, они захотят позаботиться о вас и решить вашу проблему. Вот несколько примеров я-утверждений.

- Я чувствую себя обиженным, когда вы критикуете меня лично, а не мою работу.
- Я чувствую себя недооцененным, когда вы приписываете моему начальнику работу, которую сделал я.
- Я очень счастлив, что вы выполнили проект вовремя.
- Меня раздражает, когда вы требуете надежности, но не финансируете изменения, которые я рекомендую.
- Я огорчаюсь, когда получаю жалобы от пользователей, которые говорят, что вы не выполняете своих обещаний.
- Я чувствую, что мне не доверяют, потому что вы установили программу просмотра веб-трафика на нашем шлюзе.

32.1.3.2. Активное слушание

Слушать важнее, чем говорить. Вот почему у людей ушей вдвое больше, чем ртов. Активное слушание – это прием, который обеспечивает полное общение. Мы обсудим три средства: зеркальные, обобщающие и отражающие утверждения.

Зеркальные утверждения. Стали бы вы доверять протоколу передачи файлов, который отправляет пакеты, но не проверяет, были ли они доставлены. Однако многие люди разговаривают и слушают, даже не останавливаясь, чтобы удостовериться в том, что они понимают услышанное. Фактически они относятся к разговорам как к двум односторонним потокам пакетов. Мы можем достичь лучшего, используя активное слушание, или **зеркальные утверждения**.

Активное слушание означает, что, когда слушатель что-то слышит, он пытается понять, что было сказано, прежде чем на это ответить. Вместо того чтобы отвечать своим следующим утверждением, он уделяет время для *зеркального* отражения того, что он только что услышал, при помощи точного, но более короткого утверждения. Это похоже на проверку контрольной суммы пакета перед использованием данных.

Если кто-то говорит: «Люди жалуются, что файловый сервер медленный», слушатель может поддаться на соблазн предложить решение сразу. Но вместо этого лучше сказать: «Вы говорите, что несколько человек жалуются на скорость файлового сервера?» Тогда говорящий выдает подтверждение или исправление: «На самом деле Марк получил одну жалобу и передал ее». Теперь слушатель понимает ситуацию гораздо лучше.

Марк передал жалобу на медленную работу файлового сервера. Все подобные жалобы должны проверяться, прежде чем приступают к устранению проблемы (см. раздел 14.1.2.3), однако степень обоснованности этой жалобы зависит от технической компетентности Марка. Кроме того, теперь мы знаем, что информация была повторена дважды, благодаря чему обнаружилась потеря ее части. Реакция на полную информацию будет совершенно другой и более направленной, чем обычная реакция на первоначальное утверждение.

Ваша интерпретация того, что кто-то сказал, основана на вашем воспитании и знаниях, которые абсолютно уникальны для каждого человека. Чем более разнородной является ваша организация, тем важнее становятся зеркальные

утверждения. Чем больше вы имеете дело с людьми из других частей страны или мира, тем выше вероятность, что человек, с которым вы говорите, имеет другую основу семантической интерпретации.

Не верьте своим ушам

Том работал в начинающей компании, в которой было только 10 человек, но обещали нанять еще 40 человек на следующем этапе финансирования, чтобы всего стало 50 человек. Финансирование оказалось меньше ожидаемого, и генеральный директор сказал персоналу: «Нам придется внести некоторые изменения, потому что в следующем году у нас будет меньше персонала». Генеральный директор имел в виду снижение цели в найме 50 человек, но каждый в комнате подумал, что он говорил о сокращении нынешнего штата персонала из 10 человек. Обе интерпретации были семантически правильными, но активное слушание помогло устранить путаницу. Кто-то сделал зеркальное утверждение, сказав: «Итак, я слышу, что мы уменьшаем нашу группу, вместо того чтобы набирать новых людей?» Генеральный директор сразу осознал, что его поняли неправильно, и смог разъяснить, что он имел в виду.

Чтобы не казалось, что вы спорите с человеком, полезно начинать зеркальное утверждение с фразы «Я слышал, что вы сказали...». Как только вы поймете говорящего, можно реагировать на то, что он сказал. Если каждый в вашей группе будет пользоваться одной и той же фразой, она может стать спокойным сигналом о том, что используется активное слушание и что вы пытаетесь понять человека всерьез. Это может быть действительно полезным либо может стать общепринятой шуткой. В любом случае считайте это «укреплением команды».

Пример: «Скажите еще раз»

Стандартизация определенных фраз кажется глупой, но может быть полезной. Небольшая группа работала в шумной среде, и часто сотрудники не могли расслышать друг друга. Это проблема ухудшалась тем, что некоторые слушатели, которые переспрашивали «Что?», иногда выглядели как спорящие с теми, кто говорит. Тогда последние принимали защитную позицию и заново объясняли, что хотели сказать, а не просто повторяли это. Слушатель, которому нужно было просто еще раз услышать последнюю фразу, становился раздраженным. Сотрудники группы создали правило говорить «Скажите еще раз» для обозначения «Пожалуйста, повторите, я вас не расслышал», после чего переспрашивание больше не путали с вопросом «Вы не сумасшедший? Докажите это!». Посторонний, который услышал бы, как они все время говорят «Скажите еще раз», мог бы посчитать это смешным, но это правило хорошо работало для сотрудников группы.

Обобщающие утверждения. Обобщающие утверждения высказываются, когда вы приостанавливаете беседу, чтобы перечислить упомянутые до этого утверж-

дения. **Обобщающее утверждение** – это форма зеркального утверждения, но оно охватывает больше материала. Оно часто полезно, когда человек произнес несколько длинных фраз и вы хотите убедиться, что услышали все и услышали все правильно. Иногда обобщающие утверждения используются, когда вы считаете, что людям будет полезно услышать, что они только что сказали. Иногда очень полезно услышать, как кто-то обобщает то, что вы только что сказали, особенно если человек строит утверждения немного по-другому. Кроме того, обобщающие утверждения очень важны ближе к концу собрания, чтобы убедиться, что каждый уйдет с верным пониманием обсуждаемых вопросов и последствий обсуждения.

Обобщающее утверждение должно перечислять мысли в кратких, емких фразах. Если люди исправят ваше обобщение, обдумайте его еще раз, а затем повторите обобщающее утверждение. Иногда обобщение мыслей человека помогает ему решить свою проблему.

Можно привести такой пример обобщающего утверждение: «Давайте подытожим то, что я услышал. Вы расстроены тем, как Джон к вам относится. Вы считаете, что он упрекает вас на собраниях, не соглашается с решениями, которые вы принимаете, и приписывает себе работу, которую вы делаете. Это вас очень расстраивает». Такое утверждение информирует человека о том, что его слушают, и позволяет ему убедиться, что вы не упустили никаких ключевых моментов.

Группировка вопросов изменяет их структуру и показывает лежащие в их основе проблемы, которые нужно решить, прежде чем можно будет эффективно урегулировать поверхностные проблемы. Например, посмотрите на следующее утверждение: «Давайте подытожим то, что я услышал. Два ваших вопроса кажутся проблемами, вызванными недостатком финансирования: нам не хватает персонала и мы пользуемся недостаточно мощными серверами, которые не можем позволить себе модернизировать. С другой стороны, остальные четыре ваших вопроса связаны с недостатком обучения: Джош слишком мало знает об AIX, Мэри не понимает средств отладки, которые у нас есть, Ларри не выучил Python, а Сью еще не перешла на MagentaSoft».

В конце собрания обобщающее утверждение может звучать следующим образом: «Итак, проблема заключается в низком быстродействии сервера. Пользователи жалуются. Мы исключили возможность перегрузки локальной сети или активных областей на разделах. Сара свяжется с программистами, чтобы посмотреть, хорошо ли работают их алгоритмы в WAN с высокой задержкой. Маргарет проверит два клиента, чтобы убедиться, что они не перегружены. Мы вернемся к этому на следующей неделе». Это позволяет каждому убедиться в том, что все говорят об одном и том же. Может быть полезно отправлять такие выводы всем участниками по электронной почте в качестве постоянного напоминания плана действий и соглашений.

Отражение. Отражение – это метод убедить людей в том, что их эмоции восприняты. Это особенно важно, когда человек, с которым вы общаетесь, рассержен или расстроен. Секрет общения с рассерженными людьми – немедленно сделать что-то, чтобы подтвердить, что вы понимаете их эмоции. Вы должны разобраться с их эмоциями, прежде чем сможете справиться с разборкой их жалоб. Это успокоит их. Затем вы можете начинать работать с проблемой более рационально.

Метод, которым мы здесь пользуемся, называется **отражением**: вы называете эмоцию, которая, как вы чувствуете, исходит от человека. Это кажется простым и несколько странным, но это очень эффективно[1].

Предположим, кто-то пришел в ваш офис и закричал: «Меня раздражает, что эта чертова сеть так ненадежна!» Лучшая реакция – это ответить: «Вау! Вас это действительно раздражает!» Это гораздо лучше, чем занимать оборонительную позицию.

Во-первых, человек понимает, что его услышали. Это полдела. Бóльшая часть его раздражения связана с чувством, что его не слышат. Решение обратиться к вам с жалобой потребовало от него значительной храбрости. Возможно, были и другие случаи, когда он был чем-то расстроен, но не пришел к вам. Когда он перед вами и вы подтверждаете несколько месяцев раздражения, вместо того чтобы отказывать или занимать защитную позицию, он в значительной степени успокоится.

Затем он поймет, как он сейчас выглядит. Люди часто заводятся так сильно, что не понимают, насколько рассерженными они выглядят. Отражение тонко намекает ему, как он выглядит, что может немного его смутить, но также поможет восстановить самообладание.

Теперь он начнет приходить в себя. Он может ответить: «Да, я расстроен, черт возьми!» Это показывает вам, что отражение сработало, потому что он непреднамеренно использует метод зеркальных утверждений, рассмотренный ранее. Вы можете показать открытость для разрешения проблемы, если скажете: «Тогда присаживайтесь, и мы поговорим об этом». На данном этапе он должен успокоиться, и вы сможете продуктивно обсудить проблему.

Если он не успокоится, примените свои навыки активного слушания – зеркальные и обобщающие утверждения, – чтобы обсудить эмоциональную сторону вопроса. Не стоит недооценить тот факт, что технические проблемы не могут быть решены, пока вы не ответите эффективно на эмоциональную сторону вопроса. Как только человек успокоится, приготовьте свои отражающие и обобщающие утверждения, чтобы разобраться с технической проблемой.

32.1.4. Профессиональное развитие

Профессиональное развитие означает получение обучения, необходимого для поддержания и усовершенствования ваших навыков. Кроме того, оно означает связь с профессиональными организациями в вашей области.

Могут быть профессии, которые не очень сильно меняются и не требуют владения последними технологиями и методами. Однако системное администрирование таковым не является.

Изучение новых навыков интересно и помогает в вашей карьере. Наш опыт показывает, что системные администраторы склонны считать «изучение нового» одним из самых интересных занятий. Никогда не отказывайтесь от возможности учиться.

---

[1] И мы обещаем, что впервые, когда вы это попробуете, вы будете чувствовать себя глупо.

Чтение может держать вас в курсе новых технологий. Постоянно появляются новые книги, а также отраслевые и научные журналы. Мы также рекомендуем вам подписаться на основной специализированный журнал отрасли, в которой работают ваши пользователи, чтобы вы были в курсе тенденций отрасли, интересных вашим пользователям.

Однодневные семинары и программы обучения выполняют другие задачи, нежели недельные конференции. Однодневные семинары обычно *тактические*: ориентированные на конкретную технологию или навык. Недельные конференции являются *стратегическими*: они дают возможность обсуждать более широкие темы, сотрудничать, создавать сообщество и продвигать системное администрирование как авторитетную профессию. Недельные конференции имеют сильный эффект, предоставляя такую нужную возможность расслабиться. Кроме того, они создают атмосферу поддержки, в которой вы можете отойти от своей ежедневной работы и взглянуть на картину в целом. Участники возвращаются к своей работе полными новых идей и видения: свежими, с мотивацией и вновь открытыми перспективами.

Несмотря на то что эта книга не рекомендует конкретных продуктов, мы не можем не выразить наш восторг от организаций USENIX (Advanced Computing Systems Association – Ассоциация продвинутых компьютерных систем) и LOPSA (League of Professional System Administrators – Лига профессиональных системных администраторов). Мы получаем много пользы от ежегодной технической конференции USENIX, симпозиума по безопасности и конференций LISA (Large Installation System Administration). Есть много способов вступить в эти международные группы, помимо различных местных организаций. Добровольная работа с этими группами, написание статей, подготовка статей для их информационных бюллетеней, помощь в планировании конференций и выступление на их собраниях может сильно помочь в формировании вашей репутации и развитии карьеры.

32.1.5. Оставаться техническим сотрудником

Мы часто слышим, как системные администраторы жалуются: «Они пытаются превратить меня в руководителя, но я хочу остаться техническим сотрудником!» – и просят совета о том, как не получить повышение. Если это ваша ситуация, нужно запомнить кое-что. Во-первых, если ваш руководитель пытается повысить вас до руководящей должности, он считает это комплиментом. Не обижайтесь. Несмотря на то что некоторые системные администраторы имеют негативное мнение о руководителях, сами они считают, что руководство – это хорошее положение. Может быть, руководитель видит в вас большой потенциал. Примите предложение всерьез и подумайте над ним некоторое время. Может быть, оно вам подходит. Однако помните, что переход на руководящую должность означает отказ от технических обязанностей, не думайте, что вы сможете сохранить свои технические обязанности и принять на себя новые.

Некоторые системные администраторы становятся руководителями постепенно, со временем увеличивая руководящие обязанности. Внезапно они понимают, что становятся руководителями и не хотят этого.

Чтобы не допустить этого, вы должны осознавать, какие задачи принимаете на себя. Если вы хотите оставаться техническим сотрудником, важно обсудить это

с вашим начальником. Объясните, что есть разница между «техническим лидером» группы и «руководителем» группы. Согласуйте, как будет определяться граница, то есть так называемую лакмусовую бумажку. Например, *технический лидер* – участник технического процесса разработки и установки новой системы. *Руководящие* задачи обычно предполагают обзор бюджетов, зарплаты и производительности, а также других кадровых вопросов. Мы рассмотрим управление карьерой более подробно в разделе 32.2.3.

32.2. Тонкости

Теперь, когда вы можете управлять собой, своим временем и своей карьерой, эти умения можно объединить для создания некоторых навыков более высокого уровня, например основ ведения переговоров, небольших размышлений о том, как любить свою работу, и управления вашим руководителем.

32.2.1. Учитесь вести переговоры

Системным администраторам требуются хорошие навыки ведения переговоров, потому что они часто имеют дело с поставщиками, пользователями и своими собственными начальниками. Переговоры – это искусство получать то, что вам нужно. Оно требует всех навыков общения, рассмотренных в предыдущих разделах, и некоторых других.

32.2.1.1. Работайте для достижения взаимной выгоды

Важно работать для достижения взаимовыгодной ситуации. То есть договаривайтесь о соглашении, которое будет прибыльным для обеих сторон. Бесполезно уговаривать поставщиков согласиться на такую низкую цену, что они не смогут себе позволить предоставлять вам хорошее обслуживание, или уступать до того, как вы получите то, на что имеете право. Ситуация, выгодная для вас, но невыгодная для другого человека, является второй наиболее предпочтительной. В ситуациях, невыгодных вам, но выгодных другой стороне, а также невыгодных обеим сторонам, вы проигрываете, поэтому всегда избегайте их.

32.2.1.2. Определите ситуацию

Первый шаг в переговорах – определить, что вы находитесь в ситуации переговоров. Это может звучать странно, но мы очень много раз слышали, что кто-то подписывал контракт, а потом говорил: «Нужно было просить больше денег» или «Может быть, они хотели договориться». Это означает, что человек не остановился, чтобы разобраться, является ли данный случай ситуацией ведения переговоров. В разговоре с пользователями, поставщиками, персоналом технической поддержки, продавцами автомобилей и даже с родителями всегда уместна волшебная фраза: «Можем ли мы договориться об этом?»

Когда ваша группа находится в ситуации ведения переговоров, сообщите этот факт всей группе. Устройте собрание и объясните, что происходит. Знание – сила, поэтому убедитесь, что группа знает, какая информация не должна утечь.

Пример: подготовьте группу и предотвратите ошибки

Инвестиционная фирма узнала, что высокотехнологичной начинающей компании, с которой она вела переговоры, требовалось финансирование к определенной дате. Фирма могла использовать эту информацию для своей выгоды и против начинающей компании. Как инвестиционная фирма узнала эту информацию? Сотрудники начинающей компании свободно ее выложили, потому что никто не сказал им, что этого делать нельзя. Этого можно было избежать, если бы сотрудников начинающей компании собрали и рассказали им о стратегии, в частности о том, какую информацию нужно защищать. Существуют способы действовать безотлагательно, не теряя контроля над ситуацией. Кроме того, можно было назначить человека, ответственного за переговоры по конкретным деликатным моментам, и другие сотрудники группы могли бы отправлять интересующихся к этому человеку.

Кроме того, вам нужно осознавать расстановку сил. Кто является запрашивающей стороной? Кто отвечает на просьбу? Кто владеет инициативой в переговорах? Если у вас более сильная позиция, вы можете контролировать переговоры. Если более сильная позиция у другой стороны, то вы должны лучше подготовиться для защиты своих просьб. Запрашивающая сторона не всегда является более слабой, точно так же и человек, получающий запрос, не приобретает более сильную позицию автоматически. Расстановка сил не является статичной, она может неожиданно изменяться.

Расстановка сил может меняться

Том вел переговоры с поставщиком, который был в более выгодном положении, потому что ранее у компании Тома были значительные вложения в продукт поставщика и она не могла легко его поменять. Но один из продавцов поставщика проболтался, что, если поставщик не оформит продажу до конца недели, она будет перенесена в квоту продаж на следующий год. Теперь в более выгодном положении был Том. Он знал, что поставщик скорее захочет получить свое комиссионное вознаграждение на баланс этого года. Когда продавцы отказались снижать цену, он рассказал о проблемах, которые задержат подписание контракта, но пообещал, что все препятствия будут устранены и контракт будет подписан до конца недели, если он получит продукт по желаемой цене. Поставщик уступил.

32.2.1.3. Планируйте свои переговоры

Планирование важно. Соберитесь с людьми, которые будут на вашей стороне, и решите, что вы хотите получить. Что из этого вам обязательно нужно? Чем вы могли бы пожертвовать? Что занимает среднее положение?

Решите, какие элементы нужно сохранить в тайне и как это будет обеспечиваться. Обсудите расстановку сил и то, как она влияет на стратегию. Определите

сценарий проведения встречи, что вы собираетесь говорить и какова будет ваша реакция при задавании тех или иных вопросов.

Важно точно знать, чего вы просите. Неясные просьбы могут без необходимости затягивать переговоры.

Пример: знайте конкурента поставщика

В начале 1990-х годов Sum Microsystems и HP сражались за рынок рабочих станций. Один системный администратор работал в компании, которая пользовалась рабочими станциями обеих компаний. Он считал полезным вешать на стену в своем офисе плакат Sun и пить кофе из кружки Sun, когда к нему приходили продавцы из HP, и делать наоборот, когда приходили продавцы из Sun. Это было тонким намеком на то, что он всегда мог обратиться в другое место.

Пример: делайте свои домашние задания

Выполнение домашних заданий может предоставить большое преимущество, особенно если другая сторона их не сделала. Когда Том встречается с поставщиками услуг для продления ежегодного контракта на обслуживание, он всегда приносит кучу распечаток, каждая страница которых – это заявка на устранение неисправности, с которой не справился поставщик услуг. На каждой из них есть пометки от руки, сделанные человеком, который подавал эту заявку, описывающие, что случилось. Хотя неправильно обработанных заявок всегда бывает крайне мало по сравнению с числом выполненных, Том ведь не был виноват в том, что поставщики никогда не имеют при себе данных, чтобы это показать. В результате поставщики, уличенные в фактах своих ошибок, всегда становились более сговорчивыми. В ключевые моменты переговоров Том берет страницу, читает вслух пометки, хмурится и сидит молча, пока поставщик не предложит еще одну уступку. Это было бы не так эффективно, если бы поставщики делали свое домашнее задание и привозили с собой статистические материалы, показывающие, что по большинству служебных запросов работа выполняется отлично.

Другие методы требуют репетиции

Перед некоторыми трудными переговорами о ценах Том заставлял свою группу репетировать ситуацию, в которой он представлялся крайне рассерженным и выходил из помещения на пару минут. Его группа должна была сделать вид, что нервничает, минуту помолчать, а затем сказать продавцам: «Мы никогда не видели, чтобы он был так недоволен поставщиком». Затем они нервно ерзали на стульях, пока Том не возвращался. Повторение – мать учения.

Два последних примера содержат жесткие тактики, которыми можно пользоваться очень редко. Они нарушают отношения между вами и другой стороной и повредят вам в будущем. Как было сказано выше, лучше добиваться взаимовыгодной ситуации. Каждые переговоры – это возможность создать позитивные отношения. Будущая отдача неоценима. Есть только одна ситуация, в которой можно использовать такую тактику, – если вам больше никогда не придется вести переговоры с этим человеком (Coren and Goodman 1992).

Последние два примера представляют собой в точности такую ситуацию: после переговоров этот сотрудник по продажам был «не в курсе событий», пока контракты не нужно было продлевать. Такие контракты на многолетнее обслуживание фактически гарантировали, что через несколько лет, когда будут вестись переговоры о продлении, в них будет участвовать другой человек. Ежеквартальные обновления контрактов выполнялись через горячую линию обслуживания пользователей, персонал которой не видел жесткости предыдущих переговоров. Сотрудник по продажам, с которым Том обычно общался по поводу закупок оборудования, не участвовал в переговорах о заключении контрактов на обслуживание, и поэтому здесь не нарушались никакие связи. Наконец, Том знал, что он увольняется из этой компании и поэтому не будет участвовать в следующих переговорах о продлении. Если бы связи были нарушены, его преемник мог бы воспользоваться другим известным приемом: обвинять предшественника, чтобы добиться расположения поставщика. «О, *он* был негодяем, но *я* – хороший парень. Так что давайте начнем наши отношения с чистого листа». Этот прием работает только один раз. Если вы слишком часто будете жестко вести переговоры, люди в конце концов перестанут иметь с вами дело.

Разнообразие также полезно, как видно из следующего примера.

Пользуйтесь разнообразными методами

У Тома была руководительница, которая успешно повторяла одну тактику ведения переговоров: с ней было настолько трудно иметь дело, что люди всегда давали ей то, чего она хотела. Однако скоро он понял, что это была ее *единственная* тактика. Вскоре все люди стали избегать иметь с ней дело, ее карьера остановилась и она оказалась в изоляции. Остерегайтесь разрыва слишком большого числа связей.

32.2.1.4. Установите формат встречи для переговоров

Общий формат встречи для эффективных переговоров – определить условия, прийти к соглашению по вопросам, где мнения совпадают, а затем работать над более сложными элементами. Это сразу задает позитивную обстановку для разрешения простых вопросов. Если что-то, казавшееся простым, начинает занимать много времени, отложите это. Часто вы будете доходить до окончания списка вопросов только для того, чтобы узнать, что расхождений очень мало или что один вопрос, по которому у вас есть разногласия, можно исключить. Обычно вы будете обнаруживать, что оба человека находятся на одной стороне, и в этом случае переговоры больше должны быть направлены на согласование и принятие обязательств.

32.2.1.5. Дополнительные советы по ведению переговоров

Эти советы связаны с просьбами и предложениями. Они особенно полезны при переговорах о зарплате, но справедливы для любых переговоров.

- *Просите то, чего вы на самом деле хотите.* Не ведите переговоры против себя. Некоторые начинают с заниженных запросов, потому что они стесняются просить то, чего хотят, чувствуют себя виноватыми из-за того, что хотят слишком много, или думают, что их оппонент посчитает это неоправданным и откажется продолжать переговоры. Не будьте глупыми! Занижение запроса – это задача вашего оппонента, а не ваша. Не делайте работу за других людей. Вас будут больше уважать, если вы честно станете просить то, чего хотите. Вы удивитесь, как часто просьбу принимают. Ваше дело – спросить. Дело другого человека – согласиться или не согласиться. Делайте *свое* дело.
- *После того, как вы что-то попросите или предложите, закройте рот.* Вы также не должны вести переговоры против себя, когда просите или предлагаете. Люди совершают ошибку, когда высказывают предложение, начинают беспокоиться, слыша в ответ молчание, и сразу же делают уступку, чтобы облегчить дело. Ваше дело – попросить или предложить, их дело – принять или отклонить это. Иногда люди молчат, потому что им нужно время подумать или потому что они надеются вызвать у вас беспокойство, чтобы вы улучшили свое предложение даже без просьбы. Если молчание вас беспокоит, мысленно повторяйте фразу: «Кто первый заговорит – неудачник». И терпеливо ждите ответа.
- *Не раскрывайте свою стратегию оппоненту.* Несмотря на то что вы не должны быть параноиком, вы также не должны раскрывать оппоненту свою стратегию. Не говорите самую низкую или высокую цену, приемлемую для вас, – только предложение, которое вы делаете в данный момент. Если в переговоры вступает агент по недвижимости, специалист по подбору кадров или другой подобный агент, действующий якобы в ваших интересах, этот человек на самом деле представляет того, кто ему платит. Всегда уместно прямо спросить агента: «Кто платит вам комиссионные за это?» Вряд ли вам понравится неожиданное заявление, что это вы! Если он не говорит вам, кто ему платит, то он нечестен. Если он говорит: «Не беспокойтесь, вам ни за что не придется платить», это значит, что ему платит ваш оппонент. Если ему платит ваш оппонент, значит, они в одной связке и вы должны раскрывать ему только то, что раскрыли бы оппоненту. Он может говорить, что представляет вас, но если он получает комиссионные от работодателя, землевладельца или кого-либо еще, он «представляет вашу позицию» другой стороне, но действует в интересах вашего оппонента. Следовательно, если он спрашивает вас, насколько высокую (или низкую) цену вы собираетесь установить, ведите себя с ним как с оппонентом: раскройте только ваше текущее предложение. Если он хочет узнать ваши нижнюю и верхнюю границы, чтобы он «мог вести переговоры в ваших интересах», дайте ему выдуманные цифры[1].

[1] Призывая вас не раскрывать свою стратегию, мы сразу оговоримся, что тоже не раскрыли вам все свои секреты, поэтому не пытайтесь использовать эти методы против нас. У нас есть контрмеры. Правда!

- *Всегда отказывайтесь от первого предложения. Первое предложение* всегда бывает встроено в какое-то пространство для маневра на случай, если оно будет отклонено. Следовательно, всегда отклоняйте первое предложение. Этот механизм прекрасно показан в фильме 1995 года «Бестолковый» (Clueless). Этот прием работает только один раз. Не надо автоматически предполагать, что если один раз вам пошли на уступку, то так будет продолжаться и дальше. Если ваш оппонент не хочет менять свои условия, подожмите хвост и примите первое предложение. Это рискованный метод, пользуйтесь им осторожно. Это не двоичный поиск, работодатели обычно не делают второй итерации.

32.2.1.6. Используйте молчание как средство ведения переговоров

Как было рассмотрено выше, молчание – критический навык ведения переговоров. Молчание вашего оппонента может просто означать, что он думает, ему нечего сказать или он пытается вызвать в вас беспокойство. Большинство людей беспокоятся, когда во время переговоров сталкиваются с молчанием, и реагируют, предлагая уступки, о которых их даже не просили. Другой важный момент, когда надо молчать, – момент заключения соглашения. Мы видели, как две стороны наконец приходят к соглашению только для того, чтобы разрушить его, когда кто-то поднимает новые вопросы. Вы получили то, что просите, поэтому замолчите!

Думайте, что говорите

Одна женщина переходила в другое подразделение из-за возможности продвинуться по карьерной лестнице и получить повышение зарплаты. Ее новый начальник сказал, какой будет ее зарплата, а затем спросил: «Вы хотели бы, чтобы она была больше?» Она ответила: «Да». Она была потрясена тем, что кто-то вообще может задать такой глупый вопрос. Возможен ли какой-то другой логичный ответ на него? Он мог просто подождать, пока она подпишет договор, и предложить большую зарплату, только если бы она отказалась от предложения. Теперь, когда он предложил повысить ее зарплату и она согласилась, у него не было другого выбора, кроме как немедленно увеличить размер зарплаты. Позднее она говорила, что не наняла бы никого, кто ответил бы «нет» на такой вопрос. Для нее это было что-то вроде плохо пройденного тест на IQ. Кроме того, она отметила, что не взяла бы на работу никого, кто задал бы такой вопрос. Такой человек способен обменять последнюю корову семьи на волшебные бобы.

Несмотря на то что все эти приемы ведения переговоров у нас работали, мы не являемся серьезными экспертами в ведении переговоров. К счастью, некоторые настоящие эксперты написали по этой теме книги. Часто книги являются специализированными для конкретной профессии или ситуации. Книг по ведению переговоров специально для системных администраторов нет, но *«Hagglers Handbook»* (Koren and Goodman 1992) – это очень хорошая книга общего на-

значения, и ее преимущество в том, что каждый совет занимает одну страницу. Вы можете читать по странице в день, собираясь на работу утром, и через несколько недель вы станете гораздо лучшим специалистом по ведению переговоров.

32.2.2. Любите свою работу

Счастливые системные администраторы, которых мы видели, любят свою работу. В этом нет ничего странного. Они не сразу нашли работу, которую любят, они работали на многих должностях во многих компаниях и начали понимать, что им нравится, а что нет. Затем они смогли лучше сосредоточиться при поиске работы. На то, чтобы выяснить, что заставляет вас любить свою работу, и найти работу, которая имеет эти качества, могут уйти годы и даже десятилетия, но об этом стоит задуматься с развитием вашей карьеры.

32.2.2.1. Наслаждайтесь тем, что вы делаете

В фильме 1999 года «Office Space» (Офисное пространство) есть интересная идея. Представьте себе, что вы выиграли в лотерею и вам больше не нужно работать. Чем бы вы занялись, чтобы заполнить свое свободное время? Ваш ответ – это то, какой работой вы должны заниматься. Если бы вы стали проводить свое время, восстанавливая старые машины, станьте автомехаником. Может быть, вы системный администратор, потому что вы проводили бы время, занимаясь с компьютерами. Какие аспекты работы с компьютерами вам так сильно нравятся? Займитесь их внесением в свою карьеру.

Следуйте нашему собственному совету

Кристина всю жизнь была фанатом Формулы-1 и всегда хотела работать в этой системе. Она решила, что пора двигаться к этому идеалу. После того как вышло первое издание книги, она начала работать в гонках Формулы-1. Она любит свою работу и рада, что решилась на риск, изменив свою карьеру.

Том всегда хотел заниматься политикой. В 2003 году он уволился с работы и начал участвовать в политической кампании. Он считает это очень интересным и приносящим удовольствие занятием и будет искать другие возможности принять участие в политических кампаниях, в которые он верит. Для достижения успеха кампании все чаще полагаются на технологии, и он хочет в этом участвовать.

32.2.2.2. Наличие мотивации

Нет ничего странного в наличии мотивации в своей работе. Удовлетворяющая и долгосрочная мотивация различна для разных людей. Деньги являются мотивацией, но лишь на короткий период. Мы сталкиваемся с тем, что они не очень хорошо поддерживают мотивацию. Для некоторых людей мотивацией является приятное чувство, которое они получают от того, что помогают кому-то. Это кажется простым, но помощь людям входит в привычку. Приятное чувство,

которое вы получаете, зная, что помогли кому-то, является таким сильным, что, однажды почувствовав его, вы будете желать его даже больше. Вы хотите вернуться к этому приятному чувству, поэтому помощь людям становится еще более важной и вы стремитесь помогать еще большему количеству людей. Это показано в фильме «Новая рождественская сказка» (Scrooged).

Комплименты, которые люди получают, также входят в привычку. Похвала заставляет человека двигаться вперед. Представьте, что каждая похвала от начальства дает вам новый импульс и мотивирует для серьезных продвижений.

Проблема заключается в том, что такие комплименты долго идут от вашего уха до участка мозга, который *принимает комплимент*. Где-то на этом пути находится минное поле, известное как ваш *критический внутренний голос*. Иногда этот голос становится громче, перехватывает похвалу на полпути и загрязняет ее токсическими отходами. Тогда похвала становится испорченной. К тому времени, как она достигнет пункта назначения, токсические отходы превращают ее в нечто такое, что оскорбляет вас. Таким образом, вместо потока входящих комплиментов, которые заставляют вас двигаться вперед, у вас имеется поток негатива, высасывающий вашу энергию.

У некоторых людей критический внутренний голос – это маленький управляемый зверек. У других это громкий, рычащий гигант. Терапия может помочь справиться с этим гигантом, избавляя вас от источника проблемы, будь то излишне критичный родитель, излишне властный супруг или чувство вины.

Чувство вины появляется из-за связанных с чем-то отрицательных эмоций, когда их удерживают внутри, не позволяя выйти наружу. Люди часто думают, что их личные проблемы должны оставаться дома и их не следует обсуждать на работе, но накапливание этих проблем внутри может вредить здоровью и подрывать вашу производительность. Представьте, что кто-то из ваших родителей болен и вы поделились своими чувствами об этом со своими коллегами. Позитивная поддержка, которую вы получите, должна мотивировать вас и создавать положительные эмоции, но вместо этого ядовитый стыд, например, от чувства, что вы не навещаете своего больного родителя, подавляет похвалу: «О, они бы меня не хвалили, если бы знали, какая я ужасная дочь».

Следовательно, принимать комплименты важно. Когда люди отклоняют похвалу, они наносят себе ущерб. Люди склонны отвечать на похвалу такими фразами, как «Ой, да ничего» или «Я мало сделал, на самом деле всю работу сделала Маргарет». Если кто-то достаточно вежлив, чтобы вас похвалить, примите комплимент! Если вы не знаете, что ответить, будет достаточно просто сказать «Спасибо!».

Чувство вины может принимать другие формы. Страхи расизма, сексизма и гомофобии могут препятствовать достижению людьми своего полного потенциала. Вы можете считать комплименты неубедительными, если ваш руководитель предубежден против вашего пола, расы или сексуальной ориентации. Вы можете разрешить эти проблемы, обсудив эти страхи со своими коллегами и работая для достижения лучшего понимания и оценки ваших отличий. Если ваша корпоративная культура не одобряет открытость в обсуждении личных проблем, вам может быть полезно, по крайней мере, раскрыть свои чувства кому-то персонально, например начальнику или близкому коллеге.

Небезопасное рабочее место – это непродуктивное рабочее место

Системный администратор-бисексуал потерял недельную производительность, потому что случайно услышал, как его коллега в соседнем блоке говорил, что «всех гомиков надо убить». Мог ли он безопасно дойти до своей машины после работы, если бы этот коллега узнал, что он бисексуал? Саботировал бы коллега его работу? Каждый раз, когда он пытался работать, воспоминания о словах его коллеги отвлекали его. На следующий день он обратился с этой проблемой к своему начальнику, который отказался беседовать с коллегой или переносить рабочее место системного администратора. В конце концов системный администратор ушел из компании. Руководитель мог бы сэкономить расходы на наем и обучение нового сотрудника, если бы уделил время тому, чтобы объяснить коллеге, что такие высказывания недопустимы на рабочем месте и что их компания оценивает людей по качеству их работы, а не по расе, сексуальной ориентации, полу или другим не связанным с работой характеристикам. Кроме того, руководитель мог бы объяснить, что разнообразие делало группу сильной.

32.2.2.3. Счастье

Теоретики познания считают, что ощущение себя счастливым или несчастным определяется не хорошими или плохими событиями, которые происходят с людьми, а тем, как они реагируют на то, что происходит вокруг них. Как такое возможно? И снова мы возвращаемся к концепции критического внутреннего голоса. Некоторые люди могут заставить этот голос замолчать, когда им нужно, другие уделяют ему слишком много внимания.

Например, представьте, что на чей-то дом упало дерево. Один человек может подумать: «Конечно, оно упало на мой дом, я не заслуживаю безопасного жилища». Кто-то другой может подумать: «Хорошо, что никто не пострадал!», и заняться ремонтом.

Обратная ситуация также возможна. Обычно вы считаете, что повышение зарплаты – это хорошо. Однако у некоторых людей оно может вызвать серьезное беспокойство: «Я уже работаю на пределе своих возможностей, теперь они ожидают от меня еще больше. Я обречен на неудачу!» В первой части книги *«The Feeling Good Handbook»* (Burns 1999a) предоставлены другие примеры, а также ряд прекрасных решений.

Небольшая неуверенность – это нормальная и здоровая ситуация. Она удерживает людей от безрассудства и призывает их «семь раз отмерить, один отрезать». Однако избыток неуверенности может вызвать проблемы.

К счастью, вы можете себя подготовить. Первый шаг – убедиться в том, что этот критический внутренний голос существует. Люди могут так к нему привыкнуть, что они верят ему, не останавливаясь, чтобы оценить, что он говорит. Как только вы убедились в том, что он говорит, остановитесь, чтобы подумать, о чем он говорит. Определите источник. Сомневается ли он во всем? Видит ли он мир как черное и белое? Повторяет ли он негативные высказывания, сказанные о вас посторонними?

Пример: определите источник

У одного системного администратора произошел серьезный прорыв, когда он обнаружил, что его критический внутренний голос всегда повторяет негативные высказывания, которые в детстве говорила ему его излишне критичная мать. Этот голос действительно звучал как голос его матери. Он понял, что эти мысли были просто отголосками крайней степени негатива, который он получил в детстве, а не полезными советами. Он решил развить привычку игнорировать эти мысли, пока они не исчезли. Это сработало!

Подготовить себя не так легко, но это можно выполнить успешно. Многие люди предпочитают делать это с помощью и под руководством психотерапевта. Другие делают это сами. Бернс (Burns 1999a) рассматривает большое количество приемов и предлагает полезное руководство по выбору тех, которые подходят для вас. Воспользуйтесь конфиденциальной программой оказания помощи сотрудникам (Employee Assistance Program – EAP), если ваш работодатель предоставляет ее в качестве элемента обеспечения душевного здоровья сотрудников.

32.2.2.4. Хороший начальник/плохой начальник

То, как вы относитесь к своей работе, в большей степени зависит от того, какой у вас начальник, а не от привлекательности самой работы. *Плохая работа с хорошим начальником лучше, чем хорошая работа с плохим начальником.* Представьте, что у вас была бы лучшая, самая фантастическая работа в мире. Например, представьте, что вам платили бы за то, чтобы вы весь день ели шоколад. Если бы ваш начальник был негодяем, вы все равно ненавидели бы свою работу. С другой стороны, если бы у вас была ужасная работа, хороший начальник мог бы найти способ, чтобы она стала приносить вам удовольствие. Наш личный опыт показывает, что большинство людей увольняются не из-за того, что не любят свою работу, а из-за того, что не любят своих начальников.

32.2.2.5. Принятие критики

Помимо правильного принятия комплиментов, важно уметь правильно принимать критику. Всех постоянно критикуют. Некоторые люди считают критикой все высказывания, у других малейшая критика задевает их чувство собственного достоинства. Это неправильно. Однако, если вы будете принимать критику позитивно, она может помочь вам изменить свое поведение, чтобы вы могли совершенствоваться. Критика – это хорошо: она удерживает людей от повторения ошибок. Представьте, как было бы ужасно, если бы все постоянно повторяли одну и ту же ошибку! Вместо того чтобы принимать критику пренебрежительно, лучше поблагодарить человека за честность и подумать, что можно улучшить в будущем.

Важно отличать конструктивную критику от неконструктивной. Неконструктивная критика оскорбляет чувства, не помогая ситуации. Будьте осторожны с неконструктивной критикой в отношении себя: не надо добивать себя фразой «должен был». «Должен был» – это ругательное выражение. Когда вы думаете о себе: «О, я *должен был* поступить так и так», вы ругаете себя за то, что не

можете контролировать, – за прошлое. Гораздо лучше заменить «я должен был» на «в следующий раз я сделаю».

32.2.2.6. Ваша структура поддержки

Каждому нужна структура поддержки. Каждому нужен кто-то, с кем можно время от времени поговорить. Ваша структура поддержки – это сеть людей, к которым вы можете пойти, когда вам нужно поговорить о проблеме. Наличие разных людей, к которым вы можете обратиться за советом по офисной политике, профессиональной консультацией и рекомендацией в жизненной ситуации, очень важно, когда вы чувствуете, что не понимаете чего-то. Развитие таких отношений требует времени. Иногда подходящим человеком является супруг или близкий друг, коллега или руководитель или даже друзья по интересам из списка рассылки, на которую вы подписаны.

32.2.2.7. Обращайтесь за помощью

Важно обращаться за помощью. Мы обнаружили, что у системных администраторов не очень хорошо получается искать помощи в решении личных проблем и они склонны позволять проблеме расти, пока она не станет невыносимой.

Возможно, это связано с некоторой культурой «мачо», предполагающей, что нужно быть самодостаточным. Возможно, из-за того что они привыкли решать проблемы, прежде чем пользователи их замечают, системные администраторы предполагают, что другие люди будут читать их мысли, когда проблемы возникнут у них самих. Может быть, это из-за того, что от системных администраторов ожидают самостоятельного решения технических проблем и они пытаются перенести это на свою личную жизнь. Даже когда системные администраторы обращаются за технической помощью, они часто пользуются не-человеческими ресурсами: веб-страницами, FAQ и руководствами. Даже обращение за помощью в списках рассылки по электронной почте имеет обстановку отсутствия личного разговора о проблемах.

Благополучные люди знают, что обратиться за помощью – это не слабость. На самом деле люди уважают тех, у кого хватает мужества честно попросить о помощи. Другим проще справиться с проблемой, пока она незначительна, чем когда она вырастет в крупное бедствие. Самое важное, что проблемы быстрее решаются, когда над ними работают много людей. Разделите богатство! Друзья помогают своим друзьям. Это как банковский счет: вы делаете вложение, когда помогаете своим друзьям, и вы не должны ощущать неудобство, время от времени забирая средства со счета.

Нужно было обратиться за помощью

Все было бы лучше, если бы один системный администратор обратился за помощью. Он собирался представить статью на очень крупной конференции системных администраторов. Когда он не появился в назначенное время, за 15 минут до презентации, координаторам пришлось потрудиться, чтобы изменить порядок остальных выступлений. Он появился за несколько секунд до выступления, когда ведущий конференции уже объявлял выступающего вместо него.

Он опоздал, потому что принес только слайды, а не ноутбук с презентацией. Увидев, что все остальные выступающие показывали презентации напрямую с ноутбуков, он спросил техника на конференции, можно ли выступать со слайдами. Техник не знал, что необходимое оборудование имелось в наличии, и ошибочно сказал ему, что со слайдами выступать нельзя. Вместо того чтобы обратиться за помощью к одному из координаторов конференции, системный администратор получил от своего начальника разрешение арендовать ноутбук за крупную сумму денег. Этот ноутбук работал только под Windows, а его презентация была написана под Linux, поэтому он провел несколько часов, переписывая презентацию под Windows. Его начальник в это время открыл к его презентации доступ через Интернет на случай, если он сможет найти кого-нибудь с ноутбуком под Linux, который можно будет одолжить.

Если бы он обратился за помощью, координаторы смогли бы предоставить ему оборудование для показа слайдов или легко нашли бы для него ноутбук под Linux. Вместо этого он подверг себя и других огромному стрессу и потратил много денег на аренду ноутбука. Он должен был обратиться за помощью.

У нас есть похожие истории о других личных проблемах, например финансовых, со здоровьем, семейных, а также проблемах отношений и даже злоупотребления наркотиками и алкоголем. В каждом случае друзья человека сожалели, что он не обратился к ним раньше. Для этого и существуют друзья.

32.2.2.8. Уравновешивайте работу и личную жизнь

Поиск равновесия между работой и личным временем важен для душевного здоровья. Несмотря на то что может быть приятно чувствовать себя жестким технарем, который работает днями и ночами, в конце концов можно сгореть на работе. Необходимо уделять время себе. Очень важно развить привычки устраивать перерывы в течение дня, регулярно спать, иметь общественную жизнь вне работы и не трудиться до изнеможения.

Относитесь к своей второй половине с уважением, которое он или она заслуживает. Многие системные администраторы работают так много, что их вторые половины становятся «техническими вдовами». Это неуважение к ним. Семейное время[1] – это важно, уделяйте время своим близким. Дайте им благодарность и обожание, которого они заслуживают. Поставьте на свой стол их фотографии, чтобы у вас всегда было напоминание о том, что вы занимаетесь этим для них (Crittenden 1995). Самое важное, что вы можете дать своим близким, – это время. Никто не говорил перед смертью последние слова «Жаль, что я не проводил больше времени в офисе».

Относиться бережно к своему организму также важно. Прислушивайтесь к своему организму. Если вы устали, поспите. Если вы голодны, поешьте. Если вы неважно себя чувствуете, помогите своему организму восстановиться. За-

[1] Под «семьей» мы имеем в виду очень широкое определение. У людей, не состоящих в браке, также есть семьи. У некоторых людей есть названные семьи, а не биологические (Small 1993).

бавно, что мы часто встречаем людей, которые заботятся об огромных сетях, но не знают, как позаботиться о своем собственном организме.

Ваш работодатель дает вам отпуск. Возьмите его, компания предоставляет его вам для того, чтобы вы не сгорели на работе и не стали затем совершенно бесполезным для нее. Уже давно работодатели поняли, что отпуска полезны как для сотрудников, так и для работодателей.

Вы не поможете себе или своей компании, отказываясь от отпусков. Много раз мы слышали, как люди гордились отсутствием отпуска в течение нескольких лет: «Моя компания не может без меня жить», или утверждали, что пропуск отпуска показывает ваше усердие. На самом деле справедливо обратное. Если раз в год вы не будете исчезать с работы на неделю или две, будет невозможно определить, как качественно подготовлена ваша документация и насколько хорошо обучены заменяющие вас люди. Лучше узнать о своих недоделках во время отпуска, из которого вы вернетесь, чем когда вы уволитесь или, не дай бог, попадете под машину.

32.2.2.9. Доска почета

Наконец, у нас есть еще одна рекомендация для поддержания позитивного чувства собственного достоинства и любви к своей работе. Создайте «Доску почета» – место, где вы размещаете все положительные отзывы, которые получаете: записку от пользователя с благодарностью, полученные вами награды и т. д. Убедитесь, что они находятся в том месте, которое вы видите каждый день, чтобы у вас было постоянное напоминание о хороших делах, которые вы сделали. Если вы начальник группы, то можете создать такую Доску почета для всех достижений группы и расположить ее там, где ее будет видеть вся группа. Когда вы упадете духом, вы можете взглянуть на Доску, чтобы напомнить себе о временах, когда люди хорошо о вас отзывались.

Электронная Доска почета

Большое количество позитивных отзывов приходит по электронной почте. Мы рекомендуем вам сохранять каждую благодарность в папке электронной почты под названием «Перья»[1], потому что они как перья на вашей шляпе. Когда вы составляете свой ежегодный список достижений, можно просмотреть эту папку, чтобы убедиться, что вы ничего не забыли. В те дни, когда вы в депрессии или дела идут плохо, откройте эту папку и напомните себе о том хорошем, что люди о вас говорили.

32.2.3. Управление своим руководителем

Давайте сначала рассмотрим «философию начальника». У вашего начальника есть работа. Его производительность измеряется тем, выполнены ли определенные задачи. Эти задачи слишком велики, чтобы их мог выполнить один человек. Вот почему существуете вы. Ваша задача – выполнить группу заданий, равных небольшой части задачи вашего начальника. Некоторые люди считают своей

[1] Спасибо Томми Рейнгольду за это название.

работой задания, которые им дают. Это не так. Ваша работа – обеспечить успех вашего начальника. Удивительно, но ваш начальник находится в таком же положении. Ему выделили небольшую часть того, что нужно выполнить его начальнику. В таком же положении находится и его начальник, и вся цепочка до главы вашей организации. Сумма всех этих небольших частей – это один большой успех.

Почему вы должны заботиться об успехе вашего начальника? Во-первых, успешных начальников повышают. Честный начальник возьмет вас с собой. Во-вторых, у руководителя есть ограниченное количество времени и сил и он будет тратить их на тех людей, которые с большей вероятностью помогут ему добиться успеха. Для управления своим начальником вам нужно получить его время и силы. Очевидно, что руководитель будет больше уважать пожелания «звезды», чем бездельника.

Анекдот о повышении зарплаты

Группа системных администраторов разговаривает о недавнем повышении зарплат. Человек, который не получил большого повышения, пожаловался на того, кто, по слухам, получил очень хорошую прибавку.

Он сказал: «Этот парень всегда получает больше прибавки, потому что он просто делает все, что говорит ему начальник».

Кто-то ответил: «А как у тебя работает стратегия узнай-чего-хочет-твой-начальник-и-сделай-наоборот?»

Управление – это как рулить лодкой, в которой гребут другие люди. Поворот руля задает лодке правильное направление, но кто-то должен трудиться, чтобы достичь цели. Вы можете подумать, что управлять вами – работа начальника, но обратное также справедливо. Вы должны управлять своим руководителем, направляя его так, чтобы быть счастливым.

Пример: удовольствие для мечтателя

Один системный администратор пришел в университет, чтобы исправить нестабильную, неоднородную сеть, у которой нужно было модернизировать самую основу: приобрести качественные кабели, современные коммутаторы и маршрутизаторы, обеспечить единообразную конфигурацию ОС и т. д. Однако декан считал себя возвышенным человеком и не интересовался такими приземленными проектами. Ему нужны были футуристические проекты, которые обеспечат статус, например, системы видеосвязи для рабочих станций и системы виртуальной реальности. Но ни один из этих проектов не мог быть реализован, пока не была выполнена модернизация основ. Системный администратор не мог добиться исправления фундаментальных проблем, пока не начал показывать их декану как шаги, необходимые для достижения его футуристических целей. Он объяснил декану, как он собирался помочь ему достичь успеха, а это были шаги к достижению цели.

Теперь мы можем поговорить об управлении вашим начальником. Первый элемент – поставить его в известность о ваших потребностях. Руководители не могут читать ваши мысли, поэтому не расстраивайтесь, когда они не угадывают, что вам нужно. С другой стороны, начальник думает не только о вас. Уважайте это, не переходите рамки терпимости и не надоедайте ему. Найдите равновесие.

Одна из потребностей, о которой вы должны напоминать ему один-два раза в год, – это ваш карьерный рост. Это не должен быть 20-страничный документ, разъясняющий причины вашей просьбы, но нельзя и упоминать об этом невзначай.

Направляйте на себя повышения

Том утверждает, что он никогда не получал повышения, которого непосредственно не просил. В колледже он был студентом-оператором университетского компьютерного центра. Однажды он пришел в офис директора и сказал: «Я хочу, чтобы вы знали, что я мечтаю быть здесь одним из студентов-руководителей и сделаю все возможное для получения этой должности». В конце учебного года ему сказали, что если он все лето будет усердно работать и безупречно себя вести, то получит повышение до следующего учебного года. Он работал усердно, вел себя безупречно и получил повышение[1]. История повторялась на его следующих местах работы.

Предложение руководителю идеи означает, что, когда представится подходящий случай, вы будете хорошим потенциальным кандидатом. Хороший руководитель сразу начнет тренировать вас, чтобы подготовить к этой должности, пробовать вас и смотреть, подаете ли вы надежды на успешное выполнение обязанностей той должности, которую попросили. Руководитель может задать вашей работе и обучению правильное направление.

Если вы не определились в своих карьерных целях, то должны сообщить о техническом навыке, который хотите развить. Если вы хотите остаться на текущей позиции, убедитесь, что и об этом вы сообщили своему начальнику!

Другой прием направления – позволить своему начальнику помочь вам с управлением временем. Когда у вас совершенно перегруженный график и работе не видно конца, позвольте своему начальнику установить приоритеты. Не жалуйтесь на то, что вы перегружены. Руководители весь день слышат жалобы, и не стоит повторять их лишний раз. Вместо этого покажите свой список задач с пометками, сколько времени займет каждая из них. Объясните, что общее время, необходимое для этих проектов, – больше, чем ваш 8-часовой рабочий день (40-часовая рабочая неделя), и попросите помочь установить приоритеты задач списка.

У типичного руководителя может быть несколько положительных реакций. Во-первых, обращение к мудрости начальника – это своего рода комплимент. Во-вторых, это радует руководителя, потому что, после того как он целый день получал одну эгоистичную просьбу за другой, вы придете к нему с сообщением:

[1] Ему помогло, что у него был хороший начальник.

«Шеф, я хочу выполнить ваши наиболее важные задачи, скажите мне, что это за задачи». Это может быть очень освежающим! Наконец, это предоставляет вашему руководителю явный обзор того, какую работу вы выполняете. Ваш руководитель может заметить задачи, которые должны быть полностью устранены, или может снизить вашу нагрузку, передав задания другим людям из вашей группы. Может быть, другой сотрудник группы сообщил руководителю, что ему хотелось бы больше заниматься определенной работой, и для вашего начальника это будет прекрасной возможностью дать ему такую работу.

Наконец, мы хотели бы обсудить принцип **передачи работы вверх**, или передачи задач своему начальнику. Некоторые задачи подходят для такой передачи, но другие – нет. Ваш руководитель должен заниматься управлением лодкой, а не греблей. Не передавайте вверх рутинную работу. Однако передача вверх приемлема для любой работы, для которой, по вашему мнению, у вас нет полномочий. Создание задачи для вашего начальника наиболее целесообразно, если для ее решения требуется право вашего начальника устранять другие задачи. Например, кому-то может быть трудно принимать решения в той ситуации, когда каким-то людям нужно делать резервные копии на неподдерживаемом оборудовании. Однако у вашего начальника могут быть полномочия создать правило, что резервное копирование выполняется только для официально поддерживаемых серверов, а все остальные запросы считаются проектами по развитию новых возможностей, которым устанавливается приоритет и которые финансируются или отклоняются так же, как и все запросы на обеспечение новых возможностей. Пользуясь своими полномочиями создать или изменить политику, начальник сможет устранить из вашей работы целый класс запросов или добиться приемлемого финансирования запроса.

При необходимости пользуйтесь властью своего начальника

Группа системных администраторов, ответственная за установку компьютеров, не укладывалась в сроки выполнения из-за роста запросов на индивидуальную конфигурацию. Эти особые запросы требовали огромных затрат времени. Оказалось, что многие из этих запросов не связаны с корпоративной работой. Одна из просьб к группе системных администраторов была сконфигурировать MIDI-карту (контроллер синтезатора), а это не требовалось человеку по работе. Другая просьба заключалась в создании компьютера с возможностью загрузки двух операционных систем, одна из которых не поддерживалась официально, но для нее существовали лучшие игры. Системные администраторы передали своему начальнику задачу поговорить с директором пользователей и разрешить ситуацию. Он объяснил, что системным администраторам не платят за помощь персоналу с их увлечениями или детскими забавами. Руководитель смог воспользоваться своими полномочиями, чтобы сэкономить время для целой группы системных администраторов.

Иногда кажется, что передача работы вверх приемлема, но в некоторых ситуациях это не так. Например, когда ваш руководитель просит вас что-то сделать, ответ «Нет, я считаю, что это ваша работа» всегда выглядит как неподчинение.

Например, если руководитель просит вас представить людям презентацию по определенной теме, ответ «Лучше сделайте это сами» будет неприятным. Более правильный ответ – сказать, что, по вашему мнению, презентация лучше дойдет до людей, если ее будет представлять человек с высокой должностью. Это использование авторитета начальника. (Тогда вас могут попросить написать презентацию, но представлять ее будет начальник).

Передача работы вверх создает больше работы вашему начальнику, который обычно склонен к передаче работы вниз. Следовательно, будьте осторожны с количеством и временем попыток передавать работу вверх. Не делайте их постоянно, не делайте их в неподходящий момент или во время оживленной дискуссии.

Очередь задач, передаваемых вверх

Когда нужно просить о чем-то вашего начальника? Выбрать подходящее время – это самое главное. Вы можете помнить список задач, которые хотите попросить выполнить, и выбирать из них наиболее важную, когда вас хвалят. Руководителю трудно отклонить разумную просьбу, сделанную сразу же после того, как он похвалил вас за хорошую работу или поблагодарил за экономию денег компании.

32.3. Дополнительная литература

Привычки, рассмотренные в этой главе, трудно развить. Книги и курсы могут помочь. Будьте готовы к небольшому напряжению вначале, но убедите себя в том, что со временем все будет проще. Однажды вы заметите, что развили привычку, не осознавая этого.

Навыки общения, ведение переговоров и доведение работы до конца часто являются темой книг для продавцов. Вам может быть полезно прочесть такие книги и применять полученные знания в своей карьере. Классические книги *«The One Minute Sales Person»* (Johnson 1991) и *«The One Minute Manager»* (Blanchard 1993) полны советов, которые подходят для системных администраторов.

Есть много прекрасных книг по организации и установке целей. Одна из них – *«Organizing from the Inside Out»* (Morgenstern 1998).

На рынке есть много книг по управлению временем. *«Getting Things Done»* Аллена (Allen 2002) очень популярна, не говоря уже о книге Тома *«Time Management for System Administrators»* (Limoncelli 2005)[1].

Если вы никогда не читали самоучитель, вам может быть трудно поверить, что куча бумаги с текстом способна решить ваши проблемы. Позвольте прямо здесь снизить ваш скептицизм. Самоучители – это здорово! Однако будьте реалистом: изменить себя сможете только вы сами. Книги лишь дают предложения, советы

[1] Томас Лимончелли «Тайм-менеджмент для системных администраторов». – Пер. с англ. – СПб.: Символ-Плюс, 2007.

и новый взгляд на то, что вы все время видели. Не каждая книга вам подойдет. Возможно, подача автором материала, конкретные проблемы, рассматриваемые в книге, или стиль написания вам не подходят. Вот почему можно найти десяток самоучителей по любой теме с различными стилями, подходящими разным людям. Кроме того, мы рекомендуем, чтобы вы критически оценивали предлагаемые советы, прежде чем их пробовать. Критически относитесь к любой книге, которая заявляет, что устранит все ваши проблемы. Если она кажется слишком хорошей, чтобы это было правдой, возможно, так оно и есть. Любое изменение поведения требует определенной работы, поэтому не верьте книгам, в которых утверждается обратное. Если она требует от вас, чтобы вы распространяли полученные знания среди других людей, мы бы задумались, так как подходу, который работает эффективно, не нужна схема пирамиды для распространения. Мы постарались рекомендовать классику, которая уже давно имеется на рынке: книги, доказавшие свою эффективность. Если вы все еще сомневаетесь в эффективности самоучителей, отложите книгу, которую читаете сейчас.

32.4. Заключение

Важно быть счастливым. Важно быть успешным. Эти принципы взаимосвязаны.

Успешные люди отлично доводят работу до конца и ни о чем не забывают благодаря составлению письменных или электронных списков задач и календарей. Это предотвращает забывание задач или пропуск встреч и предельных сроков выполнения.

Управление временем – это дисциплина, которая помогает вам выполнять свои наиболее важные задачи. Системным администраторам трудно управлять своим временем, потому что очень заманчиво создать рабочий процесс, управляемый прерываниями. Если системные администраторы хотят добиваться своих целей, они должны их ставить. Планировать свой день – хороший способ не сбиваться с пути. Эффективное чтение электронной почты может вдвое снизить ваше время обработки почты. Для того чтобы оставаться сосредоточенным, также требуется дисциплина. Если что-то имеет самый высокий приоритет, сконцентрируйтесь на этом, пока задача не будет выполнена. Заполните время ожидания другими приоритетами. Нахождение свободного времени – вопрос устранения задач, на которые бесполезно тратится время, а не более эффективного управления ими или их выполнения.

Мы рассмотрели такие навыки общения, как я-утверждение, которые позволяют вам заставить других услышать вас, зеркальные утверждения для подтверждения того, что вы понимаете людей, отражение, чтобы общаться с эмоциональными людьми, и обобщающие утверждения, чтобы убедиться, что члены группы едины в понимании. Эти навыки помогают людям справиться с четырьмя типами проблем в мире: моими, вашими, нашими и проблемами других людей. Эти навыки общения полезны в вашей работе, но также они являются ключом к вашей личной жизни. На самом деле этим навыкам обучают в семейных психологических консультациях. Мы надеемся, что чтение этого раздела улучшит ваши отношения на работе и вне нее.

Ведение переговоров предполагает, что вы будете просить то, что вам нужно, и бороться за достижение взаимовыгодных ситуаций. Вы должны знать о соот-

ношении сил и уметь его изменить, если вы не находитесь в более сильном положении.

В этой постоянно меняющейся высокотехнологичной области особенно важно профессиональное развитие. Однодневные курсы обычно являются тактическими (навыки), недельные конференции, как правило, стратегические (видение). Все они полезны и важны.

Мы хотим, чтобы вы любили свою работу и были счастливы. Это означает поддержание хорошего душевного здоровья, снятие стресса, принятие критики и заботу о себе. Пропуская отпуск, вы не помогаете никому.

Управление вашим начальником – это элемент обеспечения вашего счастья. Оно включает внимание к его приоритетам, чтобы он уделял внимание вашим. Стремитесь к успеху своего руководителя. Допустимо передавать своему начальнику задачи, требующие использования его права решать проблемы для многих людей, которые работают на него.

Среднестатистический человек проводит бóльшую часть времени бодрствования на работе. Вы заслуживаете счастья, когда находитесь там.

Задания

1. Представьте, что вы выиграли в лотерее и вам больше не надо работать. Чем бы вы занимались? Почему вы не занимаетесь этим сейчас? Как вы можете заниматься этим сейчас?
2. Что вы делаете для обеспечения доведения работы до конца?
3. Какая доля вашего рабочего дня приходится на прерывания? Что вы можете сделать, чтобы изменить прерывистый характер своей работы?
4. Каковы ваши цели на следующий месяц, год и пять лет?
5. Как вы проводите первый час своего рабочего дня? Что вы можете сделать, чтобы он стал более продуктивным?
6. Как вы работаете со своей электронной почтой? Какой стратегией вы пользуетесь для ее фильтрации?
7. Какое обучение управлению временем вам доступно?
8. Какие задачи вам приходится выполнять ежедневно или еженедельно? Когда вы их выполняете?
9. Назовите три задачи с низким приоритетом, которые вы можете исключить из вашего списка задач.
10. Назовите три задачи, на которые бесполезно тратится ваше время и которые вы можете устранить.
11. Какое обучение навыкам общения и межличностного взаимодействия вам доступно?
12. Насколько вы уверены в своих навыках ведения переговорах? Сколько переговоров вам приходится вести? Как вы можете развить свои навыки?
13. Опишите свои последние переговоры и то, что вы могли сделать для их улучшения.
14. Каковы ваши основные направления профессионального развития? Какую поддержку в этом вы получаете от своего работодателя?
15. Вы оптимист или пессимист? Приведите два примера.

16. Насколько у вас на работе принимается открытое обсуждение личной жизни? Если у вас на работе это не приветствуется, к кому вы можете обратиться за поддержкой при необходимости? Является ли ваше рабочее место безопасным?
17. Опишите свою сеть поддержки.
18. Когда вы в последний раз были в отпуске? Читали ли вы во время отпуска электронную почту, связанную с работой? Обещали ли вы не читать электронную почту во время своего следующего отпуска?
19. Потратьте 15 мин на создание своей Доски почета.
20. Соответствуют ли ваши приоритеты приоритетам вашего начальника? Откуда вы это знаете? Как вы обеспечиваете это соответствие?
21. Какого следующего повышения вы хотите? Кто знает, что это ваша цель?
22. Когда кто-то, попросивший вас что-то сделать, стоит в вашем офисе, пока вы это не выполните, делает ли этот человек то, что рекомендовано в разделе 32.1.2.9?
23. Опишите последний раз, когда вам потребовалась передача работы вверх. Как отреагировал ваш руководитель? Что вы сделаете в будущем, чтобы это улучшить?
24. Какой ваш любимый самоучитель?

Глава 33

Советы техническим руководителям

Технический руководитель (директор) – это человек, который глубоко понимает принципы работы системного администрирования. Он знает, что включает в себя деятельность организации и работа с клиентами. Возможно, он когда-то был главным системным администратором, но теперь переведен на руководящую должность. Возможно, он все еще участвует в некоторых технических аспектах деятельности организации. В его обязанности входит курирование неопытных системных администраторов и помощь им в развитии как технических знаний, так и навыков общения. Его технический персонал надеется, что он справится с бюрократией и другими препятствиями, которые могут возникнуть на их пути, чтобы они могли сосредоточиться на технических задачах.

Кроме того, технический руководитель работает с нетехническими руководителями как в своей цепи управления, так и по всей компании. Предполагается, что он сможет хорошо общаться как с нетехническими руководителями, так и со своим техническим персоналом. Он играет роль буфера и переводчика между этими двумя группами.

33.1. Основы

Для того чтобы быть успешным техническим руководителем, вам понадобится понимание того, как следует работать и с нетехническими руководителями, и с вашим техническим персоналом. Ваш технический персонал будет считать самым важным то, как вы с ними обращаетесь. Если вам не удастся добиться от них уважения или вы не будете помогать им, когда это необходимо, группа распадется на части. Если вам не удастся найти общий язык с нетехническими руководителями, вы не сможете установить для вашей группы реальные цели, сроки и ресурсы, а также не сумеете создать хорошее представление о вашей группе в компании. Эти проблемы также непосредственно касаются вашей группы.

В этом разделе мы рассмотрим, как успешно работать одновременно и с техническим персоналом, и с нетехническими руководителями в компании. Мы рассмотрим некоторые из ваших обязанностей как технического руководителя и подготовим вас к тем решениям, которые вам придется принимать на этой должности.

33.1.1. Обязанности

Главная обязанность технического директора – определять приоритеты и предоставлять ресурсы, необходимые для достижения тех целей, которые были выделены как приоритетные. Технический директор отвечает перед своим персоналом, компанией и самим собой. Он должен сохранять на высоком уровне моральный дух своей группы и поддерживать членов группы во всех их начинаниях. Он должен заботиться о развитии их карьеры и помогать им улучшать свои технические навыки. Ему необходимо задавать концепцию группы, поддерживать сосредоточенность людей на правильном направлении. Он отвечает за то, чтобы компания имела хорошую производительность, не выходя из бюджета. Он должен управляться со всем этим и при этом сохранять рассудительность и не отставать от современных технологий. Также он должен следить за тем, что делают его сотрудники, не вставая у них на пути.

33.1.1.1. Приоритеты и ресурсы

Теоретически, если директор дает персоналу список задач по приоритетам и достаточное количество ресурсов для их реализации, все будет замечательно. Если бы это было так просто!

Приоритетные направления обычно приходят от нетехнического руководства технического директора. Затем технический директор определяет необходимые ресурсы и работает со своим руководством, чтобы получить эти ресурсы.

Один из способов информировать о приоритетных направлениях – устанавливать SLA для всех предоставляемых служб. Это сформирует ожидания. Например, в SLA для службы поддержки может быть указано, что запросы, сделанные по электронной почте, должны быть подтверждены и распределены по категориям в течение 15 мин в рабочее время, и установлено ожидаемое время выполнения для различных категорий запросов. Для построения системы электронной почты SLA должно включать требования к продолжительности работы, количеству писем, которое система должна быть способна передавать и получать каждый день, и к времени интерактивного отклика для операций, таких как чтение нового сообщения.

Другой способ информирования о приоритетах – иметь письменные политики для руководства группой системного администрирования. Мы считаем наиболее важными следующие три политики.

1. *Как получить помощь.* Эта политика показывает пользователям, как получить лучшее обслуживание и где они могут его получить. Также она помогает вашей группе, предоставляя членам группы возможность направлять людей в службу поддержки, когда те обращаются к ним не так, как следовало бы, то есть из дома, в нерабочее время либо когда пользователь должен был напрямую обратиться в службу поддержки (см. раздел 13.1.6).
2. *Состав и объем работ* определяет, кто, где и над чем работает. Какие виды машин/служб поддерживаются? Посещают ли системные администраторы пользователей на дому? Предоставляют ли они поддержку на рабочем месте или люди должны приносить свои компьютеры системным администраторам? Что делают системные администраторы при просьбе обслужить неподдерживаемые системы? Этот документ важен, так как он говорит системным администраторам, над чем им стоит работать, и уполномочивает их отвечать «нет» на любые другие запросы (см. раздел 13.1.5).

3. *Определение экстренного случая* помогает системным администраторам отличать факт от вымысла. Наличие письменной политики помогает системным администраторам определить, что такое экстренный случай на самом деле. Все остальное не является экстренным случаем (см. раздел 13.1.9).

33.1.1.2. Структура

Ваша работа как директора также заключается в предоставлении структур, которые помогут людям достигнуть их целей. Часто это является более важным с менее опытным или менее технически грамотным персоналом, от которого не ожидается самостоятельности.

Использование контрольных списков, чтобы убедиться в том, что новые компьютеры правильно установлены, – пример структуры, которая позволяет людям добиться их целей (см. главу 3). Для неопытных системных администраторов вы можете составить контрольный список, определить в нем действия, которые каждый из них должен выполнить, и просматривать завершенные контрольные списки. Опытные системные администраторы должны сами составлять собственные контрольные списки и процедуры, но у вас могут быть дополнения, когда первый набросок контрольного списка будет готов.

33.1.1.3. Моральный дух группы

Технический директор должен стараться поддерживать моральный дух группы на высоком уровне. Если его уровень высок, члены группы будут мотивированы решать еще более трудные задачи, будут наслаждаться своей работой, работать как одна команда, а текучесть кадров будет ниже. Нанимать новый персонал будет просто. С другой стороны, когда моральный дух на низком уровне, продуктивность группы уменьшится, а утечка кадров увеличится. Также будет сложнее нанять новый персонал, поскольку соискатели будут чувствовать низкий моральный дух группы и не захотят быть ее частью. Большинство групп находятся где-то между этими двумя крайностями, и поведение членов группы также располагается где-то между ними. Они не стараются ни совершать подвиг, ни совсем ничего не делать. Если технический директор хорошо выполняет свою работу, моральный дух группы будет высоким. В разделе 34.1.2 вопросы морального духа рассмотрены более подробно.

33.1.1.4. Устранение препятствий

Другой способ предоставить ресурсы вашей группе – заново начать застопорившиеся процессы и устранить препятствия, которые не дают завершить работу. Другими словами, смажьте колеса.

Есть несколько способов оживить застопорившиеся процессы. Иногда между людьми нет связи и вы можете соединить двух правильных людей. Порой не принимаются решения, часто люди не уверены в правильности курса, не считают себя уполномоченными или погрязли в бесконечных спорах. Вы можете выступить посредником и заново озвучить ваше видение, уполномочить людей принять лучшее решение или сообщить о приоритетах для окончания спора. Все это – вопросы общения, и разрешать их – ваша работа.

Важно быть хорошим слушателем, так как проблемы часто решаются сами собой, когда вы просто выслушиваете вовлеченных людей. Например, проекты могут быть застопорены, потому что люди не знают, что им делать, и вы на самом

деле тоже. Однако вы можете вмешаться и выслушать, как люди опишут ситуацию. Принуждение людей объяснить проблему третьему лицу (вам) заставит их тщательно обдумать проблему. Решение часто становится очевидным, даже если вы не понимали, о чем они говорили. Лучше всего дать им обсуждать вопрос, пока решение не станет ясным как для них, так и для вас.

Устранение препятствий обычно включает в себя нетехнические, бюрократические задачи, тогда у персонала будет больше времени сосредоточиться на том, для чего они были приняты на работу: на отдельных технических задачах. Например, вы можете внести ясность в политику, договориться с руководством о финансировании проекта, заказать средство, позволяющее экономить время, или уполномочить людей говорить или делать что-то, если они сомневаются, должны ли они это выполнять.

Новые технические директора часто жалуются, что чувствуют себя так, как будто ничего не делают, поскольку они привыкли иметь материальные результаты – установленные машины, написанные строки кода, – но их новая должность более «простая». Вы можете весь день заниматься созданием связи между людьми, устранять препятствия и заставлять людей заниматься делом, но не иметь осязаемого результата выполненной работы. Однако такова природа вашей работы.

Часто возникают дискуссии по поводу того, как решить проблему между теми, кто хочет применить временное решение, и сторонниками долгосрочного или постоянного решения. Хороший способ разрешить такую ситуацию – остановить обсуждение и перейти к мозговой атаке для поиска наилучшего постоянного решения. Как только оно будет найдено, устройте мозговую атаку по поиску «достаточно хорошего» решения, чтобы применять его, пока вы не будете готовы к реализации постоянного решения. Разбиение процесса на две части поможет группам лучше сконцентрироваться. Обсуждение постоянного решения в первую очередь устраняет рассеянность, вызванную необходимостью держать в голове насущные проблемы. Это еще один способ, при помощи которого директор может обеспечить структуру для достижения группой своих целей.

Директор должен решить, будет ли лучше пропустить какое-либо решение или же применить их оба. Есть огромная вероятность, что оба решения будут выполнены, если группа большая и над каждым из решений будут работать различные люди.

Реализуйте краткосрочное и пропустите долгосрочное решение, если группа восстанавливается после аварии (см. главу 2) или ограничена в ресурсах. Как только ситуация стабилизируется, вы можете вновь подумать о долгосрочном решении. Может быть, к тому времени сменится персонал и появятся новые люди со свежими идеями.

С другой стороны, краткосрочные решения иногда так сильно влияют на не полностью укомплектованную группу, что важные долгосрочные решения никогда не начинают применяться. Это плохо. Старая пословица гласит: «Нет ничего более постоянного, чем временное решение».

Может быть лучше пропустить краткосрочное решение, так чтобы группа смогла сосредоточиться на долгосрочном решении, если она перегружена, недоукомплектована, переживает слишком много других кризисов или имеет проблемы с завершением проектов. Спросите группу: «А что, если мы ничего не станем делать, пока не будем готовы к реализации постоянного решения?» Иногда группа бывает шокирована, когда обнаруживает, что это не так уж и плохо. Пользователи могут пострадать от месяца плохого обслуживания, но, может быть, они и так уже привыкли к плохому обслуживанию. Иногда пользователи

устанавливают свои обходные пути и могут кое-как справляться, пока не будет готово постоянное решение; это может быть лучше, чем неудобства от двух обновлений.

Анализ издержек может помочь определить, является ли долгосрочное решение целесообразным. Иногда вовлеченные технологии будут заменены через год, что делает краткосрочные решения довольно рациональными. Иногда как директор вы будете знать, что проект планируется закрыть и все преимущества долгосрочного решения будут сведены на нет.

Технический директор часто отвечает за поиск политического, стратегического или финансового решения. Рассмотрите решение проблемы с причины, а не следствия. Поднимитесь по цепи управления и решите проблему, меняя стратегию, устраняя запреты, финансируя замену или обновляя SLA для отражения реальной значимости ситуации.

Будучи техническими людьми, мы любим решать проблемы техническими методами: устанавливая новое программное обеспечение или используя те или иные технологии, чтобы попробовать контролировать ситуацию. Нельзя решить при помощи технологий социальные проблемы. Нельзя решить проблему грубости людей в общении по электронной почте, создав программное обеспечение, блокирующее грубые фразы; люди просто станут более изобретательными. Вы не можете уменьшить потребление бумаги, накладывая ограничение на количество страниц, которое может печатать каждый человек в день; вы обнаружите, что люди, которые превысили свой предел, будут докучать тем, которые его не превысили, с просьбами распечатать за их счет (в разделе 24.1.6 есть идеи получше).

33.1.1.5. Поощрения

Как руководитель вы должны поощрять ваш персонал. Поощрения – очень мощное средство. Однако, если ими злоупотреблять, это приводит к плачевным результатам. Более подробные объяснения вы можете найти в какой-нибудь книге по управлению людьми, кроме того, есть книги конкретно на данную тему (Nelson 2005). Мы хотели бы подчеркнуть некоторые моменты.

Потратьте время, чтобы выяснить, что мотивирует каждого человека в вашей группе. То, что является наградой для одного человека, – наказание для других. Все люди разные. Обратите внимание на то, что каждый человек в вашей группе воспринимает как поощрение. Делайте заметки на вашем КПК, если это поможет вам запомнить. Публичная благодарность за хорошо сделанную работу перед другими работниками будет очень значительным поощрением для некоторых сотрудников. Другие могут считать это слишком нескромным, а кто-то – наоборот. Одним из очень значительных поощрений для системных администраторов будут новые задания, которые им интересны. Каждому человеку интересны разные вещи. Возьмите на заметку, какие типы заданий каждый сотрудник будет рад выполнять. Обычно, это те задачи, которые они решают в первую очередь, когда им дают работать по собственным приоритетным направлениям. Кроме того, вы можете спрашивать людей, какими проектами им нравится заниматься.

Поощряйте поведение, которое вы хотите наблюдать. Никогда не поощряйте негативное поведение. Например, если член персонала привлекает ваше внимание, но делает это, посылая гневные, склочные письма вам и вашему персоналу, не отвечайте на письма. Это поощрило бы негативное поведение. Вместо этого отвечайте только тогда, когда человек использует правильную линию общения. Хотя для получения требуемого результата потребуется больше времени, этот

результат будет гораздо более долгосрочным. Опять же, вы должны помнить, что различные люди считают разные действия поощрением или наказанием.

Наказание за негативное поведение – это крайнее средство. Наказание за негативное поведение менее эффективно, чем поощрение положительного. Вспомните о том, как в детстве ваши родители наказывали вас за проступки. Не возникало ли у вас желания еще чаще так поступать? Наказание давало вам внимание, которого вы так желали, а это значит, что оно награждало вас.

Если вы обязаны ответить на негативное поведение, сделайте это таким способом, чтобы никоим образом не поощрять такое поведение. Возвращаясь к нашему примеру об электронной почте, вежливо ответьте, что такие комментарии должны быть высказаны при личной встрече. Если ваш ответ будет касаться содержания письма, вы дадите понять человеку, какого поведения ожидаете от него в будущем. Если он просто желал внимания, вы вознаградили его труды, дав ему это внимание.

От людей нужно ожидать того, что входит в их служебные обязанности. Они получают деньги за выполнение этой работы. Однако выход за пределы обязанностей должен поощряться надбавками и бонусами. Путать эти два принципа может быть опасно. Если вы даете людям бонус или надбавку за то, что они просто делают свою работу, они будут ожидать бонусов просто за то, что они делают то, за что им платят. Скоро в группе возникнет чувство, что им обязаны выплачивать надбавки.

Пример: бонусы – для особых дел

Компания раздавала ненастоящие деньги (Счастливые Деньги) тем сотрудникам, которые особенно хорошо выполняли свою работу. Счастливые Деньги можно было обменять на призы. Однако руководители начали раздавать Счастливые Деньги при выполнении практически любой задачи. В результате людей поощряли за выполнение дел, которые относились к их служебным обязанностям. Поэтому персонал начинал негодовать, если ему приходилось что-то делать без получения особой награды. Руководство ненароком приучило людей думать, что они должны получать особые поощрения за простое выполнение своей работы. Персонал стал неуправляемым. Когда программа Счастливых Денег была закончена, руководству пришлось потратить годы, чтобы восстановить надлежащее отношение к труду. Руководству нужно было проявлять сдержанность при выдаче Счастливых Денег и поощрять только особо выдающиеся поступки. Оглянувшись назад, руководство сделало вывод, что, если программа направлена на поощрение чего-то определенного, она должна поощрять только это, и ничто другое.

Пример: особые достижения заслуживают бонусов

Когда компания Bell Labs была разделена на AT&T и Lucent, системным администраторам пришлось проделать много сверхурочной работы, чтобы успеть вовремя разделить сеть. Они получили символические бонусы, когда проект был закончен (Limoncelli et al. 1997). Это пример правильного применения бонуса. Такой большой проект был нетипич-

ным и выходил за пределы их служебных обязанностей. Бонус был хорошо принят.

Если бы системных администраторов нанимали специально для разделения сети, поощрение было бы допустимо только за неожиданный успех, такой как завершение с опережением графика.

33.1.1.6. Наблюдение за группой

Технический директор отвечает перед компанией за наблюдение за группой и за знание того, чем занят каждый сотрудник. Некоторые технические директора практикуют еженедельные или ежемесячные отчеты как способ слежения за тем, чем все занимаются. Другие устраивают регулярные личные встречи с каждым сотрудником. Если вы устраиваете регулярные встречи, убедитесь в том, что не назначаете их чаще, чем может позволить ваша загруженность. Назначение встреч с последующей их отменой или опозданием на них вызывает раздражение и вносит в ваш коллектив дезорганизацию. Лучше назначить одну встречу в месяц, чем назначать их каждую неделю и появляться только на одной-двух в месяц.

Встречи предоставляют хорошую возможность диалога, который не состоялся бы без них. Директор может напрямую обратиться к некоторым проблемам или получить ответы на вопросы, которые сотрудник мог не поместить в отчет. Если директор требует отчетов, он должен убедиться, что имеет достаточное количество времени как для их чтения, так и для отклика на любые поднимаемые в них вопросы. Сотрудников раздражает и дезорганизует, когда их работу прерывают для написания отчета, который никто не прочитает. Кроме того, это будет пустой тратой средств компании.

Короткие периодические отчеты могут быть полезны для технического директора, чтобы ссылаться на них, когда ему необходимо определить, может ли его группа взять новый проект, или объяснить, почему у группы не хватает времени на что-либо. Тем не менее возможны и другие способы получения этой информации, например при помощи системы отслеживания запросов.

Пример: автоматизированные отчеты

Технический директор компании среднего размера, занимающейся программным обеспечением, получал автоматизированные отчеты о том, чем занимался его персонал, запрограммировав программное обеспечение для слежения за запросами, чтобы оно оповещало его о том, какие запросы члены его группы обновляли каждый день и как долго они работали над каждым из этих запросов. Он всегда имел возможность обсудить, чем занимается персонал в данный момент времени.

Другой технический директор в консалтинговой компании запрограммировал биллинговую систему, чтобы в первую очередь она посылала ему список тех часов, которые каждый из консультантов, трудящихся под его руководством, отработал в предыдущий день. Он всегда знал, у кого будет меньше часов в неделю, а кто работал всю ночь, даже если человек был в удаленной пользовательской организации.

> Еще один технический директор написал скрипты, показывающие ему в системе слежения запросы, которые не обновлялись за последние 24 часа, в дополнение к ежедневным отчетам. Он работал в интернет-службе, где запросы были чаще всего пользовательскими проблемами, а не долгосрочными проектами по обслуживанию.

Выяснение того, чем заняты ваши сотрудники, не отрывая их от работы для составления отчета, чаще предпочтительнее, чем периодические отчеты. Тем не менее такой подход сильно полагается на дисциплину, например части группы нужно регулярно обновлять запросы или вводить оплачиваемое время. Если люди не обновляют свои запросы, это также необходимая для вас информация; вы должны узнать, почему они этого не сделали. Есть большая вероятность, что с этими сотрудниками связана какая-либо проблема. Они могут быть перегружены, или у них низкий моральный дух, или у них плохие рабочие навыки. В любом случае вам следует с ними поговорить.

Собрания группы – также очень полезный способ наблюдать за тем, что происходит, и устраивать свободное обсуждение, чтобы каждый мог узнать, чем занимается любой другой. Для членов группы важно быть в курсе работы других людей, чтобы они могли внести свой вклад в другие проекты и знать, когда другой проект может повлиять на их собственные проекты.

Для директора важно следить за количественными показателями группы. Где-то в своей цепи управления технический директор отчитывается перед нетехническим директором. Для него важна возможность продемонстрировать хорошее знание, а также полное понимание и анализ количественных показателей своего подразделения, чтобы достичь согласия с руководством. Не имеет значения, насколько важными для себя считает технический директор количественные показатели; факт в том, что часть его работы – знать данные своей группы лучше, чем кто-либо еще, чтобы он мог эффективно взаимодействовать с руководством.

33.1.1.7. Поддержка

Технический директор поддерживает свою группу, выполняя бюрократические задачи и помогая людям в их взаимодействии с остальной компанией. Ему следует поддерживать их в работе, которой они занимаются. Он должен брать на себя вину за неудачи, ответственность за которые лежит на группе, отводить обвинения от подчиненных и не переводить вину за неудачу на личности, при этом, несмотря ни на что, ожидать от группы лучших действий в следующий раз. Ответственный человек должен негласно получить предупреждение, вместо того чтобы узнать о недовольстве директора спустя месяцы во время рассмотрения данных о производительности. С другой стороны, директор должен убедиться, что члены группы признаны и поощрены за свои успехи, а не присваивать все заслуги самому себе. Технический директор должен уметь получать удовлетворение только от вида того, его сотрудники состоятельны и успешны, а не от получения похвалы за их достижения.

Помимо этого, технический директор поддерживает свой персонал, принимая на себя ответственность за заключение контрактов и бюрократические задачи: подтверждение и обновление контрактов об обслуживании, ведение соглаше-

ниями о неразглашении (NDA) и заключение договоров с поставщиками и отделом поставок, когда это необходимо. Директор обычно имеет полномочия подписывать контракты от имени компании либо знает нужные каналы, по которым можно подтвердить такие контракты, в то время как технический персонал обычно не имеет такой возможности. Также подразумевается, что он умеет лучше вести переговоры, чем его сотрудники. Выполняя все эти действия, он позволяет своей группе сосредоточиться на технических задачах, на которых они специализируются и от которых получают удовольствие, и освобождает их от утомительной бюрократической волокиты. Если некоторые сотрудники заинтересованы в освоении этих навыков, директор должен помогать им советом и передать им часть своей работы.

Кроме того, он должен поддерживать свою группу, когда сотрудникам необходимо приводить в исполнение политику компании. Временами пользователям политика компании кажется неудобной. Для принятия политики были причины, и ее неисполнение определенно повредит компании. Если системным администраторам приходится говорить «нет» своим пользователям, это может показаться неубедительным. Если «нет» исходит от кого-то из высшего руководства, оно будет принято более охотно. В любом случае это снимает ответственность с системного администратора. Если кажется, что политику следует изменить, директор должен сам продвигать предложение либо помогать своему персоналу в его продвижении.

Пример: приведение политики в действие

Один технический директор говорил своему персоналу: «Ваше дело – сказать “нет”. Мое дело – это подтвердить». Если пользователь был недоволен некоторыми положениями политики компании, системные администраторы объясняли ему, почему существовала политика, и помогали этому пользователю удовлетворить свои нужды, что обычно можно было сделать другим способом, не противоречащим установленным правилам. Однако, если пользователь все еще был недоволен, системные администраторы могли быть уверены, что их директор объяснит, почему существует данная политика и почему ее будут приводить в действие. Это позволяло системным администраторам оставаться сосредоточенными на своих технических задачах, вместо того чтобы заниматься тем, что изначально является задачей бизнеса.

Пример: дайте мне побыть плохим парнем

Другой директор помогал своим системным администраторам преодолевать все бюрократические проволочки, представляя себя как плохого парня. Этот директор часто говорил своему персоналу: «Объясните это клиенту; если клиенту это не понравится, обвиняйте меня! Сделайте меня плохим парнем!» Это предоставляло системным администраторам средство, которое помогало им отводить гнев и сохранять лицо. Системные администраторы могли кому-то сказать: «Я понимаю ваше положение, но мой босс не разрешит мне, а вы знаете, какой он строгий». Достаточно много системных администраторов пользовались этой отговоркой,

которая в итоге широко распространилась. Корпоративные бюрократы не хотели иметь дело с этим таинственным директором и быстро отвечали на все запросы от группы. Хотя они никогда не общались с ним напрямую.

Такой подход может быть успешным до тех пор, пока им не злоупотребляют. Тем не менее он работает лучше, когда рассматриваемый пользователь – сотрудник другого подразделения, располагающегося на одинаковом уровне с подразделением системного администрирования или ниже. Если этот сотрудник находится на одном уровне с руководителем системного администратора или выше, мы советуем системному администратору обращаться к своему директору, чтобы он решил проблему напрямую и затем обратился к своему начальнику, если это необходимо. Если руководитель заработает репутацию человека, с которым невозможно работать, это может плохо сказаться на его карьере.

Защита политики может быть не лишена юмора

Защищать свою группу системного администрирования можно с юмором. Данное письмо было отправлено пользователям отдельной сети после серии перебоев.

Отправитель: Глава группы системного администрирования

Получатель: Пользователи сети

Тема: Проблема сетевого воровства

Мы хотим привлечь ваше внимание к серьезной проблеме, которая затрагивает всех нас.

Мы наблюдаем растущий уровень преступности в нашей сети. По крайней мере раз в неделю группа компьютерной поддержки пару часов занимается отслеживанием источника сетевого воровства.

Для всех случаев воровства мы нашли виновных, и что особенно нас потрясло – они всегда оказывались нашими коллегами по подразделению! А еще более шокирует то, что, будучи однажды уличенным, человек зачастую не испытывает никаких угрызений совести и имеет слабое представление о последствии своих действий для коллег.

О чем я говорю?

Для людей стало обычной практикой воровать IP-адреса без их регистрации. Они устанавливают компьютер, рабочую станцию или принтер и просто используют адрес, который, как они «думают», не занят. Позднее, когда системные администраторы распределяют адреса для новых устройств, мы обнаруживаем конфликтующий IP-адрес, который уже используется в сети.

Это каждую неделю приводит к пустой трате многих часов рабочего времени службы компьютерной поддержки и затрагивает пользователей вследствие отказа систем.

Недавно мы даже столкнулись с тем, что люди используют адреса, которые зарезервированы критически важными серверами, принтерами, компьютерами других людей и т. п.

Это имеет такое же действие, как если бы кто-то подошел к чужому компьютеру и отключил от него сетевой кабель. Это затрагивает хозяина компьютера, а компьютерная группа теряет часы на отслеживание преступника, отвлекаясь от НАСТОЯЩЕЙ работы.

Пожалуйста, получите IP-адрес у компьютерной группы ПЕРЕД тем, как устанавливать любое новое устройство в сети. Ваши коллеги будут вам благодарны.

Спасибо.

P.S. Если вы работаете в лаборатории, где вам необходима динамическая установка и удаление систем, мы предоставим вам блок IP-адресов, которые вы можете изменять, или даже обеспечим вам собственную конфигурацию DHCP.

Вы легко можете сами составить подобное сообщение, взяв это за основу. На самом деле это сообщение было изначально написано Ральфом Лоурой и с того времени использовалось для множества различных случаев.

33.1.1.8. Идейный лидер

Технический директор также несет ответственность за направление деятельности группы. Он должен знать, куда направлена деятельность группы и каковы ее задачи. Выбор правильного направления для группы требует понимания курса компании в целом и определения того, как группа может помочь компании достичь ее целей. Директор должен напоминать группе о ее целях, чтобы помогать людям концентрироваться. Эти задачи должны включать как долгосрочные цели, так и краткосрочные контрольные точки, чтобы системные администраторы могли видеть прогресс, которого они добиваются при продвижении к цели группы по направлению деятельности компании. Контрольные точки могут быть ежегодными или ежеквартальными задачами группы. Директор должен удерживать твердый курс, поскольку сотрудникам нужна уверенность в том, что направление их деятельности устойчиво. Системные администраторы ненавидят, когда они в первый день они вынуждены следовать к точке А, а во второй – к точке Б, особенно если точки А и Б расположены в противоположных направлениях. Из-за повседневных проблем таких ситуаций становится больше, и бывают такие случаи, когда может показаться, что краткосрочное решение противоречит последним указаниям директора. Он должен уметь объяснить, что то, что кажется сменой направления, на самом деле является этапом на пути к долгосрочной цели.

Пример: объяснение решений, которые кажутся противоречащими направлению

У технического директора организации поддержки пользователей был штат, состоящий из восьми специалистов по поддержке пользователей

(Customer Support Engineer – CSE), поддерживающих более 180 пользователей и более 200 технологических и торговых партнеров. Поддерживаемый программный продукт был настолько сложным, что требовалось по меньшей мере 4 месяца, чтобы ввести CSE в курс дела. Директор установил, что запросы партнеров о поддержке их собственных систем имеют меньший приоритет, чем запросы пользователей и партнеров от лица пользователей. Через неделю после того, как он начал следовать этому направлению, он обнаружил, что компания ведет переговоры о крупной партнерской сделке и для запросов от этого потенциального партнера должен быть установлен более высокий приоритет. Ему нужно было сообщить это его группе, не давая при этом им повода думать, что направление деятельности группы поменялось.

Сначала он сказал группе, что этот потенциальный партнер не пользуется преимуществом перед пользователями, которые уже внесены в список обслуживания, чтобы подтвердить решение, принятое и поддерживаемое руководством. Потом он объяснил, что, хотя пользователи и важнее партнеров, этот конкретный партнер был готов заключить с ними соглашение, которое позволит им присоединиться к организации с десятками пользователей. Чем больше этот партнер узнает предварительно, тем больше запросов он сможет обслуживать в пользовательских организациях и тем меньше он будет зависеть от CSE в будущем. Это определенно приведет к лучшей поддержке пользователей. CSE понимали решение в контексте. В представлении группы это было краткосрочным исключением, не противоречащим общим установкам.

За исключением тех случаев, когда компания путается и постоянно меняет свой курс, привязка курса вашей группы к курсу компании должна придать уверенности в том, что выбранное вами направление деятельности может оставаться постоянным и непреклонным с течением времени. В компаниях, которые сбиваются с курса, выбор того, что понимается под локально стабильным курсом, может сберечь группу системного администрирования от падения морального духа, вызванного отсутствием стабильности в компании. Тем не менее директору следует искать баланс между необходимостью защищать свою группу и держать своих сотрудников в курсе событий, если кажется, что компания скоро развалится. К управлению деятельностью людей относится также помощь им в уходе из компании в подходящее время.

33.1.1.9. Подготовка

Технический директор также отвечает за подготовку своей группы. Он должен помогать людям развиваться в профессиональном и техническом плане. Хорошему наставнику нужно недюжинное терпение. Люди учатся разными способами и с различной скоростью, но большинство из них не научатся быстро, если человек, обучающий их, открыто показывает свое недовольство. Подготовка подразумевает под собой время, уделенное на объяснение людям того, что нужно делать и почему, а также на пребывание с людьми, когда им необходима помощь. Это значит, что им нужно указывать на их собственные ошибки и помогать на них учиться, при этом не давая им повода думать, что они в чем-то неполноценны. Это подразумевает, что им нужно уделять время. Как правило,

неопытным системным администраторам больше всего нужно обучение. С опытом вы можете научиться давать людям невероятно сложные задачи, чтобы они развивали свои навыки, позволяя им ошибаться, но воодушевляя их продолжать работу. Если они время от времени перестают ошибаться, значит, вы поднимаете сложность слишком медленное.

Значительной частью подготовки является делегирование. Системное администрирование означает управление машинами и сетями, а делегирование означает передачу контроля другим. Это противоположные навыки, и поэтому многим системным администраторам при обучении делегированию нужна особая помощь.

При выдаче сотрудникам особо сложных заданий вам следует позволять им совершать ошибки и поддерживать их, а не злиться на них. Помните, если бы люди знали, что им делать, они делали бы это без вашей помощи. Вы здесь, чтобы помочь им с их проблемами. В противном случае вы будете похожи на автомеханика, который жалуется на то, что люди привозят в его мастерскую только сломанные машины.

Дайте людям учиться на ошибках

Однажды Том готовил двух инженеров, которые собирались обновить Ethernet-соединение между двумя маршрутизаторами с 10 Мбит (медный кабель) до Fast Ethernet 100 Мбит (оптоволокно), и маршрутизаторы находились в различных частях здания. Он посоветовал этим двум инженерам пойти в серверную и имитировать замену (см. раздел 18.2.5), чтобы убедиться, что все нужные разъемы были доставлены и что оптоволокно было необходимой длины. Он делал это перед их глазами при выполнении предыдущих проектов. Они посмеялись над Томом после такого предложения, и Том почувствовал, что они не собираются следовать его совету. Когда пришло время ремонта, они обнаружили, что разъем на их оптоволоконном соединительном кабеле был неправильным. Ремонт пришлось перенести.

Том мог проверить все сам за их спиной. Он также мог проводить их до серверной для проведения всех тестов. И то и другое было бы оскорбительным и неприятным для их морального состояния. Вместо этого он убедился в том, что проект не очень важен и может быть отложен на неделю или около того и это никак не повлияет на другие проекты, если что-нибудь пойдет не так. Эти два техника были взрослыми людьми и сумели извлечь урок из своей ошибки. Том заметил, что в последующих проектах они всегда имитировали такие замены без дополнительных просьб.

Когда люди злятся на кого-нибудь, кто обучается, обычно это вызвано тем, что они считают себя очень хорошо подготовленными и общение с людьми, которые таковыми не являются, может их очень раздражать. Опытные системные администраторы знают, что они хорошо подготовлены: они знают технологический процесс, хорошо в нем разбираются и даже разработали несколько интересных маленьких улучшений, которые повысили производительность процесса. Эти системные администраторы знают все «горячие» клавиши на клавиатуре. Очень сложно и неприятно наблюдать за кем-нибудь менее опытным, который неуме-

ло постигает технологический процесс. Но на то, чтобы эти системные администраторы стали такими прекрасно подготовленными, потребовалось очень много времени, и им необходимо дать время начинающим системным администраторам, чтобы те достигли таких же высот. Им может потребоваться больше времени, чем нам, потому что мы так совершенны, но они однажды *станут* прекрасными специалистами. Вспоминайте это всегда, когда вы забываете о скромности.

Порой вы будете сталкиваться с тем, что человек, которого вы обучаете, кажется просто неспособным понять вопрос, вне зависимости от степени ваших стараний. Попробуйте понять, где находится затруднение и как этот человек себе его представляет, а затем начните ваше обучение в соответствии со своим пониманием. Всегда делайте все возможное и предполагайте, что у вас проблема общения, которую необходимо разрешить, вместо того чтобы сдаваться или становиться раздражительным. Время от времени вы будете сталкиваться с людьми, которые учатся гораздо медленнее, чем вы бы того хотели. Соответственно, измените свои ожидания по данному вопросу, но не прекращайте попыток. Со временем ученик будет понимать все больше и больше. Некоторые люди лучше всего учатся в одиночестве.

Учите людей документировать свое обучение. Это помогает закрепить процесс обучения и создает образовательную базу. Даже копирование и вставка того, какие команды нужно выполнить для завершения задачи, лучше, чем отсутствие документации вообще.

33.1.1.10. Техническое развитие

Технический директор несет ответственность за то, чтобы его старшие системные администраторы развивали свои технические навыки и были в курсе последних разработок. Он добивается этого несколькими способами. Он делегирует им большие и сложные задачи, в которые в ином случае напрямую был бы вовлечен он сам. Он обеспечивает, чтобы они посещали важные конференции, и советует им писать статьи и другими способами принимать участие в этих конференциях и деятельности иных технических групп. Некоторые компании выделяют каждому человеку определенное количество денег и времени на профессиональное развитие. Для системного администратора важно каждый год уделять профессиональному развитию около 40 ч. Технический директор несет ответственность за то, чтобы его руководство понимало значение профессионального развития и достаточно его финансировало.

Также техническому директору стоит работать со своими сотрудниками над тем, чтобы они выжимали максимум из этих денег и делились обретенными знаниями с остальной группой. Он должен быть уверен, что группа или подразделение имеет в наличии обширную библиотеку технических книг, к которой могла бы обращаться. Он также должен находить возможность привлекать своих старших системных администраторов к проектам в других областях, в которых они заинтересованы, чтобы помочь им расширить свой кругозор.

33.1.1.11. Карьерный рост

О планировании карьеры часто говорят, но редко это делают. Совещание о карьерном развитии – это время, когда директор может выслушать мнение сотрудника о том, где он хочет быть в ближайшие 5 лет. Затем директор должен сопоставить эти желания с навыками и задачами, которые требуются группе. Только после этого они с сотрудником могут обсудить, какие краткосрочные

и долгосрочные цели соответствуют данным задачам. Директор может обнаружить, что никто из его нынешней группы не хочет занимать какие-то должности, – это даст ему знание того, какие навыки должны быть развиты в группе или восполнены при приеме новых сотрудников.

Чтобы правильно провести карьерное планирование, техническим директорам следует выделить для каждого сотрудника один час в год, чтобы сконцентрироваться исключительно на данном вопросе. Это не то же самое, что ежегодное совещание с проверкой производительности, оканчивающееся вынесением благодарности (или выговора). Проверка производительности необходима для диалога между директором и сотрудником. А совещание о карьере должно быть направлено на то, чтобы директор выслушал сотрудника.

Эта встреча – важный опыт для директора, который может открыть для себя некоторые удивительные факты. Самый застенчивый член группы хочет стать ее лидером, или лидер группы хочет пройти необходимое обучение, чтобы стать преемником директора. Директор может выяснить, что кто-то совсем заскучал и хочет кардинально сменить направление своей деятельности. Проще переквалифицировать кого-то из своих сотрудников, нежели нанимать неизвестно кого, поэтому такие нужды следует удовлетворять. Также это поможет создать группу с широким кругозором.

Большинство людей, особенно молодых, не знают, каким должно быть их продвижение по карьерной лестнице. Техническому директору следует делать предложения только тогда, когда сотрудники исчерпают идеи о том, чем бы они могли заняться. Типичные предложения довольно очевидны: младшему системному администратору хочется стать средним, а затем старшим. Директор должен помочь им стать профессионалами в их специальности, а затем постепенно увеличивать масштаб их работ, чтобы они могли получать опыт и развивать профессионализм в других областях. Что касается системных администраторов среднего уровня, директору следует наблюдать за их развитием, за тем, какие пробелы в опыте у них есть, и помогать им устранять эти пробелы. По мере того как они будут становиться более опытными, он может захотеть способствовать их специализации в определенных значимых областях.

Старшие системные администраторы больше других подвержены карьерному кризису. Они долго трудились, чтобы достичь своей должности, но какие цели им выбрать теперь? Для некоторых решение заключается в том, чтобы расширять свою известность и уровень знаний в своей области деятельности. Они должны продолжать работать над развитием специальности системного администрирования, участвуя в организации конференций, а также выступая на них или работая с IETF либо другими открытыми сообществами, чтобы принимать участие в спецификации и проектировании будущих технологий. Другие могут захотеть освоить профессию руководителя. Дайте им возможность управлять какими-то проектами, руководить и наставлять большее количество младших системных администраторов, привлекайте их к процессу формирования бюджета и поощряйте принимать участие в собраниях межотраслевого комитета в качестве представителей группы.

33.1.1.12. Бюджет

Технический директор также несет ответственность за бюджет своей группы. Он готовит ежегодную реалистичную бюджетную заявку, включающую повышение зарплат и бонусы, новый персонал, стоимость поддержки существующих

систем, расширение существующих систем, соответствующее росту компании, развитие областей, в которых они не предоставляют требуемого уровня обслуживания, обновление тех систем, которым оно потребуется, и финансирование новых проектов, необходимых для того, чтобы компания шла по правильному курсу и в ногу со временем.

Если директору выделят бюджет, который будет меньше, чем он запрашивал для группы, он будет отвечать за то, что его группа не выйдет за пределы бюджета и при этом будет выполнять все то, что должна. Если бюджет значительно меньше, чем он запрашивал, ему будет необходимо выделить те задачи, которые не могут быть решены без дополнительного финансирования.

33.1.1.13. Быть в курсе технологий

Технический директор отвечает за то, чтобы он сам и его группа были в курсе новых технологий. Он – технический ориентир, наставник и идейный лидер группы. Если он не будет знаком с новыми технологиями, то не сможет эффективно определять правильный курс своей группы и вести ее. Кроме того, он не сможет должным образом обучать свой персонал и помогать людям технически развиваться. Он даже, быть может, станет препятствовать внедрению новых технологий, так как они ему незнакомы и он будет неуютно себя чувствовать, двигая компанию в этом направлении.

33.1.2. Работа с нетехническими руководителями

Технический директор должен хорошо уметь совместно работать с нетехническими руководителями в своей цепи управления и пользовательской базе. Ключевыми компонентами успешных взаимоотношений с нетехническими директорами являются общение и оправдание ожиданий. Применяйте диаграммы и количественные данные, относящиеся к деловым задачам компании и группы. Для технического директора взаимоотношения с нетехническими руководителями – ключ к успеху и удовлетворенности работой.

> **Применяйте аналогии, которые они понимают**
>
> Техническому директору потребовалось объяснить финансовому директору своего отдела, что такое Ethernet-коммутатор. Это было еще тогда, когда Ethernet-коммутаторы были в новинку и проект по переводу всей сети с концентраторов на коммутаторы казался очень дорогим. Для начала он определил технологии, которые директор *понимал*, по большей части они были ограничены телефонным оборудованием. Поэтому он объяснил, что компьютерная сеть похожа на телефонную. Сейчас в заданный момент времени только два любых компьютера могут «разговаривать» друг с другом. Всем остальным приходится ждать. Ethernet-коммутаторы, объяснял он, позволят любым двум компьютерам «разговаривать» в любой момент, вместо того, чтобы ждать. Это директор мог понять. Заказ был быстро подтвержден, так как технический директор нашел способ донести смысл в терминах, которые его директор мог понять.

Вообще, другим руководителям, с которыми вы работаете, нужна уверенность, что вы и ваша группа сможете выполнить то, что им нужно и когда им нужно.

Они не желают ничего знать о технических деталях того, что вам необходимо будет сделать, и рассчитывают, что вы сами определите требования, которые им нужны. Убедитесь, что любые крайние сроки, которые вы установили для себя или для своей группы, пессимистичны. Лучше давать пессимистическую оценку и удивлять людей тем, что вы рано закончили, чем разочаровывать пользователей задержками. Но не переборщите с этим: если вы будете чересчур пессимистично настроены, люди посчитают вас неудачником и будут избегать вас в своих проектах.

Ваше непосредственное руководство хочет, чтобы вы успевали в те сроки, которые оно вам задает, и не расстраивали своих пользователей. Руководство не желает иметь дела с жалобами на вас или вашу группу, но зато хочет доверять вам дела и быть уверенным, что они будут завершены согласно расписанию. Если вы рискуете затянуть сроки или не можете выполнить требование своих пользователей либо руководителей, они хотят узнавать об этом как можно раньше, чтобы можно было заблаговременно внести изменения в сдвинувшееся расписание.

Нетехнические руководители, с которыми вы работаете, также ожидают от вас, что вы установите направление деятельности группы в соответствии с требованиями пользователей. Когда они запрашивают информацию о состоянии, они хотят узнать о вашей производительности, выраженной в требованиях, задачах и сроках, которые были установлены. Они не хотят быть засыпанными техническими деталями. Тем не менее, если они просят вас углубиться в технические вопросы, не бойтесь погружаться в детали. Если вы погрузитесь слишком глубоко, они вас остановят. Избегайте расплывчатых общих рассуждений: будьте точны и последовательны.

В работе со своей цепью управления – особенно это касается бюджетных вопросов – выразите ваши представления о том, как ваше руководство поможет компании в достижении ее целей или вашей группе в выполнении задач, поставленных компанией. Руководству нужно быть в курсе тех широкомасштабных задач, над которыми работает ваша группа, чтобы дать точный ответ, когда их спросят коллеги или начальники. Информировать начальство о делах вашей группы также важно, если вы хотите защитить вашу группу от перегруженности дополнительной работой. Если руководство не знает, как распределены ваши ресурсы, оно может предположить, что ваша группа не занята ничем важным, и привлечет ее на дополнительные проекты, в ущерб уже существующим обязательствам.

Обычно нетехнические руководители ожидают от технического персонала, что тот знает или может определить, что требуется для выполнения задач, стоящих перед нетехническими руководителями. Для запросов пользователей о поддержке знание требований означает понимание корня проблемы и временных ограничений, что рассмотрено в главе 14. Для построения новой службы это означает понимание потребностей пользователей, того, как служба будет применяться, как ее необходимо расширять, требований к производительности, модели поддержки, финансовых ограничений, требований к возможности взаимодействия и всех остальных вопросов, которые рассматривались в главе 5.

Знание требований и их учет помогут вам и вашей команде лучше сосредоточиться на заданной задаче. Системному администратору очень легко потерять сосредоточенность, когда исследование одной проблемы приводит его к другим или когда поиск способов построения новой службы раскрывает возможности в других областях. Это называется **расширением возможностей**. Ваши пользо-

ватели и ваше руководство ожидают, что вы будете придерживаться требований для направления вашей командной работы, избегая отклонений, хотя бы и интересных, чтобы выполнить поставленные задачи в срок. В то же время они ожидают, что вы будете исследовать возникающие альтернативы, если они не противоречат требованиям. Решение о том, что делать, подразумевает удержание в сознании общей картины, а не только точных деталей определенной ее части. Технический директор – человек, от которого ожидают, что он будет держать в голове общую картину и задавать направление.

Связь с вашим руководством и пользователями также следует основывать на требованиях. Например, если вы создаете новую службу, ваш начальник или пользователь может захотеть узнать, почему ваша команда предпочитает этот способ, а не другой. Если вы убеждены в том, что подход вашей группы лучше, чем предлагает другой человек, используйте требования для выражения причин этого. Другими словами, объясните, какие из требований заставили вас выбрать эту структуру, а не другую. Например, может быть так, что в предложенной вами структуре легче осуществлять поддержку, она взаимодействует с другими службами, с меньшими затратами или с лучшей производительностью расширяется до необходимого уровня, может быть сконструирована за заданный промежуток времени, использует более надежные системы или обладает более важными возможностями.

Требования пользователя – значительная часть любой работы, которую выполняют системные администраторы. Выяснение этих требований включает задание правильных вопросов вашим пользователям, внимательное выслушивание их ответов и получение некоторых пояснений, если это необходимо. Процесс создания списка требований пользователей – это возможность построить с пользователями отношения сотрудничества. Также его следует использовать как платформу для предоставления пользователям обратной связи и формирования реалистичных ожиданий.

Ясное определение требований и использование их для направления деятельности группы в конечном итоге приводит к более быстрому разрешению проблем и лучшим службам, а это, в свою очередь, ведет к большей удовлетворенности пользователей и руководителей.

33.1.3. Работа с вашими сотрудниками

Сотрудники технического директора – значительная часть его работы. Ему необходимо поддерживать их высокий моральный дух и сохранять их удовлетворенность от работы с ним. Кроме того, ему нужно способствовать их хорошей производительности и быть уверенным, что они знают, чего от них ждут.

33.1.3.1. Будьте хорошим примером для подражания

Директор влияет на поведение его группы тем, как он ведет себя с другими, включая своих собственных подчиненных. Если он вспыльчив и легко раздражим, его сотрудники так же будут вести себя со своими пользователями. Если он не заботится о своей работе, его группа будет отражать это в отсутствии внимания к своим пользователям. Однако, если он хорошо обходится со своими сотрудниками, они будут внимательны к нуждам своих пользователей. Если он жертвует своими интересами, чтобы помочь другим, его персонал будет поступать так же.

Техническому директору следует проявлять то же поведение, которое он хотел бы видеть в своей группе. Он ведет своим примером, и группа последует за ним. Ему следует рассматривать своих сотрудников как самых важных пользователей и стараться поддерживать их довольными. Если его группа будет довольна, будет довольно и его начальство – по крайней мере, им самим.

33.1.3.2. Обращайтесь со своими сотрудниками уважительно

Хорошее обращение с сотрудниками – ключевая часть поддержания морального духа и верности. Один из способов, которыми директор может показывать уважение к своим сотрудникам, – это помнить дату приема каждого из сотрудников и что-нибудь устраивать на их годовщины. Что-нибудь небольшое, чтобы отметить еще один год, проведенный человеком в компании, заставит человека почувствовать, что его ценят.

Другой способ, которым технический директор может дать своим сотрудникам знать, что их ценят, – публично объявить, что они делают хорошую работу. Его комплименты должны быть особыми, искренними и актуальными. Расплывчатые, запоздалые или неискренние комплименты могут произвести обратный эффект. Отличная работа, которая включала усилия за пределами обычных рабочих обязанностей, должна поощряться по крайней мере небольшим бонусом. Признание и ощущение собственной важности и ценности – гораздо более значительные мотивационные факторы, чем деньги. Однако отсутствие обещанных или безосновательно ожидаемых денег – это всегда фактор, лишающий мотивации. Использование денег как стимула может создать ожидания, которые вы не будете способны оправдать.

Признание важно

Друг Кристины работал в Xerox PARC в неспокойный период. Моральный дух в группе системного администрирования был очень низким. Оба директора группы уволились, и его оставили исполняющим обязанности директора. У него не было средств для материального стимулирования. Он поговорил с директором кафетерия компании и спросил, может ли тот предоставить ему один бесплатный обед в неделю для кого-либо из его сотрудников, чтобы кафетерий направлял счет за обед в его подразделение. В Xerox было заведено так: внутренние деньги, которые никто не получал наличными, не вычитались из бюджета, то есть фактически такие услуги были бесплатными. Затем он объяснил своему персоналу, что каждую неделю на совещании они будут поощрять того, кто особенно отличился на работе. Он не мог позволить что-либо шикарное, но он печатал небольшие сертификаты, украшенные золотыми звездами, и раздавал бесплатные обеды. Это был большой успех. Моральный дух повысился даже несмотря на то, что еда в кафетерии не была очень хорошей. Признания и символической награды было достаточно.

Признание может быть палкой о двух концах. Люди, которые считают, что они хорошо поработали, могут почувствовать себя недооцененными, если кто-то другой получает признание. Комикс «Dilbert» полон историй о том, как портит награда признанием.

Обратная реакция должна быть своевременной и индивидуальной. Если сотрудник провалил отдельную задачу, он обычно понимает, что натворил. Если это не слишком серьезная неудача, вызовите его и скажите, что ему не следует слишком беспокоиться об этом и что все совершают ошибки. Дайте ему спокойно проанализировать свою ошибку и подумать о том, как следовало бы поступить. Если же неудача была серьезной, сделайте ему замечание, но обязательно сделайте это наедине. Важно провести небольшую беседу спустя некоторое время после происшествия, чтобы сотрудник не зацикливался на ошибке надолго и не слишком ее преувеличивал. Возьмите на себя недовольство пользователей и руководства за его неудачу. Он поймет, что вы знаете о его ошибке, и будет уважать вас за ваши действия. Он будет стараться больше не ставить вас в эту ситуацию.

Тем не менее иногда люди делают ошибки и не осознают этого. У некоторых людей свой взгляд на вещи, и вам придется объяснить им, что они совершили ошибку. Некоторые люди убеждены в том, что никогда не ошибаются. Вам необходимо ясно объяснить им, что они виноваты. Только после понимания и признания своих ошибок они смогут исправиться.

Если вы делаете кому-то замечание, делайте это с глазу на глаз и будьте своевременны и точны, объясняя поведение, которое необходимо поменять. Замечания никогда нельзя делать публично. Если вы делаете замечание сотруднику публично, чтобы дать урок для всех, вы проявляете неуважение ко всем, кто с вами работает, а это лишит мотивации всю группу. Такое неуважение отразится на вас и может привести к отсутствию проявления уважения к пользователям.

Директору следует проявлять уважение к своему персоналу, информируя людей о важных событиях, происходящих в группе или компании. Но не переборщите с этим. Знание каждого потенциального изменения, большинство из которых не произойдет, может иметь вредное и отвлекающее влияние. Для значительных новостей может потребоваться правильное представление, чтобы они не привели к нежелательным последствиям. Однако, что совершенно точно, их следует представлять своевременно. Когда директор не доверяет своим сотрудникам в том, что они спокойно, ответственно отреагируют на события, происходящие в компании, он показывает им свое неуважение.

Нехватка информации

В маленькой консалтинговой компании высшие руководители настолько заботились о представлении сотрудникам любой информации, которую можно было интерпретировать как плохие новости, что настаивали на том, что будут делать это сами, и не разрешали техническим директорам информировать свой персонал. Это привело к большому недовольству среди технических директоров и сотрудников. Был инцидент, когда один из первых пяти сотрудников компании узнал об увольнении ключевого члена компании лишь из корпоративной новостной сводки, рассылаемой одним из основателей компании. Сводка упоминала об этом уходе довольно пренебрежительно, в последнем разделе. Сотрудник был настолько расстроен (и его можно понять) этим инцидентом, что с того момента его директор и некоторые другие воспротивились инструкциям руководства и стали должным образом информировать определенных сотрудников.

Директору следует слушать своих сотрудников. У них должна быть возможность обсудить свои мысли. Если у них проблема с пользователем, коллегой или поставщиком или даже личная проблема, они должны иметь возможность поговорить об этом с директором. Ему необходимо быть доступным для своих сотрудников. Ему всегда следует создавать у них ощущение, что их потребности очень важны для него, даже если у него есть другая неотложная работа. Поддержание эффективной работы группы приведет к бóльшим результатам, чем он может достичь сам. Однако ему нужно находить время и на выполнение собственной работы, не позволяя при этом группе чувствовать себя забытой. Запланированные еженедельные совещания с каждым сотрудником могут сильно сократить количество случаев, когда его прерывают в остальные дни недели. Нет необходимости в том, чтобы эти встречи были подготовленными или длинными. Они просто дают директору возможность спросить о том, как идут дела и чем он может помочь. А сотруднику они дают шанс высказать все, что, по его мнению, директору следует знать, не боясь показаться слишком требовательным или назойливым. Кроме того, от этого сотрудник будет чувствовать себя комфортнее при общении с директором и отношения вообще улучшатся. Когда директор слишком загружен срочной работой и вынужден уединиться, хорошим способом показать, что он не забыл о коллективе, будет объявить о том, что он сейчас очень занят и не хочет, чтобы его беспокоили по мелочам, но готов отвлечься по важному делу.

Технический директор обычно любит быть вовлеченным в жизнь персонала и их проекты. Он интересуется тем, как они решают проблемы, которые он ставит, и новыми технологиями, которые они привносят в компанию. Однако ему следует опасаться того, чтобы его интерес и его знания того, как решать многие проблемы, с которыми они могут сталкиваться впервые, не привели к избыточному контролю над персоналом. Избыточный контроль раздражает системных администраторов и демонстрирует отсутствие веры в их способность решать проблемы. Вы должны верить в свой персонал. Поощряйте их сообщать вам о своем прогрессе и обращаться к вам, когда им нужно поговорить о проблемах, которыми они занимаются, но не следует требовать сводок о ходе работы несколько раз в день или постоянно спрашивать, например, выполнили ли они данную задачу или поговорили ли они уже с данным человеком. Уважайте их способность хорошо выполнять свою работу и предоставьте им простор для этого.

Один из способов достичь этого – просить их писать проектные документы для крупных проектов. Это заставит их быть изобретательными, что даст вам возможность при внесении исправлений проводить конструктивную критику. Если вы склоняетесь к избыточному контролю над людьми, отправьте их писать проекты подальше от вас.

Для технического директора важно не только верить в свою группу, но и показывать им, что он верит в их способность решить любую задачу, которую он им даст. Он должен верить в них, пока они не дадут ему вескую причину поступать иначе. Они не должны сами доказывать, что достойны его доверия; они должны иметь это доверие изначально, пока не покажут, что они его не достойны.

33.1.3.3. Будьте оптимистом

К поддержке высокого морального духа в группе также относится уверенность в возможностях и направлении группы. Технический директор должен показывать своему персоналу, что он верит в людей и сделает все от него зависящее,

чтобы предоставить им все необходимое для успеха. Он никогда не будет бубнить о том, как хорошо дела шли раньше, в этой группе или где-то еще; вместо этого он будет думать о светлом будущем.

Если он – новый директор, поставленный для управления группой, про которую руководство ему говорило, что она терпит неудачи в любых направлениях, он не должен показывать, что ждет от группы неудач. Он должен быть настроен оптимистично и поговорить с людьми в группе, чтобы понять их настроения. Ему не следует что-либо менять, пока он не поймет, почему все происходит именно так, и не сможет определить, что хорошо, а что плохо. Тем не менее ему нужно решить проблему достаточно быстро, будь то реальная проблема или вопрос недопонимания. Если ему это не удастся, он потеряет поддержку своего руководства, без которой он будет неэффективным защитником для своей группы.

Новый директор

Организация системного администрирования, состоявшая из 75 человек, получила нового директора, которому руководство сказало, что группа, поступающая под его начало, неблагополучна и не работает как единая команда. Хотя у группы имелись проблемы, у нее был сильный командный дух. В первый день директор произнес речь о том, что он собирается создать единую команду, и описал, как людям из его прежней компании нравилось работать с ним и как они рыдали, когда он уходил. Системные администраторы покинули совещание с ощущением, что они все потеряют работу из-за людей из его прежней компании, и сомнениями в правильности своих рабочих отношений. Он также заставил их сомневаться в его способности управлять группой, так как он, по всей видимости, не замечал главного преимущества данной группы: командного духа.

33.1.3.4. Задавайте точное направление

Техническому директору необходимо убедиться в том, что все в группе понимают меру ответственности, лежащей на группе, и что каждый человек следит за собственной областью. Он должен убедиться, что каждый человек работает только над теми делами, которые ему поручены, и не трудится над другими проектами, пока ему не дадут на это согласия. Ему следует дать людям знать, что, если они берут на себя ответственность за соблюдение сроков и поддержание удовлетворенности клиентов, он позаботится об аспектах, за которые сам отвечает, и им не придется детально контролировать эти аспекты.

Ему необходимо ясно выражать, чего он от них хочет. Если они часто не выполняют то, чего он требует, возможно, он просто неясно выражается. Если он убежден, что выражается ясно, но все еще не получает от них желаемых результатов, ему следует попросить какого-нибудь сотрудника подробно объяснить ему, чего, по его мнению, он от них хочет. Если все дело в недопонимании, то, по крайней мере, теперь он будет знать о корне проблемы и сможет заняться ею напрямую.

Не предполагайте, что вы хорошо выражаете свои мысли, только потому, что вы точно знаете, чего хотите. Это не всегда так очевидно для окружающих. Некоторые директора не понимают, что они не объясняют того, чего хотят, достаточ-

но ясно. Они пользуются подходом в управлении, который иногда называют подходом «принеси-мне-камень». Директор говорит сотруднику: «Принесите мне камень». Сотрудник с трудом приносит ему «камень». Он говорит: «Нет, нет! Не камень! Я хотел камень». Сотрудник ищет другой камень, и так далее, пока он наконец не натыкается на определенный тип камня, который нужен директору. Постепенно сотрудники научатся понимать, чего хочет директор, когда просит камень, но только в том случае, если директор постоянен в выборе «камней», которые он любит. Камнем может быть стиль написания, способ составления планов проекта, бюджетного запроса, спецификации конструкции проекта, реализации службы или решения проблемы пользователя. Это что-то, о чем директор просит, но не может адекватно описать. Работа под руководством директора, который использует подход «принеси-мне-камень», может быть крайне неэффективной и обычно приводит к высокой текучке кадров.

33.1.4. Решения

Обычно техническому директору приходится принимать те или иные решения. Они включают в себя кадровые вопросы, а также вопросы назначения приоритетов и распределения задач между членами группы. Техническому директору также часто приходится раздумывать, покупать ли продукт для выполнения конкретной задачи или создать внутреннее решение.

33.1.4.1. Роли и обязанности

Техническому директору следует учитывать обязанности группы и таланты людей в ней, когда он нанимает новый персонал, а также при распределении проектов или областей ответственности между различными членами группы. При найме персонала ему следует искать пробелы, которые необходимо заполнить в плане наборов навыков и типов личности. В приложении А рассмотрены различные роли, которые могут играть системные администраторы. Техническому директору следует убедиться в том, что у него хорошее соотношение должностей, актуальных для его области ответственности. В главе 35 рассмотрен вопрос найма людей, которые будут эффективно работать в вашей среде.

Техническому директору следует грамотно распределять рабочую нагрузку в группе, учитывая особенности ее членов. Если он будет так поступать, он сможет принимать во внимание таланты людей, опыт и карьерный рост. Ему необходимо ставить им задачи, которые они способны решить, которые расширят их навыки и помогут им расти и которые при этом должны быть достаточно разнообразными, чтобы работа оставалась интересной.

33.1.4.2. Приоритеты

Технический директор также должен выбирать приоритеты группы и обсуждать их со своим руководством и с пользователями. При принятии этих решений он должен учитывать важность или полезность проекта и количество времени и усилий, необходимых для его выполнения. Он должен отдать больший приоритет аспектам, которые имеют большую полезность, чем другие, как изображено на рис. 33.1.

Легко понять, почему вам следует отдавать больший приоритет тем проектам, которые требуют меньших усилий, но в результате будут приносить больше пользы. Так же просто понять, почему наименьший приоритет отдается другой

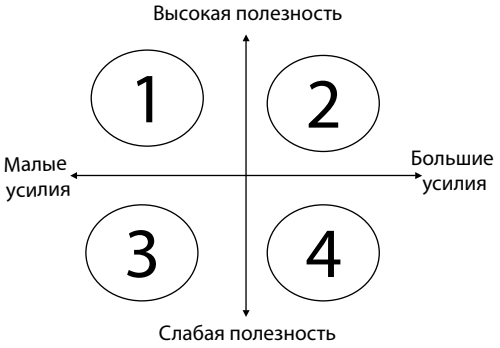

Рис. 33.1. *Установка приоритетов по признаку полезности (цифры обозначают порядок, в котором задачи должны быть выполнены)*

крайности: проекты, которые требуют большого усилия, но имеют лишь слабую полезность.

Встает вопрос, можно ли поменять между собой приоритеты 2 и 3. Мы утверждаем, что вы должны отдать большей полезности приоритет над меньшим усилием. В противном случае вы будете разрываться между маленькими проектами, от которых мало пользы. Чтобы избежать этого, требуется дисциплина. Они привлекательны из-за возможности быстрого удовлетворения; они будут выглядеть как достижения. Вы можете потратить месяцы, избегая проектов с высокой полезностью, заполняя свой день «еще одной маленькой задачкой», которую вы хотите выполнить, потому что это будет «так просто». Это одна из причин, по которым задерживаются большие проекты. Технический директор должен оберегать свою группу от такой ловушки.

Как правило, если вы точно понимаете полезность и усилия, соответствующие каждой задаче, ваше руководство будет поддерживать вас в ваших решениях. Ваши пользователи могут согласиться или не согласиться с тем, как вы оценили их проект, поскольку они могут необъективно относиться к проектам, которые не помогают им напрямую. Тем не менее те их проекты, которые вы оценили как имеющие бóльшую полезность, следует сделать для вашей группы самыми высокоприоритетными, даже если обычно у них не самый высокий приоритет.

Пример: большая полезность, больший результат

У компании было две системы, в которых не выполнялось управление изменениями. Одна успешно функционировала, другая была в аварийном состоянии. Руководство решило перевести обе системы на использование стандартных корпоративных процедур управления изменениями. Какая из них должна быть переведена в первую очередь?

Представьте требуемые затраты: проект А было легче перевести, так как группа, собравшая его, уже использовала довольно прозрачный процесс, который просто нужно было улучшить, чтобы он соответствовал корпоративным стандартам. Перевести проект В было гораздо сложнее, так как у него был гораздо менее упорядоченный процесс. Исходя из требу-

емых затрат, многие хотели начать с проекта А. На самом деле это могло стать неплохим «тестовым заездом» перед большим проектом.

Теперь давайте рассмотрим полезность этих двух переходов. Неофициальные, но в некотором смысле формальные процессы проекта А поддерживали его в довольно неплохом состоянии. Перевод его на корпоративный стандарт управления изменениями не имел бы значительной полезности. А фактически он мог разрушить так или иначе работающую систему. С другой стороны, отсутствие формальных процессов в проекте В создавало нескончаемый поток проблем и неудач. Управление изменениями здесь очень помогло бы. Новый, организованный, процесс освободил бы четырех инженеров для работы над другими проектами, вместо того чтобы заставлять их тратить день за днем на разрешение проблем. Это имело бы огромное положительное воздействие на маленькую компанию.

Изначально руководство запланировало сначала перевод проекта А – путь наименьшего сопротивления. Однако следование принципу наибольшей полезности помогло руководству начать с проекта В. После того как оба перехода были завершены, группы была рада, что выбрала именно такое решение.

33.1.4.3. Покупать или создавать

Техническому директору часто приходится принимать решения типа купить-или-создать. Должен ли он покупать продукт или выделить членов группы, чтобы они сами написали программное обеспечение? Это решение имеет несколько вариантов: покупка, интеграция, сборка или создание.

- *Покупка готового решения.* Готовые решения существуют во множестве отраслей, обычно они представляют собой хорошие, проверенные временем продукты, такие как приложения для обработки текста.
- *Интеграция или адаптация продукта к среде.* Крупные приложения требуют адаптации и настройки. Чтобы бухгалтерская система отвечала вашим деловым нуждам, необходимо потрудиться над ее настройкой. Программное обеспечение для поддержки пользователей требуется настроить, чтобы оно знало, какие продукты поддерживаются, кто поддерживается, и эффективно решало другие вопросы рабочего процесса. Если система полностью настраиваема, небольшие организации могут посчитать, что выполнение такой настройки будет не легче, чем написание системы с нуля. Часто только крупные рабочие среды могут выиграть от хорошо настраиваемых систем. Покупка системы, которая обладает более широкими возможностями по настройке, чем это необходимо организации, зачастую приводит к пустой трате времени.
- *Сборка нескольких проектов в единое целое.* Зачастую решения, необходимого организации, не существует, но для построения законченного решения можно скомбинировать небольшие системы. Основная идея в том, что для их соединения потребуется написание некоторого количества кода. Работа группы сводится к сборке компонентов в общее целое. Например, редко разные операционные системы одинаково работают с учетными записями, но они могут обращаться к определенному типу баз данных. Организа-

ции нужно развернуть базу данных SQL и создать связующий механизм, который позволил бы каждой операционной системе проводить аутентификацию через нее. Системы семейства Windows могут создавать и удалять учетные записи по мере их добавления и удаления из базы данных. UNIX-системы могут генерировать свои файлы /etc/passwd из дампа SQL-таблиц или при помощи хранимых SQL-процедур (Finke 2000). Некоторые комбинации собранных продуктов становятся настолько распространенными, что производители начинают предоставлять готовые сборки, чтобы заполнить этот пробел. Обычно такие производители могут предлагать дополнительные преимущества или более высокую производительность за счет профессиональной настройки. Компания NetApp поступила так после того, как увидела, что многие компании создавали удаленные файловые серверы из компьютеров под UNIX. Компания предоставила аппаратные сетевые/NFS-ускорители с программами для NFS и CIFS (общая межсетевая файловая система – Common Internet File System) и NIS для аутентификации. Mirapoint создала интегрированную почтовую систему, после того как обнаружила, сколько людей собирали почтовые серверы на базе компьютера под UNIX, программного обеспечения POP3 (Myers and Rose 1996) и IMAP4 (Crispin 1996) и агента пересылки сообщений, например Sendmail или Postfix.

- *Создание решения с нуля.* Больше всего возможностей по индивидуализации предоставляет именно этот метод. Техническому директору и его группе придется пройти полный путь, включающий в себя сбор требований, проектирование архитектуры, разработку, тестирование и внедрение.

Каждый вариант имеет свои положительные и отрицательные стороны. Считается, что один из вариантов – покупка – обычно требует меньшего количества работы, имеет минимальное «время до готовности» и более низкую стоимость в расчете на человеческие ресурсы. С другой стороны, такие решения имеют меньшие возможности по настройке и могут потребовать длительного обучения персонала. Поддержка может иметь как положительные, так и отрицательные стороны. Если продукт коммерческий – или имеется коммерческая поддержка для проекта с открытым кодом, – вам дается телефонный номер, на который можно позвонить, если возникает вопрос. С другой стороны, может пройти несколько долгих циклов жизни продукта, пока будут устранены неисправности, которые не считают достаточно серьезными для выпуска патча.

Построение решения с нуля также имеет свои преимущества и недостатки. Продукт создается, чтобы разрешить определенные проблемы, с которыми сталкивается группа. Он будет подходить к имеющейся среде, платформам и методам. Стоимость будет определяться скорее временем, чем денежными затратами, что может быть важно для среды, в которой мало денег, но много людей. В частности, построением систем с нуля часто занимаются университеты, так как у них немного средств, но практически неисчерпаемый запас дешевой рабочей силы. Другим преимуществом собственных решений является то, что иногда они становятся полноценными продуктами, или заключаются договора с дилерами/OEM-компаниями (Original Equipment Manufacturer – поставщик комплексного оборудования), или авторы получают известность при публикации их работы в Интернете либо представлении на конференциях, таких как LISA. Гордость за разработку оригинального программного обеспечения может мотивировать группу.

Поддержка после того, как исходная группа отошла от дел, – это отдельный вопрос. Собственные решения могут стать кошмаром для поддержки, после того как программисты покинут группу или закончат учебное заведение. Хотя производители коммерческого программного обеспечения предоставляют более надежную поддержку, они также могут приостанавливать поддержку устаревших продуктов или просто прекратить свою деятельность.

Как технический директор должен принимать решение, зная преимущества и недостатки каждого из подходов? Он должен дать объективную оценку каждому методу.

Главной причиной для покупки готового решения является минимальное «время до готовности». Основная причина для создания собственного решения – получить возможности, недоступные из внешних источников. Директор должен тщательно проанализировать, почему эти возможности необходимы. Отказываться от коммерческого программного обеспечения из-за незначительных причин, личных убеждений или неприязни к производителю просто неправильно. С другой стороны, требуемые возможности иногда нигде недоступны, так как никто еще не думал о них. Разработка собственной системы оправдана, если вы хотите получить возможности, которые не могут предоставить коммерческие системы. Это может дать вам конкурентное преимущество.

Пример: получение конкурентного преимущества

Производителю Pentium-совместимых процессоров удалось обогнать Intel по дате выпуска процессора определенной скорости, так как он разработал собственную систему фонового планирования для легкого выполнения больших объемов интенсивных вычислений. Когда чип был анонсирован, производитель связал этот успех со своим собственным решением; он не смог бы достичь успеха с коммерческими фоновыми планировщиками, доступными в то время.

Проектирующая чипы компания даже представила доклад о своей системе планирования на конференции USENIX LISA. Компания не боялась выдать свои секреты, потому что знала, что конкуренты все равно наверстают упущенное ко времени начала конференции.

В быстро развивающейся компьютерной индустрии конкурентное преимущество обычно очень недолговечно. Это следует принимать во внимание при принятии решения. Хотя, как правило, для получения значительной коммерческой выгоды обычно хватает нескольких месяцев на лидирующих позициях.

Собственные решения часто встречаются в ситуациях, когда идея достаточно нова и коммерческие решения еще недоступны. Однако техническому директору следует обращать внимание на появляющиеся коммерческие продукты и определять, когда собственное решение можно будет заменить на одно из них. Например, когда UNIX была в новинку, создание новой системы для управления резервным копированием считалось более интересным и инновационным. Однако теперь эта проблема – «решенный вопрос» для небольших компаний и такой продукт слишком сложен для внутренней разработки в крупных организациях.

Хотя возможность получить оригинальную функциональность может быть заманчивой, обычно для технического директора правильной мыслью будет не предполагать, что потребности организации очень специфические, и вместо этого рассмотреть доступные коммерческие продукты. По меньшей мере, он узнает о возможностях, о которых в противном случае мог бы и не подумать и которые он может захотеть интегрировать или отказаться от них. Одновременно с обзором популярных продуктов ему следует рассматривать результаты конференций по системному администрированию, в частности конференций USENIX и LISA[1].

Когда используется коммерческое программное обеспечение, для технического директора или старшего сотрудника группы может быть важно иметь партнерские отношения с поставщиками, чтобы влиять на решения, касающиеся разработки, в направлении новых возможностей, которые крайне необходимы его организации. В высокотехнологичных средах может быть полезно рассказывать поставщикам, какие новые возможности понадобятся всем в следующем году. Однако при создании партнерских отношений важно ясно определить, кому принадлежат идеи; могут возникнуть вопросы, связанные с интеллектуальной собственностью.

Гибридная модель заключается в использовании открытых и коммерческих решений, которые предоставляют хорошие строительные блоки, и проведении интеграции собственными силами. Некоторые системы разработаны специально для использования в данном направлении. Сложные работы по проектированию и разработке выполняются изначальным автором, но адаптация, которую вы проводите, делает систему идеально подходящей для вашей среды.

Решения типа купить-или-создать приходится принимать довольно часто, и универсального правильного ответа до сих пор нет. Он зависит от вопросов времени, уровня возможностей по настройке и функциональности. По мере развития производства будет появляться больше коммерческих вариантов. Но удовлетворение от воплощения вашей собственной прекрасной идеи нельзя переоценить.

33.2. Тонкости

Итак, теперь ваша группа благополучно работает, вы приняли решения, которые вам необходимо было принять, и все ваши обязанности находятся под вашим контролем. Что дальше? Мы предлагаем несколько способов, которые помогут вам сделать вашу группу сильнее. Но теперь, когда вы выяснили, как поддерживать удовлетворенность вашего персонала, руководства и пользователей, следует уделить некоторое время и собственным интересам. Займитесь своим карьерным ростом. Подумайте, что вы можете сделать, чтобы получать большее удовлетворение от работы.

33.2.1. Сделайте свою группу еще сильнее

Рассмотрите способы, которые позволят вам сделать группу сильнее. Способствуйте командному подходу и дайте сотрудникам возможность учиться, вовлекая их в работу над крупными проектами. Заставляйте их вместе готовить

[1] Доступны на *http://www.usenix.org/*.

доклады на конференции. Организуйте культурно-развлекательную программу и привлеките их семьи, например устройте общий обед в парке, на который каждый принесет для группы какую-нибудь еду. Такие события могут повысить удовлетворенность людей своей работой и помочь сотрудникам улучшить отношения с другими членами группы. Однако убедитесь, что никто не лишен возможности участвовать в таких событиях из-за обязанностей поддержки по вызову или по другим причинам, связанным с работой. Оставшиеся за бортом начинают чувствовать себя изолированными, ненужными и перестают ощущать себя частью группы.

Чем дольше люди остаются в группе и чем меньше текучесть кадров, тем сильнее они будут чувствовать себя частью одной команды и тем выше вероятность, что они пройдут вместе с ней через любые трудности. Выясните способы, которыми можно удержать ваших сотрудников. Таким же важным, как удержание сотрудников, является наем правильных людей. Убедитесь, что люди, которых вы берете на работу, хорошо подходят группе. Даже один неподходящий сотрудник может очень плохо повлиять на группу.

33.2.2. Популяризируйте ваше подразделение среди высшего руководства

Убедитесь, что высшее руководство знает, чем занимается ваша группа и какую выгоду она приносит компании. Чем более заметна ваша группа и, особенно, чем ярче ее успехи, тем больше шансов вы имеете получить ресурсы, которые позволят вам помогать людям в их работе и награждать их за труд. Убедитесь, что ваше высшее руководство знает о вашем вкладе в важнейшие проекты по всей компании. Если кто-то самозабвенно работает, чтобы быть уверенным, что демонстрация на конференции или перед пользователями пройдет безупречно, убедитесь, что он получает за это поощрение и признание. Когда ваша группа внедряет новые службы или обновляет существующую службу, убедитесь, что высшее руководство понимает, как это улучшает эффективность остальных подразделений и экономит деньги компании. В главе 31 подробно рассмотрены способы, при помощи которых можно сделать успехи группы заметными. Для будущих успехов группы жизненно важно, чтобы высшее руководство признавало группу активом компании.

33.2.3. Работайте над собственным карьерным ростом

Закончив помогать всем, кто на вас работает, подумайте и о себе. Убедитесь, что вы получаете признание, которого достойны как за свои собственные заслуги, так и за успехи вашей группы. Изучите деятельность компании, чтобы у вас была возможность устанавливать лучшие отношения с пользователями вашей группы и принимать более правильные решения о том, каким запросам следует отдать приоритет. Узнайте об управлении бизнесом, чтобы вы могли лучше общаться с нетехническими руководителями в своей цепи управления. Выясните, чего они хотят и почему, чтобы вы могли действовать в соответствии с их нуждами, и они будут уверены в вас и вашей группе.

33.2.4. Делайте то, что вам нравится

Последнее, но немаловажное – подумайте, как вы можете получить удовлетворение от должности технического директора. Найдите способ ставить себе зада-

чи, которыми вы бы наслаждались как перерывами в обычной рутинной работе. Для большинства технических директоров это означает участие в некоторых узкопрофильных, не очень срочных технических проектах. Немного технической работы даст вам неплохой перерыв в потоке других задач и поможет не отставать от современных технологий и быть в курсе всех типов задач, которые вашим людям приходится решать каждый день.

33.3. Заключение

Технический директор – это человек, который должен быть одновременно и опытным системным администратором, и руководителем. Как опытный системный администратор он играет роль наставника для менее подготовленных системных администраторов группы и является для группы своего рода техническим ресурсом. Как руководителю ему необходимо управлять бюджетом, заключать контракты и работать со своим руководством и пользователями, стремиться поддерживать их удовлетворенность, а также сохранять направление деятельности группы в соответствии с курсом всей остальной компании.

Это пример для подражания и идейный лидер своих сотрудников. Это человек, к которому обращается его руководство, когда хочет узнать о том, чем заняты системные администраторы. Это человек, с которым разговаривают руководители пользователей, чтобы утвердить расписания и распределение ресурсов для их проектов.

Его важнейшая обязанность – поддерживать высокий моральный дух персонала. Чтобы добиться этого, ему необходимо с уважением обращаться с сотрудниками и награждать их за хорошую работу. Ему необходимо держать их в курсе новостей, но не перегружать их постоянно меняющимися капризами других групп. Ему нужно поддерживать свою группу и защищать ее членов от гнева разочарованных пользователей, а также помогать им стать лучше в будущем. Ему необходимо способствовать их техническому развитию и направлять их карьерный рост.

От директора также требуется принятие некоторых решений от имени всей группы. Ему необходимо решать вопросы о распределении должностей в группе. Ему необходимо понимать, когда требуется больше персонала, и решать, на какие места в группе нужно поставить новых сотрудников. Ему также приходится решать, нужно ли группе приобрести коммерческие решения для устранения конкретных проблем или она должна создать решение собственными силами.

Кроме того, ему необходимо заботиться о себе самом. Он должен находить время на себя и заниматься чем-то, что доставляет ему удовольствие, например работой над узкопрофильным техническим проектом, которой он может посвящать себя в перерывах между другими делами.

Людей, не имеющих опыта в руководстве, может заинтересовать книга «*The One Minute Manager*» (Blanchard 1993) и связанная с ней книга «*The One Minute Manager Meets the Monkey*» (Blanchard, Oncken and Burrows 1989). Обе книги короткие, но очень полезные.

Задания

1. Какой пример для подражания вы показываете своей группе?
2. Кто был вашим лучшим техническим директором и почему? Какие недостатки были у этого человека?
3. Кто был вашим худшим техническим директором и почему? Какие хорошие качества были у этого человека как у вашего руководителя?
4. Если вы технический директор, как вы думаете, в каких направлениях у вас успешно идут дела? Какие области, по-вашему, вы бы могли улучшить?
5. Опишите группу с высоким уровнем морального духа, в которой вы работали. Какие факторы, по-вашему, привели к высокому моральному духу?
6. Опишите группу с низким уровнем морального духа, в которой вы работали. Какие факторы, по-вашему, привели к низкому моральному духу?
7. Опишите ситуацию, при которой моральный дух в группе, в которой вы работали, резко упал. Какие факторы, по-вашему, повлияли на падение морального духа?
8. Что вы делаете, чтобы доказать вашему персоналу, что вы цените их работу?
9. Что вы делаете, чтобы помочь вашему персоналу технически развиваться? Достаточно ли финансируется техническое развитие вашей группы?
10. Опишите свои взаимоотношения с нетехническим руководителем. Какими были или какие еще существуют самые большие трудности, которые вам нужно преодолеть для построения успешных рабочих отношений?
11. Какие виды поощрений существуют в вашей группе? Основываясь на рассуждениях, приведенных в разделе 33.1.1.5, ответьте, правильно ли они организованы. Каковы положительные или отрицательные результаты этих бонусов или прибавок?
12. Какие из своих обязанностей вы считаете самыми главными?
13. Опишите ситуацию, в которой вам приходилось принимать решение типа купить-или-создать и вы выбрали покупку. Что заставило вас сделать этот выбор? Оглядываясь в прошлое, ответьте, какой выбор был бы правильным.
14. Опишите ситуацию, в которой вам приходилось принимать решение типа купить-или-создать и вы выбрали создание. Что заставило вас сделать этот выбор? Оглядываясь в прошлое, ответьте, какой выбор был бы правильным.
15. Опишите распределение обязанностей в вашей группе. Есть что-нибудь, что, по-вашему, следует изменить?
16. Что вы делаете, чтобы себя побаловать и продолжать получать удовольствие от вашей работы?

Глава 34

Советы нетехническим руководителям

В этой главе рассматриваются взаимоотношения между нетехническими руководителями и старшим техническим персоналом в организации системного администрирования. Данная глава исследует взаимоотношения между персоналом системного администрирования и его цепью руководства, а также между руководством пользовательской базы и старшим персоналом системного администрирования. В частности, эта глава предназначена для нетехнического директора, перед которым отчитывается организация системного администрирования. Нетехнические директора также могут обратиться к главам 21 и 30, которые охватывают организационные структуры системного администрирования, сильные и слабые стороны централизованных и децентрализованных моделей и то, как они влияют на ту или иную группу.

Как у системных администраторов, так и у директоров есть конкретные требования друг к другу и взаимные обязанности. Чтобы построить хорошие взаимоотношения, и те и другие должны понимать, что это за требования и обязанности и как им соответствовать. Хорошие взаимоотношения основаны на взаимном уважении и качественном общении. Эта глава включает в себя методы, которые способствуют и тому и другому.

34.1. Основы

Главные обязанности нетехнического директора, ответственного за организацию системного администрирования, заключаются в том, чтобы устанавливать приоритеты и предоставлять ресурсы и при этом поддерживать высокий моральный дух.

Все взаимоотношения основаны на общении, и взаимоотношения, которые нетехнические директора имеют со старшим техническим персоналом, – не исключение. Мы рассмотрим способы, благодаря которым межличностные связи и собрания персонала могут помочь нетехническому директору улучшить качество общения с техническим персоналом.

Для хорошей совместной работы группе системного администрирования и директору необходимо иметь единое мнение. Чтобы способствовать его созданию, старший технический персонал следует попросить создать годовой план для каждой области специализации, основанный на той информации и том направлении, которые дает им директор. Директор будет использовать эти выкладки при формировании бюджета и при планировании, привлекая старших системных администраторов в течение всего цикла принятия решений. Такие действия могут быть полезным опытом для всех. Они помогают системным администра-

торам понять курс компании и заставляют их чувствовать себя вовлеченными в процесс получения результата и влияющими на него.

Предоставление системным администраторам возможности принимать участие в профессиональных мероприятиях, таких как конференции и учебные курсы, является необходимым элементом улучшения их производительности и повышения степени удовлетворенности работой. Системным администраторам необходимо быть в курсе постоянно меняющихся технологий, и им, как правило, это нравится.

34.1.1. Приоритеты и ресурсы

Главная обязанность нетехнического директора в технической организации системного администрирования заключается в том, чтобы устанавливать приоритеты и предоставлять ресурсы. Это ничем не отличается от руководства в любой другой ситуации. Однако нетехнический директор может не всегда понимать детали работы технической группы и поэтому нуждается в большем взаимном уважении и доверии, чтобы работать продуктивно.

Информирование о приоритетах важно не только для сообщения о направлении, но и для перевода информации на язык, который все понимают. Деловые термины, которые имеют смысл для нетехнического директора, могут быть просто непонятными для технического персонала. Это удивляет многих нетехнических директоров. Технические люди умны, но как они одновременно с этим могут быть такими безграмотными? Это происходит не потому, что технические люди намеренно игнорируют деловой сленг; они просто находят его забавным и им кажется, что директора постоянно придумывают новые слова.

Предоставление ресурсов обычно подразумевает установку правильного количества персонала и бюджета.

Два лучших руководителя Стива

Системный администратор из Нью-Йорка описал двух лучших руководителей за всю свою карьеру следующим образом. Оба они были старшими вице-президентами, но являлись противоположностями во всем остальном.

Первый руководитель раньше занимал технические должности. Когда системный администратор описывал технические вопросы, руководитель их понимал. Они сходились во взглядах. Они могли эффективно работать вместе, поскольку понимали друг друга как в технических, так и в других вопросах. Системному администратору нравился этот руководитель.

Другой руководитель, напротив, имел очень мало технического опыта. Однако у него и его системного администратора были отличные взаимоотношения, потому что они уважали сильные стороны друг друга и могли эффективно работать вместе, поскольку они знали, как договориться о необходимых вещах, и принимали вышеуказанные ограничения. У их организации были специфические задачи, связанные с нововведениями безопасности, которые компания принимала в ответ на новые нормы SEC. Системный администратор отвечал за техническую сторону вопроса, а руководитель работал над обеспечением финансирования, необходимого, чтобы воплотить планы системного администратора в жизнь. Задача

системного администратора была в том, чтобы помочь руководителю достичь успеха: системный администратор предоставлял темы для обсуждения, которые его руководитель мог использовать при поиске необходимого финансирования, а также основные этапы и информацию о ходе процесса для укрепления доверия. За исключением вопросов, связанных с бюджетом и текущим состоянием, руководитель обычно не понимал, о чем говорит системный администратор. Однако им удавалось удачно взаимодействовать и получать финансирование, необходимое для достижения деловых задач, которые перед ними стояли.

Эти два руководителя были абсолютными противоположностями, но они были лучшими из тех, с кем системному администратору когда-либо приходилось работать. В обоих случаях они находили способы использовать свои сходства или отличия для достижения результатов.

34.1.2. Моральный дух

Для того чтобы группа системных администраторов работала на пике производительности, у них должен быть высокий моральный дух. Когда моральный дух на высоком уровне, они будут делать все, что от них требуется, даже если для этого нужно допоздна задерживаться на работе или проявить героизм. Когда моральный дух падает, у персонала не будет желания вкладывать все свои силы в работу, которая стала унылой и бесперспективной.

О создании или поддержании высокого морального духа легче сказать, чем сделать это. Системное администрирование – очень напряженная работа. На ней можно столкнуться с постоянно увеличивающимся объемом работы, поджимающими сроками, гневными пользователями, множеством небольших кризисов и периодическими серьезными чрезвычайными ситуациями. Очень напряженная рабочая жизнь делает системных администраторов более чувствительными к атмосфере на работе и к тому, что их недооценивают. Грамотному нетехническому директору следует выяснить, как легкой рукой вести группу и предотвращать внешнее влияние по прерыванию их рабочего процесса или снижению морального духа.

Мелочная опека снижает моральный дух. Нетехническому директору следует управлять задачами персонала в целом, а не решениями. Старший технический персонал рассчитывает, что нетехнические директора определят направления высокого уровня, доверив воплощение этих задач персоналу, и они будет предоставлять периодические отчеты о ходе процесса. Мелочная опека проектов отвлекает, замедляет и деморализует системных администраторов, а также другой технический персонал. Системные администраторы также предполагают, что их руководители помогут им в преодолении любых препятствий, которые они могут встретить, пытаясь выполнить свои задачи, а также в получении адекватного финансирования, чтобы системные администраторы могли закончить свои проекты и достичь тех уровней обслуживания, которых от них ожидают. Нетехнический директор также должен стремиться быть своеобразным фильтром и буфером от стресса, возникающего от знания всего, что может произойти, но не происходит, и при этом он должен вносить максимальную ясность в работу технического персонала, информируя людей о проектах, которые точно будут воплощены в жизнь.

Руководитель – это человек, который предоставляет возможности. Он дает своим сотрудникам возможность выполнять свою работу, устраняя при этом худшие политические препятствия с их пути. Нетехническому директору никогда не следует пытаться принимать технические решения или управлять ими. Когда ему приходится изменять техническое решение по политическим причинам, ему следует объяснить своим людям, в чем кроются причины и почему он так поступил; в противном случае они обидятся на него и их моральный дух упадет.

Неопределенное будущее может разрушить моральный дух. Зачем работать, если вы можете завтра потерять вашу работу? Зачем создавать законченное решение, с хорошей документацией, техническим обеспечением надежности и т. п., если вы думаете, что группа перестанет существовать через несколько месяцев? Зачем выполнять долгосрочное планирование для группы, которая постоянно меняется? В крупной компании ходит множество слухов о реорганизациях, увольнениях, переменах и перестановках. И к работе нетехнического директора относится управление воздействием, которое оказывают такие слухи на группу системного администрирования. Ему следует держать в голове потенциальные перемены и информировать старший технический персонал, когда перемена кажется возможной. Но ему следует делиться этими мыслями со всеми только после того, как принято решение. Даже если он является тем человеком, который обязан принимать во внимание такие возможные корпоративные улучшения, он должен составить картину прочного будущего, или сотрудники разойдутся на все четыре стороны. Важно, тем не менее, не давать лживых или недостоверных гарантий, иначе персонал не будет ему доверять.

Пример: неопределенность плохо влияет на моральный дух

Новый директор не понимал важности создания картины прочного будущего и обсуждал каждый слух о переменах со своими старшими системными администраторами. Каждая мысль и замечания о сокращениях бюджета, повышениях, переменах и реорганизациях обсуждались со старшими системными администраторами. Вскоре каждый в группе был уверен, что руководство ведет группу к гибели, собирается провести сокращения, недовольно группой и т. д. Зачем руководству проводить эти перемены, если оно довольно группой? На самом деле в обязанности руководства входит выполнение только тех перемен, которые принесут компании выгоду. Предыдущее руководство справлялось с такими же проблемами, но не ставило группу системного администрирования в известность о каких-либо ситуациях, кроме наиболее вероятных. Поэтому группа системного администрирования в течение многих лет была уверена в прочном и предсказуемом будущем, а теперь пришел год постоянных угроз перемен. В действительности перемены проводились так же, как и раньше, но утвердилось ощущение, что нет никакой определенности относительно будущего. Системные администраторы начали один за другим покидать группу. Когда ушли некоторые старшие системные администраторы, высшее руководство запаниковало и объяснило этому нетехническому директору, как его действия влияют на группу.

Это не значит, что руководству следует принимать важные решения в вакууме, без консультаций со старшими системными администраторами. Это не так, но нужно найти какое-то равновесие.

Группе системного администрирования необходимо знать, что она всегда может обратиться к директору за поддержкой. Если у него не будет такой репутации, члены группы перейдут в компанию, где они смогут получить эту поддержку.

Поддерживайте группу

Вот история о том, как один директор дал понять своей группе, что системные администраторы всегда получат поддержку, если они достойно себя ведут. Один системный администратор во время ремонта жесткого диска на рабочей машине случайно переформатировал на машине другой диск. Стертые данные собирались на протяжении последних двух лет, у них не было резервной копии, и поэтому их нельзя было восстановить. Понимая, что ситуация может выйти из-под контроля, директор немедленно отстранил от работы этого системного администратора, который от страха был готов покончить с собой. Он встретился с пользователями, объяснил, что произошло, и взял ответственность за ошибку группы на себя. Пользователи, конечно, были в гневе от такой ситуации, но директор заступился за свою группу. Хранение данных на рабочей машине противоречило политике: все данные должны были храниться на серверах, где выполнялось резервное копирование. Диски были подключены к машине много лет назад и только с согласия пользователей на то, что не будет проводиться резервное копирование данных, поэтому они должны были использоваться только для хранения временных данных и в качестве рабочего пространства. Директор отдела системного администрирования согласился оплатить полную стоимость ремонта диска, несмотря на высокие цены и отсутствие гарантии успеха. Пользователи не были очень довольны, но они стали уважать директора за то, что тот заступился за свою группу (тот факт, что он обладал прекрасной спортивной фигурой, возможно, тоже помог). Системный администратор не был подвергнут публичному наказанию за то, что он сделал. Неделя жизни в страхе за свою работу была достаточным наказанием, и можно предположить, что это сильно повлияло на его ежегодные показатели производительности. Директор знал, что системный администратор вынес из всего этого урок, и никогда не вспоминал о происшествии, сказав только: «Я уверен, что ты многое вынес из этого и будешь осторожнее в будущем».

Действия директора прозвучали громче, чем слова: честные ошибки – это часть работы, и персонал будет получать поддержку, если станет усердно трудиться, сохранять осторожность и признавать свои ошибки.

34.1.3. Общение

Технический персонал часто может сталкиваться с языковой проблемой в разговорах с людьми, которые не знакомы с его областями деятельности. Эта проблема может привести к трудностям в общении. Как правило, технический персонал будет развивать привычку пользоваться туманными общими поняти-

ями, вместо того чтобы описывать подробности, которые могут ничего не значить для слушателя. Со старшим техническим персоналом следует провести инструктаж, чтобы они выучили язык своих нетехнических директоров и пользователей и применяли его в диалогах с ними. На этом языке излагаются те требования, на которых основывается работа, выполняемая техническим персоналом. Системным администраторам следует понимать требования, которые управляют их работой, основывать свои решения на этих требованиях и обсуждать прогресс проекта относительно этих требований.

Сленг руководителей

И по сей день Том не знает, что руководители понимали под «синергией» в начале 1990-х годов.

34.1.4. Совещания персонала

Формальные совещания персонала между системными администраторами и их нетехническим директором помогают системным администраторам быть в курсе того, что происходит в их группе и в компании в целом. Такие регулярные совещания могут стать для директора возможностью сообщить направление, в котором, по его мнению, группа должна двигаться, и уполномочивать отдельных людей решать, как достичь этих целей. Такие встречи требуют планирования. Нетехническому директору следует встретиться со старшими системными администраторами и составить план совещания. Так же, как он не понимает технический жаргон системных администраторов, им может быть сложно воспринимать сленг руководителей и их точку зрения. Важно рассмотреть со старшими системными администраторами, как можно будет представить различные идеи, чтобы они их поняли и, что более важно, чтобы избежать негативных последствий. Громкая фраза, которая означает выдачу полномочий, может оказаться губительно деморализующей, проходя через уши системного администратора. Обсуждение схемы или плана совещания со старшим системным администратором позволит избежать этой проблемы.

Репетируйте визит руководства для предотвращения катастрофы

Однажды вице-президент компании встретился с группой системного администрирования, чтобы продемонстрировать свою поддержку группы. Встреча шла очень хорошо до его последнего комментария, в котором он нечаянно задел область горячих дебатов. Он не знал, что конкретный вопрос стало опасно упоминать, не расстраивая людей. В то время как первые 45 мин прошли как по маслу, последние 15 мин были потрачены на уход от гнева по поводу данного вопроса. Вице-президент не думал, что эта тема настолько значительна, и не понимал, насколько она волновала группу. Он закончил так, как будто ему не было дела до системных администраторов. Эта встреча была такой катастрофой, что старший системный администратор собрал группу позже в этот же день, чтобы

восстановиться от полученного негатива. Его попытка не увенчалась успехом, и в итоге восстановление заняло недели. За это время группу покинули старший и младший системные администраторы. Всего этого можно было избежать, если бы вице-президент перед этим встретился со старшим системным администратором.

Преподаватель театрального кружка Тома в школе всегда любил говорить: «Никогда не делай на представлении того, чего ты не делал на репетиции». Вице-президенту сильно помог бы этот совет.

Нетехническому руководителю также следует способствовать проведению еженедельных встреч для поддержания согласованности в технических вопросах. Эти встречи должны предоставлять системным администраторам возможности по поиску помощи у других и вовлечению в проекты или стандарты, над которыми работают иные люди в группе. Эти встречи могут стать полезным методом, посредством которого можно поддерживать группу единой, заинтересованной, и довольной.

Системные администраторы, как и большинство других людей, хотят знать, что происходит вокруг них на работе, и принимать участие хотя бы в небольшом количестве проектов, которые их затрагивают или просто интересуют. Из-за того что многие системные администраторы, особенно те, кто находится на должностях по непосредственной поддержке пользователей, проводят бóльшую часть времени, работая с пользователями, а не с другими системными администраторами, они могут почувствовать себя изолированными от группы системного администрирования. Важно сделать их частью группы и держать их в курсе направления, которому следует группа в новых технологиях и стандартах. Регулярные встречи персонала – хороший способ для руководителей системных администраторов поддерживать свои группы едиными и информированными. Такие встречи предоставляют сотрудникам группы возможность узнать, над чем работают другие, в каких вопросах и проектах другие находятся впереди и где они могут получить комментарии по поводу тех или иных идей или помощь по конкретным проблемам. Встреча персонала должна держать системных администраторов в курсе всего важного, что в последнее время происходит где-то в другой части компании. Ее можно использовать как сбор, на котором системным администраторам регулярно напоминают о важных политиках, процедурах, требующих соблюдения, или о внутренних стандартах.

Кроме того, такие встречи полезны, поскольку это один из тех немногих случаев, когда люди из передней линии поддержки встречаются с людьми из задней линии поддержки. На таких встречах обычно задняя линия поддержки узнает о систематических проблемах, которые им необходимо решать для персонала из первой линии. Также такие встречи – отличная возможность для опытных технических лидеров обучать остальную группу техническим тонкостям.

Пример: используйте встречи персонала для передачи знаний

В одной группе системного администрирования еженедельные встречи включают 20-минутную часть, на протяжении которой ведущий систем-

ный администратор объясняет какой-либо технический аспект работы группы. Это дает старшим системным администраторам дополнительный опыт по представлению информации и способствует обучению остальных системных администраторов в технических вопросах.

34.1.5. Годовые планы

Работа системных администраторов по своей природе состоит из большого количества маленьких задач и нескольких крупных. В результате для системного администратора довольно просто потерять общее видение того, что происходит в компании, и упустить из виду соответствующее направление, которое должна принять его собственная работа. Периодическое составление годовых планов может помочь вернуть в память общую картину. Оно также помогает руководителю системного администратора и его пользователям проводить лучшее планирование на последующий год.

Нетехнические директора также рассчитывают, что их старший технический персонал имеет представление о направлении, которому следует компьютерная среда компании. Старшему техническому персоналу следует заранее учитывать новые эксплуатационные требования и устанавливать необходимые обновления, а также подумать о путях оптимизации задач системного администрирования или других методах улучшения обслуживания. Старший системный администратор должен смотреть по меньшей мере на год вперед и планировать проекты на следующий год так, чтобы они были ровно размещены, а не потребовали немедленного выполнения все сразу.

Конечно, непредвиденные проекты, такие как слияние или поглощение, всегда будут возникать, но мудрые старшие системные администраторы будут ожидать непредвиденное и оставят запас в расписаниях проектов, чтобы учесть такие ситуации.

Нетехническому директору следует требовать от старшего технического персонала, чтобы он имел в наличии план на год и держал его в курсе этого плана. Это дает ему возможность знать, какое количество денег доступно, если доступно, для этих проектов системного администрирования. Это также дает ему шанс найти средства на проекты от групп, которые заинтересованы в успехе этих проектов.

34.1.6. Технический персонал и процесс составления бюджета

Помимо создания старшими системными администраторами плана на год, важно вовлекать их в процесс составления бюджета. Старшие системные администраторы всегда должны уметь составлять подробный план расходов на следующий год, используя свой план на год, свои знания вопросов ежедневного обслуживания и роста, сроков разработки проектов и доступности персонала.

Привлечение старших системных администраторов к процессу составления бюджета дает им поле действия для выражения своего видения собственных областей деятельности. Это помогает директору составлять лучший бюджет, учитывая в нем все проекты, рост, затраты на обслуживание, о которых старшие системные администраторы осведомлены, вместо того чтобы удивляться им,

когда подразделению системного администрирования вдруг понадобятся деньги на что-то очень важное.

Это дает системным администраторам возможность объяснить, что им нужно и почему, а также получить некоторый контроль над финансированием своих областей деятельности. Кроме того, это раскрывает для них одну из сторон руководящей деятельности, что может быть полезно для тех системных администраторов, которые заинтересованы в том, чтобы стать руководителями.

Вовлекайте технический персонал в процесс составления бюджета

Директор группы инфраструктуры компании Synopsis привлекал архитектора из каждой технической области к своему процессу составления бюджета. Когда приходило время составлять бюджет, он просил своих архитекторов составить список проектов и сопутствующей работы, связанной с ростом и обслуживанием, которые они со своей группой хотели бы выполнить в следующем финансовом году. Им следовало расположить их в порядке приоритетности. Для каждого проекта они должны были оценить расходы основных и неосновных средств, а также количество людей, необходимых для достижения данной цели. Им следовало разделить эти расходы по кварталам финансового года, в которые предположительно они будут потрачены. Он также попросил их провести в списке черту. То, что находилось над чертой, требовало обязательного выполнения, а пункты под чертой были желательны для выполнения, но не являлись критически важными.

Он брал эти списки и использовал их для составления своего собственного списка по приоритетам, группируя некоторые элементы в одну строку и затем прочерчивая линию там, где ему казалось правильным. Он также добавил зарплаты и другую информацию, к которой был доступ только у него или за которую он отвечал. Этот список передавался директору группы, который составлял свой список, опираясь на свои источники, и т. д.

Этот директор обсуждал составленный список со всеми архитекторами, используя его в качестве средства, чтобы поддерживать их информированность о том, что происходит в других направлениях инфраструктуры. По мере составления бюджета он уведомлял архитекторов о состоянии списка и его элементов. Такой уровень вовлечения помогал архитекторам увидеть более общую картину того, что происходит в компании, и понять, почему некоторые элементы бюджета получали финансирование, а другие нет. Он также предоставлял архитекторам план на следующий год и позволял им решать, как обходиться без тех вещей, которые они оценивали как критически важные, но которые не получили финансирования, до возникновения проблем.

Этот поквартальный бюджет следует использовать для проверки прогресса группы по отношению к ее задачам. Запись этой информации в бюджетную электронную таблицу и предоставление к ней общего доступа помогает людям увидеть, что происходит в других областях. Если в течение года происходит что-либо непредвиденное, руководители могут воспользоваться таблицами, чтобы выяснить, как найти для этого средства.

В некоторых компаниях очень важно расходовать деньги в начале года, так как бюджет может быть сокращен в течение года, лишая всех или почти всех неизрасходованных средств. В таких компаниях системным администраторами следует планировать вторую часть года для работы над проектами, которые не требуют нового оборудования или используют оборудование, купленное ранее в этом году.

Некоторые компании также автоматически списывают определенную сумму от каждой бюджетной заявки. Например, высшее руководство может посмотреть на список проектов подразделения системного администрирования, которые, по его мнению, являются оправданными, а затем списать 25% от запрошенной суммы. Такой подход к формированию бюджета принят по всей компании, и поэтому все, кто знает о нем, добавляют к бюджету эту сумму, чтобы быть уверенными, что получат необходимое количество денег. В такой компании важно понимать, что бюджетные сокращения и расширения продолжаются. Нетехнический директор должен быть уверен, что понимает реальные потребности группы и делает все, что нужно, чтобы удовлетворить эти потребности. Если необходимо, ему следует добавить некоторые проекты, которые, по его мнению, оправданны, но без которых группа сможет справиться.

Как только бюджет утвержден и передан группе, важно, чтобы нетехнический руководитель передал ответственность за выполнение финансируемых задач, а также полномочия по использованию бюджета техническому руководителю. Если техническому руководителю передана только ответственность, но не полномочия на расход бюджета, он расстроится и вскоре покинет свой пост. Ничто не может быть унизительнее, чем наличие ответственности за что-либо и отсутствие полномочий для выполнения этой задачи.

34.1.7. Профессиональное развитие

Предоставление системным администраторам возможностей по профессиональному росту – один из ключевых методов повышения их удовлетворенности своей работой. Для компании выгодно держать их в курсе последних технологий и методов решения проблем, которые они встречают в повседневной работе. Кроме того, для компании выгодно улучшать навыки системных администраторов и держать их в курсе разработок и направления отрасли. К профессиональному развитию относится посещение соответствующих конференций, прохождение необходимых курсов, а также наличие подходящего набора книг. Нетехнический руководитель группы системного администрирования должен быть уверен, что каждому сотруднику доступно некоторое финансирование для профессионального развития.

Технологии быстро меняются. Некоторые утверждают, что 30% технических знаний, которые им необходимы, устаревают каждый год. Когда системные администраторы довольно долго не обучаются, им становится сложно выполнять свою работу. Установка системы этого года выпуска на основе прошлогодних знаний может быть крайне разочаровывающим занятием. Иногда это разочарование становится причиной моральных проблем и риска качества IT в вашей компании. Профессиональное развитие не стоит денег, оно приносит дивиденды.

Руководителям следует поощрять посещение техническим персоналом конференций и курсов для улучшения их навыков и понимать различия в направлен-

ности однодневных семинаров и недельных конференций. Однодневные семинары и тренировочные программы могут быть тактическими, сконцентрированными на конкретной технологии или навыке. Недельные конференции являются стратегическими и предоставляют возможности для обсуждения более широких тем.

Посещение конференций позволяет системным администраторам быть в курсе достижений индустрии посредством официальных презентаций, выставок производителей и просто общения с коллегами из различных компаний с целью обмена опытом. Преимущества так называемого кулуарного пути на конференциях – разговоров в кулуарах между сессиями, – при котором посетители делятся проблемами и идеями, нельзя переоценить. Конференция или семинар может быть очень интенсивным, но он также предоставляет системным администраторам некоторое удаление от своей работы и другой взгляд на нее, что также может помочь с неприятными проблемами. Обучение следует проводить вне рабочего места, чтобы его не прерывали. В идеале как конференции, так и семинары должны проводиться за пределами города, чтобы у системных администраторов была возможность сосредоточиться на профессиональном развитии и ни на что не прерываться. Им следует даже отключать свои мобильные телефоны и пейджеры во время сессий.

Начинающим системным администраторам часто очень полезно посещать курсы и конференции. Некоторые специализированные курсы могут быть полезны и для опытных системных администраторов. Помимо предоставления обучения, курс позволяет опытным системным администраторам полностью посвятить время – которое в другом случае они просто не смогли бы найти – глубокому изучению конкретной технологии.

Многие задачи системного администрирования требуют глубокого понимания работы протокола или конкретной технологии. Для системного администратора невозможно держать в голове все подробности о каждом протоколе или технологии, поэтому ему необходимо каждый раз обращаться к качественной справочной информации. У каждого системного администратора должны быть книги, которыми он пользуется чаще всего, и в идеале у компании должна быть большая библиотека книг по системному администрированию, к которым можно было бы обратиться.

Нам нравится наблюдать за компаниями, в которых каждый год каждому сотруднику выделяется определенное количество средств на профессиональное развитие. Оно включает в себя конференции, курсы и заказы на книги для каждого системного администратора. Такой подход подтверждает, что все системные администраторы могут выиграть от возможности развития. Привлекайте системных администраторов к определению того, как они хотят использовать выделенные им средства, и способствуйте им в реализации своих планов. Профессиональное развитие – в общих интересах, а поощрение заставляет системного администратора чувствовать себя значимой частью компании и ощущать, что его уважают.

Профессиональное развитие также обсуждается в разделе 32.1.4.

34.2. Тонкости

После того как были выстроены основы хороших взаимоотношений с техническим персоналом, нетехнический руководитель может попробовать несколько приемов, чтобы сделать эти взаимоотношения еще более непринужденными.

Кроме разработки подробного плана на год, нетехническому директору следует способствовать созданию техническим персоналом также и пятилетнего плана. Он должен найти способы связать эти планы с ежегодным планом, чтобы иметь уверенность, что средства, необходимые им для их проектов, появятся тогда, когда они понадобятся.

Нетехническому директору также следует установить взаимоотношения между каждым членом технического персонала, ориентированного на работу с пользователями, и пользователем, который может играть роль единственной точки контакта с целой группой. Также ему следует обеспечить, чтобы системный администратор назначал регулярные встречи с этим человеком для обсуждения актуальных тем и чтобы представитель пользователей помогал системному администратору в установке приоритетов задач пользовательской группы и разрешении споров о приоритетах между людьми в группе.

Нетехнический руководитель также должен знать, чем занимается технический персонал в его группе. Ему необязательно быть экспертом в технических областях, но понимание работы группы поможет ему общаться с персоналом и пользователями.

34.2.1. Пятилетний прогноз

В главе 5 мы упомянули, что, если системный администратор создает службу, он должен попытаться создать ее так, чтобы она работала от 3 до 5 лет, поскольку оборудование периодически устаревает – даже для систем без движущихся частей, а также потому, что организованный рост требует обновления технологий примерно с такой частотой. Следствие состоит в том, что ему будет необходимо обновлять службы примерно раз в 3–5 лет. Однако переустройство и обновление служб необходимо провести во всех проектах, которыми он занимается, и при этом ему все еще нужно уделять время ежедневному обслуживанию и поддержке пользователей.

Планирование проектов системного администрирования на 5 лет вперед – это хороший способ убедиться в том, что они проходят в правильное время. На пять лет вперед? «Но мы не знаем, что случится на следующей неделе!» В действительности есть множество долгосрочных вопросов, которые стоит принять во внимание. Сетевые технологии имеют тенденцию меняться так часто, что каждые 5–10 лет требуются новые кабели. Быстрый сервер, который вы установили в этом году, будет самым медленным через 5 лет, если машина вообще еще будет существовать. Сетевая скорость каждые несколько лет повышается на порядок, поддерживая темп роста процессорной скорости. Абсолютно новые парадигмы хранения данных меняются примерно каждые 5 лет[1]. Долгосрочные стратегии, которые подразумевают замену или обновление машины в строго определенные интервалы времени, следует пересмотреть, основываясь на том, как развиваются технологии. Обновления должны быть проведены до того, как служба начнет

[1] Интересно отметить, что каждый раз, когда требования к хранилищам данных вырастают на три порядка, требуется практически полностью изменить метод хранения данных, чтобы управлять дополнительным пространством. Непосредственно подключенное хранилище данных прекрасно подходило для мегабайтов, а подключаемые по сети хранилища позволили нам управлять гигабайтами данных; SAN позволяют нам управлять терабайтами информации, а без параллельных файловых систем не обойтись на уровне петабайтов.

разваливаться на части. Во множестве рабочих пространств ожидание бюджетных средств на конкретную службу иногда может растянуться на несколько лет, перед тем как эти затраты будут утверждены. Начать просить деньги до того, как группе они действительно понадобятся, может быть хорошим методом добавить уверенности в том, что проекты будут проведены в нужное время. Очевидно, что группе нужен пятилетний план, если нетехнический руководитель собирается искать средства заранее. Будьте осторожны и не распределяйте средства до того, как они действительно потребуются, или вы рискуете потерять их и не получить финансирование для других проектов в будущем.

Пример: правильно выбирайте время заявок на выделение средств

Старший сетевой администратор из компании Synopsis достиг совершенства в составлении расписаний и бюджетных заявок. Он научился точно предсказывать, сколько лет ему понадобится запрашивать средства на конкретный проект, прежде чем их выделят. Он мог даже приблизительно предсказать, сколько раз группа руководства оставит данный проект «за чертой», прежде чем их побеспокоит то, как долго они отказывали его новой службе или обновлению, и они поставят его «перед чертой». Он планировал проекты и начинал искать на них средства заранее, благодаря чему всегда мог завершить проект в нужное время.

Каждой группе необходим пятилетний план, который учитывает процесс составления бюджета и готовит высшее руководство к грядущим проектам. Лучше, чтобы это делал нетехнический руководитель, а не все подряд из старшего технического персонала.

Для пятилетнего плана нетехническому директору необходим технический персонал, который в состоянии прогнозировать, какие новые, перспективные технологии компания захочет использовать в будущем, когда технологии станут достаточно зрелыми, чтобы их стоило использовать, и когда пользовательский спрос на эти технологии сможет окупить затраты на них. Высшее руководство и пользователи узнают о новых технологиях и интересуются, когда компания собирается предоставлять соответствующую услугу. Для архитекторов важно быть в курсе новых технологий и степени их зрелости, чтобы помочь ответить на эти вопросы грамотно и исчерпывающе, если они будут заданы. Если архитектор сомневается или не знает хорошего ответа на вопрос, возможно, группу заставят внедрять технологию до того, как она станет достаточно надежной и терпимой. С другой стороны, системные администраторы получают много опыта и могут облегчить давление новой технологии, если их директор в состоянии ответить на такие вопросы следующим образом: «Мы ожидаем, что технология будет разработана до такого состояния, когда она станет достаточно полезной и стабильной для выполнения наших задач, через 18 месяцев, и мы планируем выполнить проект по проверке удовлетворения поставленным требованиям к этому времени. Мы будем запрашивать ресурсы на этот проект в бюджете на следующий год». Если он даст подобный ответ, ему придется обосновывать запрос времени, а также объяснять, почему группа уверена, что технология еще не готова для использования в компании. К беседе следует подключить архитектора, чтобы он мог предоставить подробности, необходимые директору.

Начинающие компании или компании электронной коммерции могут обнаружить, что планировать на 5 лет вперед невозможно, потому что риски слишком высоки. Однако в такой ситуации системные администраторы, скорее всего, будут гораздо ближе к главному исполнительному директору в представлении о том, как группа будет развиваться дальше. Это может сделать процесс получения долгосрочного прогноза проще, чем, например, в крупной компании, где системные администраторы удалены на 5 уровней управления вглубь от корпоративного стратегического планирования. Если стратегия компании в том, чтобы ее приобрели, ваш пятилетний план не должен включать слишком много вложений в долгосрочную инфраструктуру. Если эта стратегия в том, чтобы расширяться за счет открытия офисов продаж по всему миру, планы группы могут сконцентрироваться на различных потребностях, которые могла бы вызвать подобная среда, например построение WAN и центра управления сетью. Даже нечеткое видение будущего может предоставить группе лучшее направление, чем его полное отсутствие.

34.2.2. Совещания с единственным контактным звеном

Во многих частях этой книги мы говорили об общении между системными администраторами и их пользователями. Регулярное назначение встреч с единственным контактным звеном пользовательской группы для обсуждения актуальных вопросов – хороший метод частично формализовать общение. Это не заменяет дискуссий, связанных с проектами и запросами поддержки, и других специфичных обсуждений, которые системный администратор проводит со своими пользователями, а дополняет их. Директор организации системного администрирования должен потребовать от пользовательских организаций, чтобы те выделили единственное контактное звено для таких встреч.

Такие запланированные встречи играют роль концентрационного узла как для системных администраторов, так и для их пользователей. Перед каждым совещанием люди с обеих сторон должны потратить некоторое время на то, чтобы обдумать самим и обсудить с коллегами из соответствующих групп, о каких проектах, обслуживании или проблемах следует знать другой стороне. На совещаниях следует проверить состояние ранее рассмотренных проблем, а также обсудить новые темы и добавить их в список. Системный администратор может использовать этот список для определения приоритетов задач с пользователем и установить реалистичные цели для новых проектов.

Такие совещания предоставляют пользователям важное понимание того, над чем работают их системные администраторы. Они дают пользователям информацию о ходе больших проектов и помогают им понять, почему некоторые из их заданий могут завершиться позже, чем они этого хотели бы. Это позволяет кому-либо из пользовательского подразделения применять свои знания о работе группы для установки приоритетов. Людям в группе, у которых не конфликтуют сроки выполнения, следует решить между собой, что для них важнее, и сообщить об этом системным администраторам через их контактное звено. Подобный метод выделения приоритетов правильно распределяет ответственность за принятие таких решений, с самого начала формирует ожидания пользователей и должен приводить компанию к правильному принятию решений. Когда системных администраторов заставляют устанавливать приоритеты задач без какой-либо обратной связи с тем, кто действительно в курсе всех проектов, которые относятся к этим задачам, они могут принять неправильные решения или попытаться что-либо завершить в нереальные временные рамки.

Такие совещания, как правило, экономят время системных администраторов и пользователей, потому что они позволяют избегать активной электронной переписки или обсуждений по проверке состояния бессчетного количества задач, над которыми работают системные администраторы. Пользователи знают, чего ожидать и когда этого ожидать, и могут быстро получить обновленную информацию о состоянии от своего единственного контактного звена или, возможно, на веб-странице, если системные администраторы указывают там состояние. Кроме того, совещания являются средством укрепления доверия и взаимной уверенности. Никто не любит отправлять задачи в долгий ящик и надеяться, что они будут выполнены, или даже хуже – ожидать, что они не будут выполнены.

Пример: еженедельные встречи с пользователями экономят время

Один старший системный администратор неохотно начал устраивать еженедельные встречи с главой каждого подразделения в блоке групп, которые он поддерживал. Изначально встречи длились целый час, но по мере стабилизации рабочего процесса они превратились в 15-минутные совещания, на которых приводились сводки. Когда ожидалась большая перемена или возникала проблема, совещания занимали больше времени, пока вопрос не разрешался. Эти совещания помогали поддерживать сосредоточенность системных администраторов, что было важно для пользователей, а также помогали разъяснять пользователям моменты, которые были важны для системных администраторов, например необходимость потратить несколько больше времени на определенные проекты, чтобы убедиться, что они будут хорошо расширяться или могут лучше поддерживаться, и т. д. В результате удовлетворенность пользователей очень сильно возросла, так как они почувствовали, что системные администраторы их слушают. Как то раз системный администратор сказал человеку, который посоветовал ему проводить такие совещания, о своем сожалении, что раньше он им противился. «У меня такая же рабочая нагрузка, и я делаю такое же количество работы, но теперь пользователи гораздо довольнее, и я гораздо доволенее. С математической точки зрения это бессмыслица! Это магия!» Да, это магия.

Иногда пользователи будут избегать таких встреч, а некоторые станут активными противниками подобной идеи. В идеале они услышат от своих коллег, насколько полезными являются для них такие встречи, и поменяют свою точку зрения. В противном случае вы можете выбрать другие способы повышения качества общения с ними. Однажды глава подразделения отклонил подобное предложение и сказал: «Я доволен тем, что вы делаете. Разве я не жалуюсь, когда что-то не так?» В действительности у этого человека было хорошее представление о своих потребностях по управлению временем и он хорошо умел доносить проблемы до системных администраторов, не бросая их на произвол судьбы. Однако гораздо более необходимым было взаимодействие в другом направлении.

Тем не менее не все могут иметь действительно единственное контактное звено. Например, системные администраторы, которые отвечают за инфраструктуру всей компании в целом, не могут ожидать, что единственный человек на всю компанию будет в состоянии определить потребности всех сотрудников или

стать посредником в их спорах об установке приоритетов. Таким системным администраторам следует собирать все вопросы, относящиеся к инфраструктуре, от системных администраторов, которые непосредственно работают с пользовательской базой; а также им потребуется самим устанавливать приоритеты, не без помощи своего руководства. В особых случаях они могут собирать контактные звенья групп с конфликтующими требованиями и способствовать тому, чтобы те пришли к какому-нибудь единому решению. Руководитель организации системного администрирования также должен всегда быть готов помочь в таких вопросах.

34.2.3. Понимание работы технического персонала

Нетехническому директору следует делать все, что в его силах, чтобы понять, чем занимается его технический персонал. Ему не нужно становиться экспертом в данной области, но ему следует понимать и оценивать предпринимаемые действия и что из того, что от них требует он или их пользователи, относится к этим действиям[1]. Он сможет лучше общаться с техническим персоналом и пользователями группы, если понимает, что делает его персонал. Пользователи ожидают определенного уровня знаний от нетехнического директора, отвечающего за эту группу. Он должен стараться не разочаровывать их, так как это отразится на его группе. Он также сможет лучше представлять бюджетные потребности группы своему высшему руководству и увереннее договариваться с руководителями и пользователями от имени группы, если понимает работу своих сотрудников. Он будет принимать лучшие решения с этими знаниями. Группа будет более довольна тем, как он ее представляет, а также станет ценить любые попытки, которые он делает, чтобы понять то, чем она занимается.

Обучение помогает

Одному руководителю пришлось управлять группой технических сотрудников, чьи специальности относились к сферам, с которыми он до этого никогда не имел дела. У него были хорошие взаимоотношения с ними, но они заметно улучшились, когда он немного почитал об их работе и продемонстрировал им свое новое понимание.

34.3. Заключение

Успешные рабочие взаимоотношения между нетехническими руководителями и старшим техническим персоналом построены на общении и взаимном уважении. Работа нетехнического руководителя заключается в том, чтобы поддерживать моральный дух, защищая свою группу системного администрирования от политических проблем и поддерживая членов группы, заступаясь за них как в хорошие, так и в тяжелые времена. Руководители должны держать системных администраторов в курсе того, что происходит, особенно в областях, которые непосредственно относятся к работе системных администраторов, но при этом

[1] Эта книга может быть отличной отправной точкой для нетехнического руководителя, который хочет понять, чем занимаются системные администраторы!

не беспокоить их по каждому пустяку. Официальные совещания между техническим персоналом и их директором, а также между каждым системным администратором и его единственным связующим звеном с пользователями – хороший способ быть в курсе последних событий.

Создание ежегодных или пятилетних планов дает руководителям и пользователям уверенность в системных администраторах и лучшее понимание работы, которую они делают. Кроме того, это предоставляет руководителям возможность рассматривать выделение бюджетных средств на проекты, на которые рассчитывают системные администраторы, вместо того чтобы регулярно накладывать запреты из-за нехватки финансов. Вовлечение старших системных администраторов в процесс составления бюджета предоставляет им понимание того, как это происходит, что может помочь им при планировании и просто дать хороший опыт.

Задания

1. Как вы проверяете, были ли ваши приоритеты переданы системным администраторам?
2. Как вы заставляете системных администраторов выполнять их обязательства?
3. Каков ежегодный план вашей группы? Насколько хорошо бюджет ему соответствует? Как вы можете улучшить ситуацию?
4. Как ваша компания вложилась в профессиональное развитие персонала системного администрирования за последние 3 года? Как, по-вашему, это должно происходить в последующие годы?
5. Какие конференции, по вашему мнению, следует посетить членам вашего технического персонала? Какие преимущества они от этого получат? Как вы можете распределить между персоналом посещение конференций и при этом не подвергать опасности обслуживание на время этих конференций?
6. Если вы устраиваете регулярные совещания персонала, информируете ли вы их о последних событиях и обсуждаете ли темы, в которых ваша группа заинтересована? Как бы вы улучшили эти встречи? Если у вас нет регулярных встреч, что бы вы выбрали в качестве программы для их проведения и как часто проводили бы их?
7. Попросите свой старший персонал составить приблизительный пятилетний план. Сколько, по-вашему, будет стоить каждый из проектов в этом списке?
8. Основываясь на этом пятилетнем плане и на ваших знаниях о процессе составления бюджета, когда вы бы начали искать средства на финансирование каждого проекта?
9. Посмотрите на каждую из имеющихся в вашей компании организаций пользователей. Кто мог бы стать идеальным связующим звеном с вашими системными администраторами в каждой организации? Если у вас еще не настроена такая схема, попытайтесь установить взаимоотношения и проводить регулярные совещания о ходе процесса между соответствующими системными администраторами и единственным контактным звеном.
10. В истории в разделе 34.1.2 рассказывалось о защите группы системного администрирования, даже несмотря на пагубную ошибку, которая была сделана. Соотнесите ее с похожей ситуацию, с которой сталкивались вы, или опишите свои действия, если бы вы были директором в этой истории.

Глава 35

Наем системных администраторов

В данной главе рассмотрен наем системных администраторов, и основное внимание уделяется аспектам, которые чем-то отличаются от найма других сотрудников. Их нужно знать системным администраторам и руководителям. Об остальном должен позаботиться отдел кадров.

В данной главе не рассматриваются аспекты найма которые являются общими и применяются для всех сотрудников: заработная плата, оплата по вызовам, оплата за сверхурочную работу, отгулы или традиционные схемы вознаграждений, например право купить акции по льготной цене, премии при найме и премии за производительность. Также в данной главе не рассматривается, как в процесс найма могут быть вовлечены местоположение, стиль жизни, надомная работа, средства для удаленной работы или обучение и конференции.

Вместо этого в данной главе раскрываются основы того, как набирать сотрудников, проводить собеседование и удерживать системных администраторов. Кроме того, в ней рассмотрены меры, которые компания может предпринять, чтобы людям хотелось в ней работать.

35.1. Основы

Процесс найма можно упрощенно разделить на два этапа. Первый этап – определить людей, которых вы хотите нанять. Второй этап – убедить их, что они хотят на вас работать.

Определение тех, кого вы хотите нанять, – во многом более сложный этап. Чтобы определить, хотите ли вы кого-то нанять, вам сначала нужно узнать, чего вы хотите от нового сотрудника и насколько опытным он должен быть. Затем вам нужно набрать подходящих кандидатов, получив резюме от заинтересованных квалифицированных системных администраторов. Затем вам нужно собрать группу проведения собеседования, убедиться, что они соответствующим образом проинструктированы по процессу собеседования, и определить, кто какую информацию будет узнавать. Опрашивающие должны знать, как задавать специфичные вопросы кандидатам и как относиться к ним в процессе собеседования.

Второй этап, убеждение кандидата работать на вас, немного пересекается с первым. Самая важная часть привлечения кандидата – хорошее проведение собеседования. Опрашивающие должны показать кандидату все самое лучшее в компании и в его должности, и эти впечатления должны вызвать у него желание здесь работать. Время также должно быть подходящим, с нужными канди-

датами следует работать быстро. Наше рассмотрение мы завершим советами о том, как избежать найма за счет удержания персонала.

35.1.1. Должностная инструкция

Первый шаг в процессе найма – определить, почему вам нужен новый человек и что он будет делать. Выясните, какие пробелы есть в вашей организации. В главе 30 рассмотрены организационные структуры и построение гармоничной команды. Это рассмотрение должно помочь вам решить, с кем должен работать новый сотрудник и какие наборы навыков должны у него быть, чтобы они дополняли уже имеющиеся в команде навыки. Затем подумайте о том, исполнения каких ролей, описанных в приложении А, вы хотели бы от нового сотрудника. Это должно дать вам представление о типе личности и навыках, которые вам нужны. Из этого списка требований выясните, что является обязательным, а что желательным. Теперь у вас есть основа для должностной инструкции.

Составьте инструкцию для каждой должности, хотя это и требует много времени. Письменная должностная инструкция – это средство распространения информации. Его написание – это катализатор, который призывает сотрудников группы выражать свое видение должности, разрешать противоречия и останавливаться на четком определении. Однажды написанное, оно информирует потенциальных кандидатов о том, что будет представлять собой их работа. Во время собеседования оно помогает опрашивающим правильно расставить основные акценты. Когда приходится выбирать между двумя кандидатами одинаковой квалификации, должностная инструкция дает возможность принять более обоснованное решение.

Должностная инструкция должна включать две части: список обязанностей, который будет у человека, и список навыков, которыми ему необходимо обладать. Чтобы должностная инструкция была простой в написании и чтении, оформите ее в виде маркированного списка, в котором самые важные элементы будут находиться вверху. Однако не путайте должностную инструкцию с **объявлением о приеме на работу**, которое является общим описанием работы с добавлением контактной информации и всех остальных требуемых законом данных.

В разделе 9.1.1 мы выяснили, что документирование задач, которые вам не нравятся, упрощает их передачу другим людям. В следующий раз, когда у вас будет возможность найма, вы можете воспользоваться подобными документами для создания должностной инструкции. Список задач, которые вы документировали – и хотите передать другим, – можно добавить в список обязанностей. Навыки, необходимые для выполнения этих задач, можно добавить в список необходимых навыков. Должностная инструкция практически составляется сама собой.

С принятием сотрудника на вакантную должность связаны две конкурирующие теории. *Нанимать навыки* означает искать кого-то с точными навыками, указанными в должностной инструкции. Вы предполагаете, что годы спустя будете видеть, как этот человек выполняет ту же самую работу, для которой его наняли, без вариантов. *Нанимать человека*, напротив, означает искать и нанимать способных людей, даже если их конкретные навыки только пересекаются с тем, что перечислено в должностной инструкции. Если вы «нанимаете человека», вы делаете это за его интеллект, творческий потенциал и воображе-

ние, даже если ему не хватает некоторых конкретных способностей, связанных с должностью, на которую вы его берете. Эти люди могут удивить вас настолько значительным изменением работы, что будет требоваться гораздо меньше усилий, а результаты окажутся гораздо лучше, возможно, благодаря устранению ненужных задач, автоматизации рутинных процессов и нахождению общедоступных ресурсов для выполнения задач.

«Нанять человека» проще, когда у вас есть много вакантных должностей, каждая из которых требует различного набора навыков. Если у первого способного человека, которого вы наймете, будет несколько навыков из каждой должностной инструкции, вы можете перестроить должность под этого человека. У следующего способного человека, которого вы будете искать, должны иметься остальные навыки.

Обычно мы нанимаем главным образом старших системных администраторов в таких количествах, что занимаемся почти исключительно «наймом человека». Мы рекомендуем «нанимать навыки» только в особых тактических условиях.

Пример: когда надо «нанимать навыки»

В Bell Labs группа системного администрирования Тома «нанимала человека» на одни должности и «навыки» – на другие. Например, от старших системных администраторов ожидали творческого подхода к решению имеющихся проблем. Эти должности требовали «найма человека». С другой стороны, группе техников, которые устанавливали новые компьютеры, требовалось только запускать автоматизированные процедуры по загрузке ОС, а затем доставлять полностью настроенные компьютеры в нужный офис. Для этой функции лучше всего работал «наем навыков».

Стратегия найма человека работает только до какого-то предела. Убедитесь, что у вас найдется, чем занять этого человека. В одной компьютерной компании Силиконовой долины была стратегия найма талантливых людей и предполагалось, что они сами найдут себе проекты и будут творить чудесные дела. Однако вместо этого многие из нанятых сотрудников растерялись и почувствовали себя ненужными и обескураженными. Такая стратегия хорошо работает при найме исследователей и реформаторов, но не системных администраторов.

Некоторые кандидаты хотят, чтобы им очень четко объяснили, в чем будет заключаться работа, чтобы решить, хотят ли они ею заниматься и позволит ли она им достичь своих карьерных целей. Такие кандидаты откажутся от предложения о работе, когда обязанности будут нечеткими или непонятными им. Другим кандидатам хочется знать, есть ли в работе гибкость, чтобы они могли приобрести опыт в различных областях. В обоих случаях проводящим собеседование нужно знать, что включает работа и где она может быть гибкой, чтобы обе стороны видели, подойдет ли кандидат для этой работы. Будьте гибкими, если доступно несколько должностей. Некоторые кандидаты могут быть идеальными для части одной работы и части другой. Для максимального расширения возможностей обеих сторон проводящие собеседование должны знать все требования всех инструкций вакантных должностей, чтобы они могли поговорить с кандидатом о других вариантах, если это возможно.

35.1.2. Уровень навыков

После создания базовой должностной инструкции у вас должно быть разумное представление об уровне навыков, необходимом для должности. В идеальном случае установите соответствие между должностными инструкциями и уровнями навыков SAGE, описанными в их буклете *«Job Descriptions for System Administrators»* (Darmohray 2001). Это стало стандартным способом рассказывать о таких вопросах в должностных инструкциях, объявлениях и резюме.

Уровень навыков человека, которого вы нанимаете, имеет экономическое влияние. Чтобы сэкономить деньги, многие организации стараются нанимать для поддержки первого и второго уровня людей с минимально возможными навыками. Идея заключается в том, что самая распространенная должность должна стоить меньше всего и нанимать на нее стоит минимально обученных людей.

Другие организации предпочитают нанимать умных людей с хорошей мотивацией, которые находятся на грани избыточной для должности квалификации. Этих людей будет утомлять монотонная работа, и они станут устранять ее, создавая автоматизацию или рекомендуя изменения процессов, которые будут постоянно совершенствовать организацию. В сущности, эти люди с радостью выйдут за пределы своих обязанностей, поскольку знают, что их мотивация приведет их на другие должности в организации.

Талантливый, имеющий мотивацию системный администратор, который находится на грани избыточной квалификации, ценнее, чем два неопытных и лишенных мотивации системных администратора, нанятых для количества. Идеальный кандидат для младшей позиции – яркая и заинтересованная личность, которая недавно начала работать в этой области. Если вы будете вкладываться в таких людей и предоставите им возможность изучать и делать больше, их уровень навыков быстро поднимется, что предоставит вам идеальных кандидатов на повышение до более высоких должностей, которые может быть труднее заполнить. Если вам повезло и вы наняли таких людей, обеспечьте, чтобы их зарплаты и премии соответствовали их растущему уровню навыков, даже если это означает повышение в особом порядке помимо стандартных периодов повышения. Такие люди ценны, и их трудно заменить, и если вы не будете поддерживать это соответствие, их переманит другая компания. Кроме того, предоставление дополнительных повышений помимо стандартных в долгосрочной перспективе обеспечивает лояльность.

При перестроении плохо справляющейся с обязанностями группы важно нанимать ориентированных на преобразования сотрудников старшего звена, у которых есть опыт «правильной» работы, чтобы они с большей вероятностью работали по более высоким стандартам. Когда группа работает хорошо, вы можете позволить себе такую роскошь, как нанимать и старших, и младших сотрудников для заполнения различных специальностей. В истории «Когда дела совсем плохи, наймите кого-нибудь получше» из раздела 30.1.4 есть связанные с этим советы и примеры.

35.1.3. Подбор кандидатов

Как только вы решите, на какую должность вам требуется сотрудник и какой уровень навыков у него должен быть, вам нужно будет найти подходящих кандидатов для работы. Лучших кандидатов обычно находят по личным рекомендациям сотрудников группы системного администрирования или пользователей.

Рекомендация от пользователя обычно дает кандидата, успешного во всех аспектах работы, в том числе в общении с пользователями и доведении работы до конца.

Конференции по системному администрированию также являются подходящим местом для подбора кандидатов. Возможно, на конференции получится провести определенное собеседование, также кандидаты могут поговорить с сотрудниками группы системного администрирования, чтобы узнать, что они из себя представляют и какова работа в компании. Системные администраторы, посещающие такие конференции, часто являются хорошими кандидатами, поскольку они в курсе того, что происходит в их профессиональной сфере, и заинтересованы в обучении.

Упоминайте технологии, если вы хотите привлечь людей, которые их ценят. Объявления в газетах вряд ли привлекут опытных, высокотехнологичных сотрудников, которых вы ищете. По нашему опыту, объявления в Сети более эффективны, чем в газетах, даже если газету читает больше людей.

В Интернете полно сообществ, связанных с конкретными специальностями, во многих из них есть области объявлений о работе. Благодаря поиску людей в таких сообществах можно найти лучших кандидатов. Например, в сообществе FreeBSD есть список рассылки для его членов, которые ищут работу или предлагают ее.

Многие кадровые агентства специализируются на поиске системных администраторов, они могут иметь полезную базу данных системных администраторов и типов работы, которые их интересуют. Вакантные должности должны рекламироваться на собственном веб-сайте вашей компании. Если вы не разместите на своем сайте никакой информации о вакансиях, люди подумают, что вам никто не требуется. Есть много политических барьеров, которые затрудняют размещение на веб-сайте вакантных должностей, но вам стоит преодолеть эти препятствия.

Одна из проблем, которые часто возникают при найме системных администраторов, заключается в том, что отдел кадров не понимает резюме или должностные инструкции системных администраторов так, как сами системные администраторы. Самая лучшая компания по подбору персонала провалится, если резюме не пройдут через отдел кадров. Прекрасные резюме часто отклоняются даже до того, как их увидит группа системного администрирования, потому что кадровик не поймет, что резюме хорошее, особенно если компания пользуется компьютеризированной системой поиска и обработки резюме. Такие системы обычно настраиваются на поиск ключевых слов, и хороши, если вы хотите «нанять навыки», но неудобны, когда вам требуется «нанять человека» (Darmohray 2001). Наилучший способ обеспечить, чтобы хорошие резюме не пропадали, – выделить отдельного кадровика на наем системных администраторов и организовать его сотрудничество с системными администраторами и их руководителями, чтобы он понял, как выявлять хорошие и плохие резюме, что важно для той или иной должности и т. д. В конце концов, кадровик должен научиться просматривать резюме и выбирать все хорошие. Кадровик будет стараться уделять основное внимание ключевым словам, например, касающимся сертификации, конкретных технологий, продуктов и торговых марок. Мы пытались объяснять терминологию, в частности тот факт, что все слова Linux, IRIX, Solaris и AIX означают UNIX. Предоставить отделу кадров схему – простой способ помочь. Мы также обнаружили, что полезно давать персоналу отдела кадров копии буклета SAGE (Darmohray 2001).

После обучения руководители системных администраторов могут позволить кадровику работать самостоятельно и будут уверены в том, что он не пропустит хороших кандидатов. Поощряйте обученного вами кадровика, когда он достигает успеха. Обеспечьте, чтобы он был первым человеком в отделе кадров, которому модернизируют компьютер. Постарайтесь заинтересовать подобным обучением других кадровиков.

Некоторые компании вообще не доверяют оценку резюме отделам кадров. Вместо этого инженеры и руководители берут на себя оценку резюме и их распределение на группы «звонить», «не звонить» и «может быть». Это может быть особенно полезно, когда отдел кадров еще учится или когда наем не является постоянной задачей и обучение кадровиков не принесет большой выгоды. Убедитесь, что у вас есть механизм информирования отдела кадров, когда вы ожидаете резюме от кого-то, заслуживающего особого внимания: человека, известного в той или иной профессиональной области, специально подобранного кандидата или кого-то, привлеченного иным путем.

Иногда сотрудник, подбирающий персонал, или кто-то из отдела кадров первым говорит с кандидатом и опрашивает его по телефону. Важно обеспечить, чтобы этот первый контакт прошел хорошо. Сотрудник по подбору персонала, который знает, что нужно искать в резюме, также должен знать, как опрашивать по телефону.

Плохой опрос по телефону отпугивает кандидатов

В крупной компании-разработчике программного обеспечения опрашивали по телефону кандидата на вакансию по разработке программ. У кандидата была ученая степень по информатике и некоторый опыт разработки программ. Кадровик, опрашивавший кандидата по телефону, спросил его, как тот оценивает свои навыки программирования относительно других людей, с которыми он работал в исследовательской группе. Кандидат попытался объяснить, что в группе все хорошо программировали, но способность понимать и решать проблемы была более важным и актуальным навыком. Кадровик не понял, что тот сказал. В конце собеседования кадровик сказал кандидату, что с ним очень интересно разговаривать и что он никогда раньше не разговаривал с учеными, в отличие от программистов. В этот момент кандидат решил, что он ни за что не хочет работать в этой компании. После его отказа от вакансии ему несколько раз звонили различные руководители и сотрудники по подбору персонала, пытаясь убедить его, что ему будет интересна эта работа. Однако они продемонстрировали некоторую корпоративную заносчивость: даже после того, как он сказал, что устроился на другую работу, они не могли понять, почему он не заинтересовался работой в их компании, если *они* были заинтересованы продолжить собеседование с ним. Такое отношение укрепило его решение не работать в этой компании.

Если в вашей компании есть собственный сотрудник по подбору персонала, нужно организовать обучение. Лучшая кампания по подбору персонала в мире провалится, если потенциальные кандидаты будут считать вашего сотрудника по подбору персонала идиотом.

35.1.4. Время

При найме время – это все. Есть короткий промежуток, когда кто-то доступен для найма, и короткий промежуток, когда у вас есть вакантные должности. Ситуация, при которой эти промежутки полностью перекрываются и у вас есть возможность нанять человека, – практически чудо. Иногда должности освобождаются прямо после того, как прекрасный кандидат устроился в другое место или появляется замечательный кандидат, когда работа была предложена кому-то еще. Иногда несогласование времени неизбежно, но в других случаях неспособность компании быстро работать стоит ей потери лучших кандидатов.

При попытке привлечь системных администраторов в компанию, которая считает себя высокотехнологичной и интересной, у компании должна быть возможность быстро принимать решения о найме. Если компания долго принимает решения или у нее длинный, затянутый процесс собеседования, лучшие кандидаты успеют принять предложения от других. В некоторых компаниях трудовой договор подготавливают еще до того, как кандидат прибудет, особенно если он летит издалека. Предложение можно сделать сразу, и кандидат может остаться еще на день или два, чтобы при необходимости найти дом и школы.

Нужно найти равновесие между собеседованием с большим количеством кандидатов для поиска лучших и быстрым принятием решения при выявлении потенциально подходящего кандидата. Излишняя медлительность может привести к потере кандидата и его уходу в другую компанию, но слишком быстрое принятие решений может привести к найму неподходящего человека.

Не спешите с решением о найме

Средней компании по разработке программного обеспечения потребовалось нанять сетевого администратора для разработки сетевых средств. Группа провела собеседование с кандидатом, который имел достаточно хорошую квалификацию, но раньше работал с другим оборудованием. У него уже было предложение от другой компании. В группе знали, что решение надо принимать быстро, но не были уверены в том, что его навыки подойдут и что он сработается с коллективом. Группа хотела провести еще одно собеседование, но на это не было времени. Было принято решение взять его на работу, и он согласился. К сожалению, он не смог ни хорошо работать на этой должности, ни сработаться с группой. Группа попала в трудное положение из-за неверного решения, принятого в спешке. Если бы у группы было больше времени и она смогла бы провести еще одно собеседование, возможно, было бы принято решение не нанимать его.

Наем нового сотрудника – это долгосрочное обязательство, и оно требует времени для выбора подходящего человека. Если человек действительно заинтересован, он попросит у другой компании больше времени подумать над решением и ему позволят, боясь потерять его из-за излишней навязчивости. Все стороны должны уделять процессу найма необходимое время и позволять это другим.

Куй железо, пока горячо

Начинающая компания из Силиконовой долины обанкротилась и вынуждена была уволить всех своих сотрудников в пятницу утром. Один из них был известным системным администратором. Несколько компаний спешили его нанять. В течение следующей недели у него были первоначальные и последующие собеседования с несколькими компаниями, а в конце недели у него имелось несколько предложений и он принял решение. В одной из компаний, где он решил не работать, собеседование с ним проводили неподходящие люди, которые не были обучены проводить собеседования и непреднамеренно оттолкнули его. Другая компания, которая была очень заинтересована в том, чтобы его нанять, не могла работать так же быстро, как остальные, и ей не удалось до конца недели даже провести его собеседование с необходимыми людьми.

31.1.5. Условия коллектива

Важно убедиться, что человек, которого вы нанимаете, сработается с коллективом. Один из элементов этого – убедиться, что у него нет серьезных личностных конфликтов. Личностный конфликт может привести к тому, что люди не будут получать удовольствие от своей работы и станут использовать свою энергию негативно, что снижает моральный дух в группе. В главе 34 более подробно рассмотрено, почему низкий моральный дух вреден для коллектива. В буклете SAGE *«Hiring System Administrators»* (Philips and LeFevbre 1998) прекрасно рассмотрена психология найма и то, как каждый новый сотрудник, который присоединяется к коллективу, меняет динамику группы.

Иногда такое решение трудно принять, потому что очевидных личностных конфликтов может не быть, но по стилю работы кандидат отличается от остальной группы. Здесь должно помочь внимательное рассмотрение должностной инструкции до собеседования с кандидатами. Стиль работы кандидата может быть чем-то, чего не хватает группе, и в результате все, проводящие собеседование, будут знать, что это желательное качество.

Проверка «Dilbert»

В одной группе всегда просили кандидатов «рассказать сюжет своего любимого комикса “Dilbert”», чтобы узнать, впишется ли человек в ее веселую культуру. «Правильного ответа» не было, но комикс, выбранный кандидатом, говорил о многом. Иногда он показывал, с какими людьми кандидат не хотел бы работать, на какого персонажа он больше всего похож или какой была его нынешняя обстановка на работе. Самое главное, это показывало, мог ли человек шутить. Никто из кандидатов не отвергался только потому, что не любил «Dilbert», однако интересно заметить, что однажды был нанят кандидат, который никогда не слышал про «Dilbert», и по какому-то удивительному совпадению он не сработался с группой и ему пришлось искать работу в другом месте. Мы не призываем не нанимать кого-то только из-за того, что он не слышал про «Dilbert»,

но этому человеку потребуется особое обучение и выделение небольших денежных средств на покупку последней книги Скотта Адамса.

Еще одна проверка «Dilbert»

Один кандидат всегда рассматривал комиксы на стенах офисов и блоков в компании, где проходил собеседование. Люди склонны считать комиксы более смешными, когда они связаны с происходящим в компании. Изучение комиксов предоставляло ему хорошие данные о том, какова на самом деле была работа в компании.

Знайте, что вы ищете

В одной средней компании пытались нанять второго человека в группу безопасности. Организация системного администрирования была молодой, динамичной, быстро работавшей и растущей группой. Руководитель системного администратора по безопасности возложил на него ответственность за выбор подходящего кандидата для группы безопасности. Однако руководитель не дал указаний или советов о том, чего не хватает в организации. Системный администратор опросил одного кандидата, который имел хорошую квалификацию, но решил не брать его, потому что не был уверен, что тот сработается с коллективом. Он был спокойным, надежным работником, который всегда внимательно изучал и рассматривал все варианты, тогда как остальная группа системного администрирования состояла из людей, которые принимали быстрые решения, почти всегда оказывавшиеся хорошими, но иногда имевшие негативные последствия. Он не был уверен, что такой человек хорошо впишется в коллектив. Потом он понял, что это был идеальный кандидат как раз из-за такого отличия в стиле.

Еще один аспект разнообразия группы связан с культурными и национальными различиями. Разнообразием группы можно управлять для получения отличных результатов. Каждый сотрудник коллектива приносит свою уникальную историю и прошлое, и эти различия обогащают группу. Это одна из причин, почему группа может принимать лучшие решения, чем отдельный человек. Мы все выросли с различным опытом, основанным на нашем уровне благосостояния, национальной культуре, стабильности и многих других факторах. Этот опыт влияет на наш процесс мышления, из-за него мы все думаем по-разному. Если бы у всех нас был одинаковый жизненный опыт и мы думали одинаково, мы были бы избыточными; вместо этого можно использовать разнообразие как сильную сторону.

Три различных истории

У трех системных администраторов, которые работали вместе, было очень разное воспитание. У одной были строгие, религиозные родители, которые дали ей упорядоченное воспитание. Поэтому порядок предоставлял

ей комфорт и безопасность: прежде чем она могла двигаться дальше, все должно быть подробно документировано. Другого родители выгнали из дома подростком, когда узнали, что он гей. Ему пришлось выживать самому, он сопротивлялся порядку и ценил уверенность в своих силах. Третий системный администратор вырос в очень неупорядоченной семье, которая много ездила по стране. Он хотел порядка, но ожидал непредвиденных изменений. В результате у каждого из трех человек были относительно предсказуемые рабочие привычки и стили проектирования. Поскольку они смотрели на эти различия как на наличие большого количества элементов в их наборе, это приносило значительные результаты. В любой структуре должно было быть достаточно порядка, чтобы удовлетворить первого человека, каждый компонент должен был быть достаточно надежным, чтобы соответствовать характеру второго, и система должна быть способна достаточно хорошо справляться с изменениями, чтобы понравиться третьему. Когда нужно было написать документацию, они знали, кто проследит за ее полнотой. Такая ситуация могла бы стать катастрофой, если бы приводила к несогласованности, но вместо этого разнородность стала сильной стороной группы.

Руководитель должен создать среду, которая поддерживает и приветствует разнообразие, а не пытается подогнать каждого под одни и те же критерии. Создайте стремление слушать и понимать. Призывайте сотрудников группы понимать друг друга и находить решения, которые устраивают всех.

Четыре взгляда на мир

Однажды Том проводил собеседование с самой успешной инженерной группой в своем подразделении, чтобы найти секрет ее успеха. Один из инженеров сказал, что все четверо имеют различное религиозное прошлое, каждое из которых дало им различный взгляд на мир. Он считал, что это было самой сильной стороной группы. Для одного человека бог был внутри всех нас, для другого он смотрел на всех сверху заботливым взглядом, еще один бог был центром всего сущего, а последний был недостижим ни для кого, кроме нескольких человек. Эти взгляды на мир отражались в том, как они относились к инженерным проблемам. Несмотря на то что у них были различные взгляды на мир, все они согласились, что ни один из них не является подходящей аналогией для любой инженерной проблемы. Вместо этого все могли провести собственный анализ проблемы, пользуясь очень различной философией. Когда они собирались, чтобы поделиться результатами, проводился очень тщательный анализ. В результате проходили обсуждения, которые помогали каждому сотруднику получить более глубокое понимание проблемы, потому что каждый человек находил различные вопросы и решения. Когда они собирались вместе, они могли создать решение, содержащее все наилучшее из работы каждого.

Другой не менее важный аспект коллектива – обучение и предоставление возможностей для карьерного роста младшим сотрудникам группы. Младших системных администраторов нужно обучать, также им нужна возможность расти и демонстрировать свои таланты, особенно на первой работе по системному администрированию. Иногда полезно рискнуть и нанять младшего системного администратора, у которого, возможно, имеется потенциал, если для него есть подходящий наставник, который может быть назначен на эту роль до выхода нового сотрудника на работу. Никогда не нанимайте младших системных администраторов на должности, на которых за ними не будут внимательно наблюдать и проводить ежедневное обучение. Люди, нанятые на такие должности, не будут получать от своей работы удовольствие и часто станут совершать ошибки, которые придется исправлять другим людям. Нанимать начинающих сотрудников на должность системного администратора и давать им привилегированный доступ – это путь к катастрофе, и они скорее создадут больше работы для других, чем облегчат нагрузку.

Почему начинающим системным администраторам нужны наставники

Начинающий интернет-провайдер разделил свою организацию системного администрирования на две части, чтобы избежать конфликта приоритетов. Одна группа занималась обслуживанием пользователей Интернета, а другая следила за корпоративными системами и сетями. Старшие системные администраторы переходили из корпоративной группы в группу обслуживания пользователей, и в какой-то момент в корпоративной группе осталось только двое начинающих системных администраторов. Старшие системные администраторы из группы обслуживания пользователей отвечали на вопросы этих новичков и по возможности помогали им, но их основным приоритетом было поддержание работоспособности службы. Однажды корневой раздел корпоративного почтового сервера заполнился. Младший системный администратор, который обнаружил проблему, обратился за помощью к старшим системным администраторам, но они все были сильно заняты какой-то важной работой по обслуживанию и не могли уделить ему много времени. Он решил, что стоит найти несколько больших файлов, которые, скорее всего, не очень интенсивно использовались, перенести их в другой раздел диска и создать на них ссылки из первоначального местоположения. К несчастью, он выбрал общие библиотеки (UNIX-аналог DLL-файлов в Windows), не зная, что это такое и к чему приведет их перемещение.

Когда он перенес библиотеки, то обнаружил, что не может создать на них ссылки, потому что команда больше не работает. Пока он пытался разобраться, что было не так, он обнаружил, что не работает ни одна команда, которую он пытался выполнить. Он решил попробовать перезагрузить систему, чтобы проверить, не устранит ли это проблему. Конечно же, система не смогла загрузиться без общих библиотек, что ухудшило ситуацию. В конце концов он разобрал почтовый сервер и другую систему в серверной, чтобы попробовать загрузить машину и вернуть ее к рабочему состоянию. По закону подлости в самом разгаре этой работы, когда

компьютерные запчасти были разбросаны по полу, в серверную вошла телевизионная съемочная группа, снимавшая репортаж о компании, и посчитала, что системный администратор подходит для интересного сюжета. Это сделало еще кошмарнее и безнадежнее и без того ужасную ситуацию.

В конце концов, когда корпоративный почтовый сервер не работал несколько часов и высшее руководство выразило неудовольствие, один из старших системных администраторов группы обслуживания пользователей смог оторваться от работы и помочь устранить проблему. Кроме того, он потратил время на то, чтобы объяснить, что такое общие библиотеки и почему они так важны. Если бы у младшего системного администратора был наставник, который мог бы проводить с ним больше времени и помогать в таких проблемах, ситуация была бы разрешена быстро, без долгого отключения и смущающего телевизионного сюжета.

35.1.6. Группа собеседования

Для правильной оценки кандидатов опрашивающие должны работать вместе, чтобы определить, есть ли у человека необходимые технические навыки и личностные качества и подойдет ли он коллективу. Это еще одна ситуация, в которой важную роль играет должностная инструкция. Каковы точные навыки, ожидаемые от кандидата? Разделите желательные навыки на небольшие взаимосвязанные группы и выделите одну группу каждому из проводящих собеседование. Выбирайте опрашивающих по их способности опрашивать и оценивать кандидатов по определенной группе навыков. Некоторые люди опрашивают лучше других. Если вы нанимаете много сотрудников, убедитесь, что опрашивающие не будут полностью загружены первоначальными собеседованиями. Постарайтесь сохранить их для последующих собеседований. Убедитесь, что все опрашивающие знают, о каких навыках они беседуют и о чем говорят другие люди, чтобы обеспечить полное покрытие и минимум пересечения. Только действительно важные навыки можно выделять более чем одному человеку. Если на беседу об одном и том же навыке выделено два человека, убедитесь, что они задают разные вопросы. Убедитесь, что опрашивающие смогут дополнять друг друга, оставаясь в своих сферах компетентности, чтобы они комфортно себя чувствовали в групповой роли.

Если у вас есть много вакансий, пусть группа собеседования работает по навыкам, необходимым для всех должностей. Возможно, заполнение всех рабочих мест займет некоторое время. По мере заполнения рабочих мест поиск можно сужать, а диапазон необходимых навыков может быть ограничен теми, которые требуются для закрытия пробелов, оставшихся в диапазоне навыков группы системного администрирования. Если должностей много, опишите кандидату их все и, если это допустимо, покажите возможность перераспределения обязанностей. Выясните, какие должности кандидат считает самыми интересными и подходящими для своих навыков.

Как кандидаты, так и сотрудники группы захотят знать, с кем они будут работать. Очень важно, чтобы во время собеседования кандидаты проводили время с человеком, который будет их руководителем, и с людьми, с которыми они будут взаимодействовать наиболее тесно. Дайте кандидату возможность встре-

титься с максимально возможным количеством сотрудников группы, не делая процесс подавляющим и утомительным. Рассмотрите возможность добавления в группу собеседования внутреннего пользователя, что поможет кандидату и вашим отношениям с пользователями. Приведите кандидата на обед с двумя или тремя системными администраторами. Это предоставит ему возможность узнать некоторых из его возможных коллег в более непринужденной обстановке, что поможет ему решить, хочет ли он работать в вашей группе. Одна из распространенных ошибок – игнорировать человека за обедом. Убедитесь, что вы стараетесь вовлекать кандидата в разговор. Задавайте открытые вопросы, чтобы заинтересовать его беседой с группой.

Вовлекайте кандидата

Однажды Том работал в компании, где кандидатов всегда брали на обед со всей группой, чтобы узнать, хорошо ли кандидат впишется в коллектив. Тому было противно смотреть на то, что с человеком никто не говорил. Том пытался вовлечь кандидата в разговор, но его сразу же кто-то перебивал и внимание отводилось от кандидата. В результате Том провел курс обучения «Как правильно обедать», чтобы научить всех пользоваться такими полезными фразами, как «О, это интересно, расскажите об этом подробнее».

35.1.7. Процесс собеседования

Самое важное, что должны помнить проводящие собеседование, – нужно уважать кандидата. Кандидат всегда должен уходить с ощущением, что собеседование стоило потраченного времени и что люди, с которыми он говорил, были теми, с кем он хотел бы работать. У него должно складываться впечатление, что собеседование с ним было самым важным делом для тех, кто его проводил. Помните, вам нужно, чтобы кандидаты хотели с вами работать. Вам нужно, чтобы они рассказывали своим друзьям, что в вашей компании здорово работать. Они должны уходить из здания с незатронутым чувством собственного достоинства и симпатией к компании. Вот другие способы показать уважение:

- *Прочтите резюме перед собеседованием.* Ничего так не раздражает местного кандидата, как вопросы о том, как прошел перелет, или обсуждение того, что было явно указано в резюме.
- *Приходите на собеседование вовремя, не заставляйте кандидата ждать.* Кандидат выделил на собеседование много времени, не заставляйте его думать, что это было зря.
- *Перед встречей с кандидатом выключите все рации, пейджеры и сотовые телефоны.* Ваша компания сможет час прожить без вас, даже если она так не считает. Вам не нужно, чтобы кандидат подумал, что в компании творится бедлам и его тоже не оставят в покое ни на минуту. Точно так же и вам не нужно тратить ценное время собеседования на то, чтобы беспокоиться о проблемах в компании или устранять их.
- *Проявляйте внимание к кандидату.* Легко ли он нашел здание? Были ли пробки на дороге? Какое у него впечатление от тех, кто проводит собеседование? Не хочет ли он выпить кофе или прерваться ненадолго?

- *Убедитесь, что все задают разные вопросы.* Это демонстрирует кандидату взаимопонимание и сплоченность группы. Это показывает, что процесс собеседования был продуман и подготовлен. Постоянные ответы на одни и те же вопросы – пустая трата времени кандидата. Кроме того, задавание разных вопросов дает опрашивающим более широкое представление о кандидате при дальнейшем сравнении записей.
- *Не пытайтесь доказать, что вы знаете больше.* Смысл собеседования в том, чтобы узнать, как много знает кандидат, а не показать вашу собственную уникальность или попытаться поймать его на какой-то незначительной мелкой подробности, с которой большинство системных администраторов никогда не встретятся в своей работе.
- *Упрощайте разговор для кандидата.* Начните с относительно простых вопросов, чтобы он смог почувствовать уверенность в себе, и постепенно усложняйте их. Такой процесс даст вам хорошее представление об уровне навыков кандидата, а кандидату предоставит возможность показать свои реальные навыки, а не занервничать и все забыть. Показать истинные навыки кандидата в интересах обеих сторон.
- *Не продлевайте страданий.* Если вы обнаружили недостаток знаний кандидата в одной области, отступите и поговорите о его опыте в другой области. Дайте ему возможность восстановить уверенность в себе, прежде чем проверять его подготовленность.
- *Старайтесь сразу рассеивать все свои сомнения.* Если вы затрудняетесь определить, как человек поступит в той или иной ситуации, лучше постараться выяснить это во время собеседования, когда у вас есть возможность задавать различные вопросы, чтобы подтвердить или опровергнуть свои подозрения.

Заботьтесь о кандидате

Начинающая интернет-компания проводила собеседование со старшим системным администратором, который был лично рекомендован и подобран двумя самыми старшими системными администраторами в компании. Собеседование шло с 6 до 10 ч вечера. Сотрудники начинающей компании все время работали допоздна и всегда заказывали ужин в офис в близлежащих ресторанах. Во время собеседования кто-то спросил сотрудника, проводящего опрос, не хочет ли тот поужинать, но не поинтересовался об этом у кандидата, который тоже ничего не ел. Другой опрашивающий принес свой ужин и начал есть прямо перед кандидатом, и не думая спрашивать, не хочет ли тот чего-нибудь перекусить. То же самое произошло на втором и третьем собеседованиях. Кандидату предложили работу, и все были очень удивлены, когда он отказался. Впоследствии он рассказывал другим об этом ужасном собеседовании и встретил тех, кто тоже побывал в подобной ситуации и также отказался от работы в компании.

Успешное собеседование требует подготовки, практики и координации. Записывайте свои мысли о собеседовании и кандидате сразу же после завершения собеседования. Это даст вам самые свежие и точные данные о кандидате, когда группа соберется и будет решать, кого нанимать. Кроме того, это предоставит

возможность подумать о вопросах, которые не были заданы на собеседовании, и попросить тех, кто будет проводить дальнейшее собеседование, выяснить эти вопросы.

Одна из наиболее серьезных ошибок, которые делают компании, – это «реклама компании» только после того, как будут заданы вопросы, определяющие, достаточно ли кандидат квалифицирован для работы. Они считают, что все остальное – это пустая трата времени на людей, которых не будут нанимать. В результате квалифицированные кандидаты уходят с собеседования с мыслью «Какая ужасная компания!» или «Какое сборище придурков!». Вместо этого начинайте каждое собеседование, рассказывая, какая у вас замечательная компания и почему лично вам она нравится. Это пробуждает в кандидате желание получить работу, расслабляет человека и обеспечивает более плавное собеседование. Кроме того, это показывает вас в лучшем свете. Если кандидат недостаточно квалифицирован для должности, у него могут быть достаточно квалифицированные друзья. Кроме того, недостаточно квалифицированный человек может обучиться в ходе дальнейшей работы и будет очень жаль, если вы отпугнете его от своей компании одним плохим собеседованием.

35.1.8. Техническое собеседование

Техническое собеседование позволяет выяснить, есть ли у кандидата знания и навыки, необходимые для работы (нетехническое собеседование рассмотрено ниже).

Для опроса кандидатов об их технических навыках следует выделить специальных сотрудников. В такой широкой области, как системное администрирование, эта задача может быть достаточно сложной. Однако должностная инструкция должна обеспечить основу для подхода к техническому собеседованию. Например, оно должно определять, нужны ли человеку конкретные технические навыки и опыт или более общие навыки по решению проблем. Техническое собеседование на должность разработчика архитектуры должно выявлять навыки по проектированию, а не подробные знания о последнем оборудовании от конкретного производителя.

Опрашивающие сотрудники должны задавать вопросы на правильном уровне. Разработчикам архитектуры следует давать архитектурную проблему и обсуждать с ними, с какими проблемами они сталкиваются и как они их решают. Для старших системных администраторов проводящий собеседование должен выбрать общую для них область технических знаний и задавать вопросы по всей глубине. Помимо умения выполнять задачи проверьте навыки решения проблем и способность объяснить, чем занимается кандидат. У системных администраторов среднего уровня должен быть достаточно широкий опыт, навыки решения проблем и способность объяснить, что они делают. Младшие системные администраторы должны показать, что помимо выполнения своей конкретной работы они пытались понять, что они делали и как все работает. Ищите методичных и внимательных к деталям младших системных администраторов. В собеседовании с неопытными системными администраторами ищите тех, кто интересуется компьютерами и тем, как вообще все работает. Писали ли они компьютерные игры или разбирали свой домашний компьютер?

При поиске навыков решения проблем может быть полезно узнать, понимает ли кандидат, как работает что-то помимо компьютеров. Попросите человека объяснить, как работает пара устройств повседневного пользования, например

двигатель внутреннего сгорания или сливной бачок. Узнайте, что еще ремонтировал кандидат. Может ли он починить сломанные электроприборы, забившиеся раковины или мебель? Знает ли он, как менять в своей машине масло или выполнять какую-то небольшую работу по ее обслуживанию? Некоторые считают, что умение читать ноты демонстрирует логическое, методическое мышление и хорошие навыки по решению проблем. Найдите творческие способы определить способ мышления кандидата. Спросите его, почему крышки люков круглые, и следите за ходом мысли и логикой человека по мере того, как он обясняет это. Попросите кандидата оценить количество факсов в Манхэттене и следите за логикой, которой он пользуется для выполнения инженерных оценок.

Всегда хорошо ознакомиться с предыдущим опытом кандидатов и узнать их мнения о нем. Например, вопрос о том, каким своим достижением они больше всего гордятся и почему, может дать вам хорошее представление о том, что они могут и что считают сложными проблемами. Спросите их о ситуациях, в которые они попадали и в которых хотели бы поступить по-другому, а также о том, что бы они теперь сделали иначе и почему. Вам нужно убедиться, что они умеют учиться на своих ошибках. Попросите кандидатов описать серьезную проблему, которую им пришлось устранять: как она появилась, как они с ней справились и в каких условиях им приходилось работать при ее решении. Кандидатам нравиться рассказывать истории из своей жизни, а вам они покажут, как кандидаты думают и работают. Попросите их рассказать вам о большом проекте, над которым они работали в одиночку или в группе. Если вы заинтересованы в конкретном навыке, спросите кандидатов о проблеме, которую требовалось решить в этой области. Спросите их о сложной проблеме, с которой вы столкнулись в этой области, и посмотрите, как бы они к ней подошли. Больше всего старайтесь говорить с ними об их опыте из реальной жизни. Это проще и интереснее для них и предоставляет вам лучшее представление о том, что они могут, чем сухие вопросы «Как это работает?».

Не задавайте «мелочные» вопросы – вопросы с единственным, точно определенным правильным ответом. В стрессовой ситуации люди могут забыть его. Если их работа требует от них знания, какой контакт интерфейса V.35 используется для передачи данных, они могут найти это, когда им понадобится. Общие вопросы позволяют вам больше понять о кандидатах, чем детали. Вопросы о деталях также называются вопросами на засыпку, потому что очень заманчиво сказать «Попался!», когда кандидат не знает ответа.

Мы также не любим вопросы-головоломки. Нас раздражает, когда мы видим, как в компаниях просят кандидатов соединить девять точек, расположенных рядами 3×3, четырьмя прямыми линиями, не отрывая карандаша от бумаги (*www.everythingsysadmin.com/p/e*). Эти вопросы не имеют никакого отношения к тому, может ли человек выполнять конкретную работу. На самом деле мы утверждаем, что они проверяют лишь то, слышал ли кандидат этот вопрос раньше.

Секрет хорошего собеседования – в уточняющем вопросе. Вопросы, которые вы задаете первоначально, могут быть пустяковыми по сравнению с последующими вопросами, которые вы задаете после ответа кандидата. Вот пример:

Опрашивающий: Вы знаете C++?

Кандидат: Да.

О: Вы знаете, как настроить MS-Exchange?

К: Да.

О: Вы знаете Apache?

К: Да.

О: Вы знаете PHP?

К: Да.

О: Вы знаете брандмауэры SonicWall?

К: Да.

Вау! Какой замечательный кандидат. Он знает все, от программирования на C++ до настройки веб-серверов, почтовых серверов и даже брандмауэров! Однако мы не задали никаких уточняющих вопросов. Теперь давайте посмотрим, как уточняющие вопросы позволяют собрать в процессе собеседования более точную информацию.

Опрашивающий: Вы знаете C++?

Кандидат: Да.

О: Какую самую большую программу на C++ вы написали?

К: Программу из 200 строк, которая преобразовывала CSV-файлы в шаблон.

О: Что заставило вас выбрать C++? Почему вы не воспользовались таким языком, как Perl?

К: Это было домашнее задание по курсу C++. У меня не было выбора.

О: А как насчет программ на C++, которые вы писали вне учебы?

К: На самом деле я не очень много писал на C++.

О: В каких ситуациях вы могли бы предпочесть C++ другим языкам?

К: Я не знаю. C++ сложный, я бы лучше выбрал что-нибудь попроще.

О: У вас есть опыт работы с Apache?

К: Да.

О: Вы поддерживали систему Apache или настраивали ее с нуля?

К: С нуля. Я загрузил пакет и установил его на системе Linux. Затем я поддерживал сайт для компании. Дизайн был выполнен консалтинговой фирмой, но мне нужно было устранять проблемы с ее HTML-кодом и изменять конфигурацию для работы с ее CGI-скриптами.

О: Когда я запускаю Apache, я вижу много подпроцессов. Что они делают?

К: На самом деле я никогда не задумывался об этом.

О: Что вы можете предположить?

К: Может быть, каждый из них обрабатывает свой запрос?

О: Зачем это нужно?

К: Чтобы разделить нагрузку.

О: Ну, у машины только один процессор. Почему несколько процессов поможет?

К: Я не знаю.

О: Давайте сменим тему. Вы работали с брандмауэрами SonicWall?

К: Да.

О: В общих чертах, как работает брандмауэр?

К: (Кандидат дает очень подробное техническое описание того, как работает брандмауэр).

О: В каких ситуациях может заполниться таблица состояний?

К: (Кандидат рассказывает про долгие соединения, превышение времени ожидания и способы настройки времени ожидания соединения. Он также объясняет обработку пакетов FIN и другие подробности).

Так как мы использовали уточняющие вопросы, у нас сложилось гораздо более ясное представление об истинных навыках человека. Мы видим, что у него есть зачаточные навыки программирования на C++, которые не использовались с колледжа. По крайней мере, человек понимает некоторые принципы программирования. Знания кандидата о веб-серверах Apache весьма поверхностны, но достаточны для запуска простого веб-сервера. Он ничего не знает о внутренних рабочих процессах Apache, что было бы полезно для крупных процессов по расширению или устранения необычных проблем, но опыт изменения конфигурации, чтобы работали CGI-скрипты – если это не делалось через меню, – показывает реальное понимание. Наконец, вопросы про брандмауэры показывают, что кандидат обладает глубокими знаниями по этой теме и не только понимает, как они работают, но и имеет опыт работы с распространенной проблемой расширения.

На самом деле никто не проводит собеседование так плохо, как в предыдущем примере. Мы преувеличили нехватку уточняющих вопросов, но нам приходилось видеть собеседования, которые проводились очень близко к этому. Однако второй пример показывает другой недостаток в подходе опрашивающего: очевидно, он не был хорошо подготовлен. Предварительное изучение резюме кандидата показало бы, что он инженер по сетям или безопасности, и вопросы должны быть направлены в эти области. Вопросы про C++ и Apache были бы неплохими для дальнейшего собеседования, чтобы увидеть широту знаний кандидата. Однако задавание вопросов в таком порядке могло обеспокоить кандидата тем, что он проходит собеседование не на ту работу.

Определяйте пределы знаний кандидата, задавая все более и более глубокие вопросы, пока человек, наконец, не скажет: «Я не знаю». Недостаток такого подхода заключается в том, что кандидаты могут подумать, что по каждой теме, которую вы обсуждали, они не смогли ответить на последний вопрос, в то время как вы будете довольны тем, что их «предела» вполне хватает.

Определение предела знаний кандидата в тех областях, где они чувствуют себя наиболее сильными, – прекрасный способ оценить их основные знания. Затем задавайте вопросы по связанным темам, чтобы определить, насколько широкими являются их знания. Чтобы определить начальную тему, спросите их, в чем они считают себя наиболее сильными: например, в сетевых протоколах (как они работают), сетевом оборудовании, внутренней структуре операционной системы или написании скриптов. Темы должны быть основаны на опыте, описанном в их резюме. Попросите их назвать свою самую сильную область.

Не просите их оценить свои навыки по десятибалльной системы для каждой темы. Исследования Крюгера и Даннинга (Kruger and Dunning 1999) показали, что неопытные люди не знают о недостатке своих навыков и будут их переоценивать, тогда как более опытные люди лучше осведомлены о пределах своих знаний.

Просьба к кандидатам оценить свои навыки

Просьба к кандидатам самостоятельно оценить свои навыки может помочь показать их уровень уверенности в себе, и ничто другое. Вы не знаете, с чем они сравнивают. Некоторые люди были воспитаны так, что их всегда учили преуменьшать свои достоинства. Однажды менеджер по персоналу практически упустил кандидата, который сказал, что не слишком много знает про Macintosh. На самом деле он пользовался Macintosh 8 ч в день и поддерживал четыре приложения для своего подразделения, но не знал, как для них программировать. Лучше просите людей рассказать о своем опыте.

35.1.9. Нетехническое собеседование

Для нетехнического собеседования может быть особенно полезным пройти курс обучения проведению собеседований. Есть несколько подходов к проведению собеседований. По нашему опыту, один из тех, которые хорошо работают, – собеседование по поведению, при котором поведение в прошлом оценивается для прогноза будущих действий. Этот подход может использоваться и для технического собеседования. Вопросы задаются в виде: «Вспомните время, когда... Опишите мне ситуацию и расскажите, что вы делали». Делайте это так, чтобы было понятно, что вы не обвиняете человека в возникновении проблемы, а просто хотите узнать, как он с ней справился. Например, вы можете спросить у кандидата на должность системного администратора: «Все мы сталкивались с тем, что работы было слишком много и что-то было упущено или задержано. Вспомните о том, когда это происходило с вами. Опишите мне ситуацию и расскажите, как вы с ней справились. Что дал вам этот опыт?» Спрашивайте как о хорошем, так и о плохом. Например, спросите о лучшем проекте, над которым работал кандидат, и о том, почему он считает его лучшим, а затем спросите о худшем. Спросите о лучшем и худшем начальниках человека, чтобы определить, что ему нравится и не нравится в руководителях и каков его стиль работы. Этот прием работает лучше, чем подход, при котором задается вопрос о том, что кандидат *сделал бы* в определенной ситуации, потому что при такой академической постановке вопроса людям проще представить, как они должны себя вести. Однако, когда такие ситуации возникают на самом деле, присутствуют другие условия и факторы, которые приводят к другому поведению. Собеседование по поведению оценивает, как человек вел себя в реальных жизненных ситуациях.

Нетехнические собеседования проводятся для оценки личностных качеств кандидата: как человек работает в коллективе, относится к пользователям, организует свое время, нужно ли ему жесткое управление или лишь небольшое, нравится ли ему узкая специализация или возможность работать во многих областях и т. д. Обычно на эти вопросы нет правильных и неправильных ответов. Группе проведения собеседования нужно услышать ответы, чтобы решить, впишется ли человек в коллектив, подойдет ли для определенной должности или, возможно, лучше подойдет для другой.

Например, компания может проводить собеседование с кандидатом, который очень умен, но, выполнив 80% задачи, теряет к ней интерес, потому что все

трудные проблемы были решены. Если этот человек может работать вместе с кем-то другим, кому нравится доводить задачи до конца и учиться у другого человека, он станет хорошим сотрудником. Однако, если для этого человека нет подходящего партнера, скорее всего, он не будет хорошим приобретением для вашей группы.

Постарайтесь выяснить, каков привычный стиль работы человека. Если он поддерживает свой уровень знаний о технологиях, читая списки рассылок, группы новостей и сайты, делает ли он это в ущерб своей остальной работе или находит подходящий баланс. Проводящий собеседование должен получить хорошее представление о подходе кандидата, поговорив с ним о том, как тот поддерживает свой уровень знаний о технологиях и какие списки рассылки он читает. Некоторые люди тратят огромное количество времени на то, чтобы быть в курсе последних технологий, читая большое количество списков рассылки. Такие кандидаты могут быть приятны и интересны в общении, но работа с ними может раздражать, если они не способны выполнять большой объем реальной работы.

Оцените заинтересованность кандидата в компьютерах. Если компьютеры – смысл всей его жизни и его единственное времяпрепровождение, то в какой-то момент он «сгорит на работе». Он может работать очень долго, потому что ему это так сильно нравится, но это небезопасно для здоровья и не приводит к успеху в долгосрочной перспективе. Кроме того, он может проводить много времени в офисе, занимаясь интересной технологией, которая не имеет никакого отношения к работе. Поскольку он работает так долго и так много времени проводит с компьютерами, ему будет тяжело определить, сколько реальной работы он выполняет, а сколько – просто играет. С другой стороны, некоторые кандидаты могут удивительно не любить компьютеры. Они могут не желать прикасаться к компьютерам или видеть их в нерабочее время. Обычно эти люди ведут сбалансированную жизнь и не сгорят на работе – возможно, у них уже был такой опыт, – но они с меньшей вероятностью будут счастливы работе продолжительное время. Однако они также с большей вероятностью будут продуктивными в течение всего своего рабочего времени. Кроме того, вряд ли они будут первыми, кто услышит о новой технологии или испытает ее и предложит ввести. Несмотря на то что идеальный кандидат должен представлять собой баланс между этими двумя крайностями, некоторые профессии подходят для людей с одним из крайних случаев. И опять же, проводящие собеседование должны знать, что они ищут в кандидате.

35.1.10. Реклама должности

Помимо выяснения того, с какими кандидатами хочет работать группа, собеседование – это также время для того, чтобы убедить кандидатов в их желании работать в компании. Первый шаг на этом пути – проявить к кандидатам уважение и обеспечить, чтобы процесс собеседования не тратил зря их времени и не заставлял их чувствовать себя униженными. Люди, с которыми кандидаты встречаются на собеседовании, должны быть лучшими представителями группы. Они должны быть теми, с кем кандидаты захотят работать.

Сама должность также важна. Выясните, чего ищет кандидат, и определите, можете ли вы предложить это на данной должности. Хочет ли кандидат работать в конкретной области системного администрирования или со многими различными направлениями? Дайте кандидату знать, можно ли сделать из этой долж-

ности то, что он хочет. Каждый опрашивающий должен думать обо всех положительных чертах компании и группы и делиться этим с кандидатами.

Компании интернет-коммерции, интернет-провайдеры и компании-консультанты в области системного администрирования могут извлечь максимум выгоды из того факта, что системное администрирование – это элемент основного бизнеса компании и поэтому оно хорошо финансируется и рассматривается как центр получения прибыли, а не центр расходов (или к нему должны так относиться). Нам всегда больше нравилось работать в компаниях, где системные администраторы считаются ценными ресурсами, в которые нужно вкладывать средства, а не нахлебниками, расходы которых нужно снижать.

35.1.11. Удержание сотрудников

Когда вы наймете хорошего сотрудника, вы захотите, чтобы человек остался надолго. Мотивация системных администраторов остаться в компании различна для разных людей, но некоторые аспекты справедливы для большинства.

Спрос на системных администраторов следует за взлетами и падениями высоких технологий, как и зарплаты системных администраторов. Несмотря на то что зарплата важна – поскольку, в конце концов, никто не хочет чувствовать, что его эксплуатируют, – предложение самых высоких зарплат необязательно удержит сотрудников. Зарплаты должны быть конкурентоспособны, но для системных администраторов более важно быть счастливыми на своей работе.

Один из секретов удержания системных администраторов – поддерживать их интерес к работе. Если есть утомительные, многократно повторяемые задачи, пусть кто-нибудь их автоматизирует. Человеку, который будет создавать автоматизацию, это понравится, системные администраторы, которым больше не надо будет выполнять монотонную работу, примут ее, и эффективность повысится.

Как и большинство людей, системные администраторы любят признание своего усердия и хорошей работы. Премии за продуктивность – один из способов показать сотрудникам признание, но простая благодарность, высказанная на собрании группы, может работать так же эффективно.

Ключ в признании и удовольствии

Консалтинговая компания, в которой работало много прекрасных системных администраторов, проходила через сложный период и потеряла многих сотрудников. Один из ушедших системных администраторов сказал, что высшее руководство компании не представляет себе, что мотивирует людей. Большинство из тех, кто ушел, имели хорошую зарплату, и, чтобы они остались, им предлагали повышение зарплаты. Но, как сказал этот уходящий сотрудник, «люди работают за деньги, люди усердно работают за признание, но усерднее всего люди работают, когда они любят свое дело. Людей признают “лучшими”, когда они любят то, что делают, и тех, для кого они это делают».

Хорошим системным администраторам нравится работать с другими хорошими системными администраторами. Системным администраторам нравится видеть

финансирование важных инфраструктурных проектов и участвовать в построении хорошей инфраструктуры. Им нравится видеть поощрение долгосрочного планирования. Системным администраторам нравится ощущать себя частью компании, а не бесполезным, часто игнорируемым придатком. Им нравятся хорошие отношения с людьми, с которыми они тесно взаимодействуют, – обычно это их пользователи. Несмотря на то что большинству системных администраторов нравится быть занятыми, они не любят перегрузки до такой степени, когда работа становится неподъемной. Часто системные администраторы не являются самыми общительными сотрудниками, но им нравится быть информированными и они надеются, что их руководители замечают, когда они перегружены или совершают подвиги. Кроме того, системным администраторам нужна возможность развивать свою карьеру, они уволятся, если будут знать, что продвижения не будет.

Также системные администраторы любят «классные вещи». Быстрые соединения из дома, самые современные ноутбуки и возможность работать с новыми технологиями помогает поддерживать комфортную рабочую обстановку. Нахождение для системных администраторов возможности работать дома также может помочь их удержать.

Последний элемент, требуемый большинству системных администраторов для счастья, – это их непосредственный руководитель. Некоторым людям нравится дружеское общение с начальником, другие предпочитают четкие указания начальства и уверенность в том, что их начальник верит в них и поддержит их при необходимости. В главах 33 и 34 подробно рассмотрены задачи технических и нетехнических руководителей. Люди устраиваются на работу из-за денег, но увольняются из-за плохих начальников. Как говорилось в разделе 32.2.2.4, это касается не того, что вы делаете, а того, для кого вы это делаете.

35.2. Тонкости

Когда компания овладеет основами найма системных администраторов, останется рассмотреть, как обеспечить такое представление компании, чтобы системные администраторы хотели в ней работать. В данном разделе рассмотрено несколько способов того, как компания может стать заметной.

35.2.1. Станьте заметными

Использование некоторых нетрадиционных стимулов может помочь сделать компанию заметной и развить ее репутацию как места, где интересно работать. Например, в одной из компаний всем кандидатам, успешно прошедшим собеседование, выдавали КПК Palm Pilot – новейший на то время продукт. В другой компании совершались неформальные групповые походы в ближайший парк аттракционов, и компания оплачивала сотрудникам сезонные абонементы. Еще в одной компании в комнатах нескольких зданий комплекса были новейшие игровые консоли и видеоигры. Старшие системные администраторы и некоторые руководители еще одной компании создали традицию играть в сетевые компьютерные игры раз в неделю вечером. Другие создавали в компании или вместе с иными компаниями спортивные или игровые лиги. Несмотря на то что большинство из этих занятий не привлекает всех поголовно, они интересны достаточному количеству людей, чтобы выделять эту компанию как интересное для работы место. А это может помочь привлечь даже тех сотрудников, которые не заинтересованы в предлагаемом занятии.

Выгодно отличить компанию могут и другие, ориентированные на работу схемы. Например, в некоторых местных организациях системного администрирования есть регулярные собрания, которые нужно где-то проводить. Размещение местной группы SAGE или регулярные обсуждения актуальных вопросов раз в месяц вечером делает компанию более привлекательной для системных администраторов. Если поощрять системных администраторов писать и представлять на конференциях статьи и учебные пособия, это также показывает, что компания является хорошим местом для работы системных администраторов, и обеспечивает известность компании в области системного администрирования.

В конечном итоге, цель – сделать компанию заметной и известной как интересное место для работы, где ценят системных администраторов. Мыслите творчески!

35.3. Заключение

Секрет найма заключается в хорошем планировании и проработке. Наем системных администраторов начинается с составления хорошей должностной инструкции. Должностная инструкция помогает определить необходимый уровень навыков и личностные качества и направить вопросы проводящих собеседование сотрудников на актуальные темы. Кроме того, она используется для подбора подходящих кандидатов. Лучший способ подбора кандидатов – личные рекомендации от пользователей и персонала. Другие способы, ориентированные на людей с техническим мышлением, также подойдут.

Уровень навыков нанимаемого человека имеет финансовую сторону, и компания должна понимать скрытые расходы при найме недостаточно квалифицированного персонала с меньшими требованиями по зарплате. Процесс собеседования должен предоставить кандидату возможность встретиться с ключевыми людьми, с которыми он будет работать, если его наймут. Проводящие собеседование сотрудники должны представлять компанию с лучшей стороны. Они должны проявлять уважение к кандидату и обеспечить приятное впечатление от собеседования. Технические навыки и личностные качества, необходимые для работы, должны быть разделены между опрашивающими сотрудниками, и все они должны знать, как проводить опрос о выделенных им навыках.

Секрет хороших вопросов на собеседовании – это уточнение. Вопросы должны давать кандидату возможность показать себя в наилучшем свете благодаря простому вовлечению в беседу и сохранению уверенности в себе. В этой главе рассмотрены способы оценить навыки по решению проблем и проектированию. Личностные качества почти так же важны, как технические навыки. Курсы обучения проведению собеседований могут быть очень полезны в предоставлении способов точно оценить эти качества в кандидатах.

После определения подходящего кандидата его нужно убедить согласиться на работу. Этот процесс начинается с первого контакта кандидата с компанией. Кандидат должен чувствовать уважение к себе и хорошее отношение в процессе собеседования. Бесполезно пытаться нанять кого-то, оскорбленного в процессе собеседования. Зарплата – это часть привлечения кандидата, но большую роль играют и положительные аспекты работы в группе, например хороший коллектив или нормальное финансирование. Наличие репутации интересного для работы места или места, где ценят системных администраторов, может здорово помочь в найме подходящих сотрудников.

После найма людей их нужно удерживать. Собеседование – это дорогостоящий процесс.

Задания

1. Напишите подробную инструкцию для вакантной должности в своей группе или для должности, на которую вы хотели бы кого-нибудь нанять.
2. Нанимает ли ваша компания людей с более высоким, более низким или точным уровнем навыков, необходимым для должности? Проиллюстрируйте свой ответ несколькими примерами.
3. Кто в вашей группе хорошо проводит собеседования, а кто нет? Почему?
4. Как вы думаете, каких ролей не хватает в вашей группе?
5. Насколько разнообразна ваша группа? Что вы можете сделать, чтобы нанять людей, отличающихся по своим национальным и культурным традициям от тех, кто работает сейчас?
6. Кто мог бы стать наставником для младшего системного администратора, если бы вашей группе пришлось его нанять?
7. Есть ли в вашей группе младшие системные администраторы, которых не обучают? Если да, какой положительный и отрицательный опыт есть у младших системных администраторов из-за недостатка обучения?
8. Как вам удавалось сделать процесс собеседования приятным для кандидата?
9. Как вы делали процесс собеседования неприятным для кандидата? Почему это произошло? Что можно сделать, чтобы этого больше не произошло?
10. Напишите должностную инструкцию для кого-нибудь с навыками, которых, по-вашему, не хватает вашей группе.
11. Какие технические вопросы вы задали бы кандидату на должность, для которой вы написали должностную инструкцию?
12. Какие нетехнические вопросы вы задали бы кандидату на эту должность?
13. Что является наилучшим в работе вашей нынешней компании?
14. Что является наихудшим в работе вашей нынешней компании?
15. Что мотивирует вас оставаться в той компании, в которой вы сейчас работаете?
16. Если бы завтра вам потребовалось начать искать работу, где бы вы хотели работать и почему?
17. Насколько хорошо у вашей компании получается удерживать сотрудников? Как вы думаете, почему?
18. Как вы думаете, что ваша компания делает или могла бы делать, чтобы выглядеть хорошим местом для работы?

Глава 36

Увольнение системных администраторов

Эта глава о том, как отстранить системных администраторов от доступа к вашей системе после их увольнения. Мы желаем, чтобы вам никогда не понадобилась информация этой главы. Но реальность такова, что всем рано или поздно приходится пользоваться этой информацией. Вы можете и не быть директором, на которого возложена обязанность решать вопрос об увольнении кого-либо, но вы можете быть системным администратором, которому придется справляться с последствиями этого.

Эта глава не о том, по каким причинам следует кого-либо увольнять. Мы не можем вам с этим помочь. Вместо этого глава рассказывает о технических задачах, которые должны быть выполнены в такой ситуации. Можно сказать, что действие данной главы начинается после того, как руководство приняло решение о чьем-либо увольнении и вам нужно лишить этого человека доступа к сети.

Лишение системных администраторов доступа против их воли – уникальная задача. У системных администраторов есть привилегированный доступ к системам, и, скорее всего, у них есть возможность доступа ко всем системам. Некоторые системные администраторы могут разбираться в системе лучше вас, так как сами ее построили. С другой стороны, методы, приведенные в данной главе, также могут быть использованы для улаживания дел с системными администраторами, которые покидают компанию, оставаясь с ней в хороших отношениях. Но вне зависимости от того, уходят ли люди в хороших или плохих отношениях с компанией, вероятность того, что ситуация может ухудшиться, делает их потенциальной угрозой для компьютерной инфраструктуры компании.

У крупных компаний обычно есть процедуры для лишения доступа на случай, когда кто-либо увольняется. У компаний малого и среднего размеров могут быть специально подготовленные процедуры. Мы надеемся, что эта глава может послужить вам отправной точкой, если у вас появится необходимость создания процедуры отстранения.

Описываемый процесс не является чисто теоретическим. Он основан на лучшем на сегодняшний день опыте опрошенных нами компаний.

36.1. Основы

С точки зрения системного администратора, основной процесс увольнения сводится к следующим трем вопросам[1]:

1. Процедура
   a. Соблюдайте вашу корпоративную кадровую политику – это самое важное правило.
   b. Пользуйтесь контрольным списком, чтобы ничего не забыть.
2. Доступ
   a. Лишить физического доступа: «Может ли он войти в здание?»
   b. Лишить удаленного доступа: «Может ли он удаленно подключиться к нашей сети?»
   c. Лишить доступа к службам: «Были ли аннулированы права доступа к приложениям?»
3. Постоянное улучшение
   a. Используйте меньше баз данных управления доступом: чем меньше контрольных точек, тем легче кого-либо заблокировать.

В этом разделе мы подробно рассмотрим каждую из этих областей, а также приведем истории, показывающие, как они применялись в некоторых реальных ситуациях.

36.1.1. Соблюдайте вашу корпоративную кадровую политику

Единственное самое важное правило заключается в том, что вы должны следовать правилам своей компании по увольнению сотрудников. Эти правила написаны людьми, которые понимают сложные правовые нормы, регулирующие увольнение сотрудников. Экспертами в данной области являются эти люди, а не вы. У них есть указания о том, что говорить, что не говорить, как это делать или как это не делать. Обычно это настолько редкое и деликатное событие, что вами руководит кто-либо из отдела кадров.

Кадровики могут посоветовать много способов увольнения, начиная от звонка сотруднику с просьбой больше не приходить на работу и заканчивая чем-то конфронтационным, например два охранника и человек из отдела кадров в кабинете сотрудника информируют его о том, что его личные вещи будут выданы ему, когда охрана проводит его из здания.

36.1.2. Пользуйтесь контрольным списком по увольнению

Создайте перечень задач, которые необходимо выполнить, когда сотрудника увольняют. Первая часть должна быть составлена с помощью отдела кадров. Вторая часть должна содержать технические детали того, как происходит лишение доступа. Этот список должен легко обновляться; в любой момент при добавлении новой службы должна быть возможность просто внести в этот спи-

[1] Эта модель – развитие модели, описанной в книге Ringel and Limoncelli 1999.

сок соответствующую процедуру отстранения. Этот список должен быть аналогичен контрольному списку, используемому при создании учетных записей, но, скорее всего, он будет содержать значительно больше пунктов для служб, еще не внедренных тогда, когда производился прием на работу.

Преимущество использования контрольного списка в том, что он исключает необходимость помнить, что должно быть сделано, когда кто-то увольняется. Если вам приходится думать о том, что необходимо сделать, вы можете что-нибудь забыть. Чье-либо увольнение – это эмоциональный момент, поэтому вы можете потерять собранность в этот период. Кроме того, контрольный список предоставляет возможности для учета. Если вы распечатаете контрольный список и пометите каждый пункт как сделанный, то вы создадите полноценный документ. В некоторых средах такой законченный список задач передается IT-директору, который подписывается под заявлением об увольнении.

36.1.3. Лишите физического доступа

Физический доступ описывается довольно простой фразой: «Убедитесь, что человек не может войти в здание». Обычно это находится в компетенции отдела кадров или корпоративной службы безопасности. Например, у отдела кадров уже должна быть процедура изъятия удостоверения личности, которое проверяется охраной на входе. Если используется доступ по ключам-картам, то система проверки карт должна быть запрограммирована таким образом, чтобы запрещать доступ недействительным ключам-картам, независимо от того, были ли они возвращены. Должны быть возвращены ключи от всех комнат либо проведена смена замков. Коды на замках, сейфах и т. д. следует сменить. Есть ли подсобное помещение, ремонтный цех, будка, сарай, конура или пристройка с доступом к сети? Проверьте и их тоже. Поскольку физические инструменты, такие как двери и ключи, используются гораздо дольше компьютеров, у большинства компаний обычно уже есть для них процедуры. Соблюдайте их. У очень небольших компаний может и не быть системы идентификации на основе удостоверений личности или подобной. В этом случае сообщите секретарю в приемной и другим сотрудникам, что предпринимать, если они увидят данного человека в здании.

Вы также должны определить время, когда системный администратор должен вернуть все оборудование, которое он может иметь дома. Любые возвращенные компьютеры должны рассматриваться как подозрительные. Диски следует очистить, чтобы предотвратить распространение вирусов.

36.1.4. Лишите удаленного доступа

К **удаленному доступу** относится множество способов, при помощи которых кто-то может подключиться к сети. Помимо прочего они включают модемные пулы, линии ISDN, xDSL, входящие соединения через брандмауэр и службу VPN. Доступ ко всем этим системам должен быть закрыт. Это может быть сложно реализовать, если каждая из них находится в ведении разных групп или они имеют различные системы управления.

36.1.5. Лишите доступа к службам

Доступ к службам касается приложений и служб, находящихся внутри сети. Обычно у каждой из этих служб есть пароль. В качестве примера можно привести POP3/IMAP4 (Crispin 1996, Myers and Rose 1996), серверы, серверы баз

данных, UNIX-серверы (для каждого из них нужно проверить собственный файл /etc/passwd или глобальную базу данных NIS либо Kerberos), учетные записи NT Domain, SMB серверы (NT File Server), Active Directory, LDAP и т. д.

Рассмотренные выше вопросы относятся к действиям, которые предпринимают, когда кого-либо увольняют. Технически каждый из этих вопросов следует решать отдельной подгруппе: руководители будут заниматься управлением персоналом, корпоративная служба безопасности обеспечит лишение физического доступа, у администраторов удаленного доступа будут свои задачи, а системные администраторы сосредоточатся на лишении доступа к службам.

Рассмотренный процесс устойчив к некоторым ошибкам. Доступ разделен на три уровня: физический, удаленный и служебный. Если есть ошибки на любом из уровней, доступ все еще будет закрыт. Если, например, учетная запись на одной из служб не была отключена, но человек не может физически войти в здание или подключиться удаленно, он не сможет использовать учетную запись и нанести ущерб. Если удаленный доступ по случайности не был закрыт, ущерб будет сведен на нет отключением всех служб.

Приведенные ниже истории реальны. Имена были изменены для сохранения приватности.

Увольнение начальника

В большой производственной компании было необходимо заблокировать доступ руководителя группы системного администрирования на время проведения расследования. У этого человека был административный доступ ко всем системам в его подразделении, а также удаленный доступ к сети всеми способами, которые предоставляла группа системного администрирования.

Без ведома подозреваемого директора его руководителем было созвано совещание с главным системным администратором и службой корпоративной безопасности. Сотрудник корпоративной службы безопасности объяснил ситуацию и план действий. Главному системному администратору предстояло сменить все пароли привилегированных учетных записей в этот вечер; утром директор встречался с группой системного администрирования без присутствия ее руководителя, чтобы проинформировать о ситуации остальных сотрудников. Им было сказано приостановить доступ к системам. Если где-то его нельзя было приостановить, доступ следовало закрыть. Группа системного администрирования была разделена на несколько подгрупп по принципу удаленного доступа и доступа к службам.

Главный системный администратор провел вечер, меняя пароль `root` на каждой системе. Утром всех системных администраторов созвали на закрытое совещание и объяснили им ситуацию. Служба безопасности занималась вопросами физического доступа. Группе системного администрирования были поручены вопросы удаленного доступа и доступа к службам. Они отдельно устраивали мозговую атаку по данным вопросам, что помогло им определить главные моменты. Все изменения были запротоколированы, и протоколы были переданы главному системному администратору.

Была одна проблема; говоря кратко, она заключалась в том, что, если человек имел фотографическую память, он мог воспользоваться какой-либо формой удаленного доступа для проникновения в сеть. Для решения этой проблемы требовалось несколько дней, и ничто не могло помочь сделать это быстрее. Но при этом риск данного события считался низким и группа системного администрирования была уверена, что физический доступ и доступ к службам был полностью закрыт, а для выявления проникновений можно было следить за журналами. Другими словами, они были уверены, что законченная работа на двух уровнях компенсирует незаконченную на третьем.

Во время расследования обвиняемый директор ушел в отставку. Записи о том, какой доступ был закрыт, были очень полезны как инструкция: какой доступ был приостановлен и теперь требуется закрыть его окончательно.

Подход сработал очень эффективно. На повышение эффективности повлияло деление на группы. Потенциальная проблема с удаленным доступом была компенсирована полным закрытием всего остального доступа.

Увольнение в учебном заведении

Учебные заведения обычно преуспевают в процессе прекращения доступа, так как в конце каждого учебного года у них часто имеется большое количество учетных записей с прекращенным действием. Университет – это хороший пример того, как «практика доводит до совершенства». Однако в этой истории замешан человек с привилегированным доступом ко многим машинам.

В крупном государственном университете нужно было лишить доступа долго работавшую там женщину-оператора с `root`-доступом ко всем UNIX-системам. Она так долго работала там, что все были убеждены в невозможности блокировки всего доступа. Раньше с такой ситуацией не сталкивался никто.

Так как весь доступ нельзя было отключить мгновенно, люди беспокоились, что оператор сможет снова войти в систему. Возмездия не ожидалось, но университет не мог допустить такого риска. Так как это был открытый университет, физический доступ в здание не мог быть исключен, но изменения ключей-карт не позволяли оператору получать физический доступ к важным машинам. Удаленный доступ нельзя было отключить, потому что в крупном университете не использовали брандмауэр.

После некоторого обсуждения было решено воспользоваться следующей процедурой: была собрана небольшая группа, чтобы перечислить весь доступ, который имелся у оператора, в том числе доступ к ключам-картам и узлам, и обсудить способы его отключить. Когда пришло назначенное время, ей сказали, что ее начальнику нужно поговорить с ней в своем офисе. Два офиса находились в противоположных частях здания, и путь занял бы как минимум 10 мин. За это время все старшие системные администраторы работали для отключения ее доступа. К тому вре-

мени, как она дошла до офиса начальника, все ее учетные записи были отключены.

Поскольку у оператора был такой широкий доступ, такие крайние меры были единственной возможностью для обеспечения полного покрытия.

Мирный уход из компании

Системный администратор в небольшой компании, разрабатывающей программное обеспечение, объявил о своем уходе и предложил месяц помогать компании с переходом. Системный администратор был привлечен к поиску своей замены. К дате ухода были переданы все обязанности. В свой последний день работы системный администратор пришел в кабинет своего начальника и вошел в систему на его компьютере под учетной записью `root`. На глазах начальника он удалил свою рабочую учетную запись. Потом он выполнил команды, чтобы активизировать процедуру «смена пароля `root` на всех системах», и позволил своему руководителю ввести новый пароль. Директор был удивлен тем, что сотрудник, который скоро увольняется, проводит такую полную работу по передаче обязанностей и удалению своего присутствия в системах. Наконец системный администратор положил свою ключ-карту и обычные ключи на стол начальника и покинул здание. Примерно через две недели бывший сотрудник вспомнил, что он забыл поменять пароль на одной непривилегированной учетной записи на машине с модемом. Бывший сотрудник узнал от своих бывших коллег по работе, что его бывший работодатель не сменил пароль, пока он не сообщил об этой ошибке.

С одним исключением, лишение доступа было закончено. Однако исключение проходило через уровни удаленного доступа и доступа к службам, так как учетная запись (доступ к службам) находилась на машине, которая была напрямую подключена к окружающему миру (удаленный доступ). Кроме того, было небезопасно устанавливать новые пароли перед увольняющимся сотрудником, который мог смотреть на клавиатуру. Также сотрудник мог записать новые пароли по мере того, как они устанавливались. Обычная команда `script` в UNIX не записывает неотображаемый ввод, например пароли, но существует множество утилит по перехвату клавиатурного ввода, которые это делают, на всех операционных системах.

Компания рисковала, не отключая доступ, до тех пор, пока не пришло уведомление. Тем не менее это был вполне оправданный риск, если учитывать, что уход был мирным.

36.1.6. Используйте меньше баз данных управления доступом

Говоря о задачах, которые требуется выполнить системным администраторам, в их терминах, закрытие доступа связано с обновлением баз данных управления доступом, которые указывают, кто и что может делать: списки RADIUS, сетевые настройки ACL и Active Directory – это все базы данных управления доступом. Чем меньше этих баз данных, тем меньше работы. Поэтому системным архи-

текторам следует всегда проектировать системы с наименьшим количеством таких баз данных.

Одна из сторон этого процесса включает мозговую атаку, проведенную с намерением вспомнить все способы, которыми должен быть закрыт доступ. Этот процесс может быть улучшен при помощи хорошего оборудования и механизмов глобального контроля среды, основанных на обновлении базы данных, как рассмотрено в разделе 8.2.2.

36.2. Тонкости

Теперь, когда мы рассказали об основах, мы приведем некоторые рабочие нормы, которые могут сделать процесс стабильнее и уменьшить риск.

36.2.1. Пользуйтесь единственной базой аутентификации

Хотя меньшее количество баз данных управления доступом – это преимущество, проведение аутентификации всех служб через одну базу данных влечет за собой новый подход. Это легко сделать, если все службы контролируются портативными средствами аутентификации (HHA) которые осуществляют доступ к единственной базе данных.

В первом примере (раздел 36.1.5) доступ ко многим службам – VPN, внутреннему `telnet`-соединению через брандмауэр, `root`-доступу и т. д. – контролировался одной системой HHA. Отключение записи руководителя в базе данных HHA приводило к немедленному одновременному прекращению работы многих служб.

Это не освобождает системных администраторов от необходимости удаления информации о человеке из конфигурационных файлов, индивидуальных для каждой службы. Система HHA предоставляет информацию об аутентификации, а не о полномочиях. То есть HHA сообщает системе, кто стучится в дверь, а не то, следует ли его впустить. Это решение остается за локальной службой. Например, основанная на HHA замена UNIX-команды `/bin/su` запросит сервер HHA, чтобы выяснить, кто ввел команду, но у программного обеспечения, как правило, есть локальный файл настроек, который указывает, кто может стать пользователем `root`. С отключенным HHA никто и никогда не сможет пройти аутентификацию как этот пользователь, но это не ставит под вопрос имя пользователя, записанное в файле настроек. Процессы не завершаются; `cron`, `at` и другие автоматизированные службы продолжают выполняться. В итоге все ссылки на человека должны быть перемещены или удалены.

Централизация всех этих локальных файлов настроек и баз данных управления доступом в единственную базу данных – следующий шаг, к которому мы должны стремиться. LDAP, Kerberos, NDS и другие технологии приближают нас к этой цели.

36.2.2. Изменение системных файлов

Если кто-то боится, что его могут уволить, он может создать **потайной вход** – тайный путь проникновения в систему – или заложить **логическую бомбу** – установить программное обеспечение, которое принесет ущерб, когда он уйдет.

В идеале вы можете сохранить образ всего программного обеспечения, пока человек ни о чем не подозревает, и регулярно сравнивать его с действующей системой. Однако это потребует очень много времени и дискового пространства и попросту подскажет человеку, что скоро что-то произойдет.

Тем не менее, если проводить это регулярно, никаких подозрений это не вызовет. Программы для подсчета контрольных сумм системных файлов и уведомления об изменениях используются повсеместно. Простейшее решение называется Tripwire. Если этот процесс – автоматизированная система, которая регулярно используется для выявления проникновений извне, системных ошибок или других проблем, будет гораздо проще использовать его без возникновения подозрений. Однако следует убедиться, что человек, которого собираются уволить, не изменяет базу данных так, чтобы его действия остались незамеченными.

Такая система – отличный способ обнаружения любого типа вторжений. Однако она требует большого количества времени для обработки всех ложных ошибок. Встает вопрос о ее расширении на слишком большое количество машин.

36.3. Заключение

Увольнение системного администратора – не простое и отнюдь не веселое событие, но иногда его не избежать. Основы очень просты. Самое главное правило – следовать политике вашего отдела кадров. Персонал отдела кадров – эксперты, и вам следует поддерживать их действия. Должно быть закрыто три уровня доступа: физический доступ, удаленный доступ и доступ к службам. Главное преимущество трехуровневой модели в том, что она предоставляет структурированный подход, в отличие от ситуативной модели, и нечувствительна к ошибкам, совершенным на одном из трех уровней. Архитектуры, которые стремятся уменьшить количество баз данных управления доступом, и хорошо организованная опись оборудования определенно облегчат процесс.

При создании контрольного списка для всех способов закрытия доступа следует начать с процедуры найма: все, что делается для нанимаемых сотрудников, должно быть отменено для увольняющихся. Хотя ни один контрольный список не является полным, мы собрали несколько контрольных списков того, что нужно отменить в процессе отстранения сотрудника:

- *Физический доступ*. Смените коды на замках, все комбинации для сейфов и замки на дверях с ключами, даже если ключи возвращены. Закройте доступ во все здания: например, удаленные филиалы, будки и технические помещения.
- *Возврат собственности*. Заставьте бывшего сотрудника вернуть все ключи, ключи-карты, значки, HHA, КПК и любое оборудование, принадлежащее компании.
- *Удаленный доступ*. Модемные пулы, ISDN-пулы, VPN-серверы, внутрисетевой доступ – в том числе `ssh`, `telnet`, `rlogin`, – доступ через кабельные модемы, доступ xDSL X.25.
- *Доступ к службам*. Закройте доступ к серверам баз данных, NIS-доменам, NT-доменам, идентификаторам доступа привилегированных пользователей, идентификаторам Netnews, файлам паролей и серверам RADIUS.

Тонкости – это набор структурных и операционных факторов, которые лучше подготавливают организацию к таким нежелательным, но важным задачам. Чем меньше административных баз данных, тем легче будет задача, процесс

в целом становится гораздо проще. Регулярно проверяемый файл истории контрольных сумм предоставляет способ обнаружения и предотвращения создания потайных ходов и логических бомб.

Деление процесса на кадровую политику и физический, удаленный доступ и доступ к службам вносит ясность. Это деление можно легко объяснить. Персонал можно разделить на физическую, удаленную группы и группу служб. Каждая группа после этого может работать, не отвлекаясь ни на что другое, так как у нее будет единственная задача.

Лучше всего этот процесс работает, когда имеется возможность максимально использовать инфраструктуру, которая должна быть в каждой системе. Сильная инфраструктура безопасности не позволит проникнуть внутрь нежелательным людям. Использование единственной (или малого количества) административной базы данных, как в хорошо организованной архитектуре HHA, упростит управление всем доступом с центрального терминала. Хорошо документированные системы и хорошо организованная опись оборудования улучшат способность быстро закрывать весь доступ. Программа Tripwire и процессы мониторинга системы относятся к автоматизации, которая и так может существовать в системе. Чем лучше инфраструктура, тем легче становится данный процесс.

Метод, описанный в данной главе, может быть успешно применен в чрезвычайной ситуации лишения доступа системного администратора, но помимо этого является полезной моделью, которую можно применить, когда кто-либо другой покидает компанию, просто выходит из вашей области поддержки либо меняет должность в компании на другую и более не нуждается в привилегированном доступе к системам, которые он до этого администрировал. Мы не раскрываем эти темы прямо. Мы считаем, что было бы гораздо интереснее раскрыть один чрезвычайный случай и оставить другие в качестве упражнения читателю.

Наше обсуждение было ограничено технической стороной данного процесса. Но нетехническая сторона, человеческий фактор, не менее важна. Вы очень сильно меняете жизнь человека. У человека есть счета, по которым нужно платить, семья, которую нужно кормить, и жизнь, которую нужно прожить. Корпоративная политика может варьироваться от «немедленно выставите его вон» до «мы откажемся от ваших услуг через шесть месяцев». С обоими вариантами могут возникнуть потенциальные проблемы, но, с нашей точки зрения, последний не только работает гораздо лучше, но и показывает доверие и уважение. Этот вопрос важен не столько для человека, который уходит, сколько для тех, кто остается.

Задания

1. Знает ли отдел кадров, к кому обратиться в IT-организации для лишения человека доступа, когда он увольняется?
2. Что должно быть отключено в вашей текущей среде, если бы вас собирались уволить? Сколько отдельных административных систем вам придется затронуть, за исключением проверки индивидуальных машин на локальные учетные записи?
3. Какие улучшения в вашей среде могли бы облегчить лишение вас доступа при вашем увольнении?
4. Система типа Tripwire выполняет периодические обращения к подсистеме ввода/вывода файловой системы. Как это отразится на планировании и внедрении такой системы? Чем это отличается от файлового сервера, сервера электронной коммерции и сервера баз данных?

Эпилог

В начале этой книги мы задались вопросом, как дать четкое определение системному администрированию. Сейчас мы не подошли ближе к ответу. Мы лишь расширили данное определение. Вместо того чтобы искать более четкое определение, мы рассматривали такие вопросы, как поддержка пользователей, ремонт, эксплуатация, разработка архитектуры, внедрение, аварийное планирование, и даже поговорили о навыках управления. Системное администрирование – очень широкая область человеческой деятельности, и ни одно простое определение не может полностью его охватить.

Мы надеемся, что вы многому научились, читая эту книгу. Мы определенно многое узнали в процессе ее написания. Необходимость преобразовывать в слова то, что стало второй натурой, заставляла нас глубоко задумываться над каждым нашим действием, над каждой привычкой, которую мы выработали. Благодаря проверке нашей работы наставниками и коллегами мы смогли подойти более критично к нашим принципиальным убеждениям. Мы стали лучше после написания этой книги и надеемся, что вы станете лучше после ее прочтения. Мы надеемся, что однажды и вы напишете книгу и получите от этого такое же удовольствие.

Самым интересным при создании этой книги было вспоминать и записывать диалоги и истории, которые мы собрали в процессе своей работы. Мы отвечали на некоторые технические и нетехнические вопросы, вставая на свои импровизированные трибуны, чтобы высказать свои взгляды. Наши попытки переделать эти монологи приводили лишь к тому, что мы снова и снова возвращались к их дословной передаче. Мы можем честно заявить, что все наши рассуждения в этой книге выданы с предсказуемостью на уровне собаки Павлова. Также эта книга содержит все полезные истории из нашего опыта. Каждая история преподносит важный урок, а то и два. Теперь мы знаем, что эти истории для чего-то пригодились, и можем спокойно ожидать новых, которые произойдут в будущем.

Системное администрирование – это культура. В каждой культуре есть свои легенды, мифы и притчи. Они позволяют нам передавать свою историю новым поколениям и распространять традиции и культурные ценности, которые для нас важны. Лучше всего мы учимся, когда слушаем легенды и притчи нашей культуры. Каждый раз, когда мы делимся подобной легендой или притчей, мы обогащаем эту культуру.

Мы бы хотели поделиться с вами одной последней историей.

Четкое определение

В одну организацию на лето приехали несколько исследователей из различных университетов. Осенью, когда они уехали, системным администраторам нужно было списать их компьютеры и очистить большую комнату, которую они занимали. Системные администраторы нашли клочок бумаги, который был прикреплен рядом с телефоном. На нем было написано «Решение всех проблем», а дальше следовал телефон отдела системного администрирования.

Это был наивысший комплимент, который они когда-либо получали.

A

Множество ролей системного администратора

Это приложение во многом философское. Если это вас раздражает, можете пропустить его, но мы думаем, что оно поможет вам подумать о вашем месте в мире или, по крайней мере, в вашей компании, организации либо группе системного администрирования. Определение своего места в организации помогает вам сосредоточиться, что, в свою очередь, способствует лучшему выполнению вашей работы. Оно может дать вам взгляд на карьеру в долгосрочной перспективе, что поможет вам принять серьезные карьерные решения, необходимые для счастливой и успешной жизни.

Кроме того, оно может предоставить вашей организации структуру для рассмотрения задач, которые в ней хотят выполнять. Каждая из этих задач каким-то образом затрагивает вашу организацию. Это ни в коем случае не полный список, однако это хорошая начальная точка. Вам нужно пользоваться этим списком, чтобы выяснить, каких ролей в вашей организации не хватает, и, возможно, начать действия по их заполнению.

Интересно подумать о том, какие и сколько из этих ролей вам пришлось играть по мере развития вашей карьеры. Этот список может помочь вам ее планировать. Некоторых системных администраторов начального уровня просят выполнять одну задачу, а с увеличением опыта они доходят до выполнения большего количества задач. Иногда системные администраторы начинают с загруженности большим количеством задач, а со временем специализируются.

В небольшой компании может потребоваться, чтобы ее единственный системный администратор взял на себя много задач. По мере роста организации определенные задачи могут быть переданы новым системным администраторам. Иногда вы можете обнаружить, что определенная роль вам не нравится и вы стараетесь избежать ее при смене работы. Рассмотрение этих задач также может помочь управлять вашей карьерой в плане того, в каких компаниях вы хотите работать: в небольших компаниях обычно требуют от людей выполнения нескольких задач, в компаниях покрупнее часто нужны более специализированные сотрудники, а в транснациональных корпорациях есть настолько узкоспециализированные сотрудники, что посторонним это может показаться диким. Технические компании уважают и поощряют тех, кто выполняет задачу по внедрению новых технологий, тогда как в других компаниях часто не одобряют слишком сильных изменений.

A.1. Распространенные положительные роли

Некоторые роли в компании важнее других, какие-то из них хорошие, а другие – плохие. Здесь мы приведем много распространенных ролей и объясним, какую пользу они приносят компании, как эти люди получают удовлетворение от работы и чего от них ожидают пользователи.

A.1.1. Установщик

Некоторые рассматривают системного администратора как человека, который устанавливает «всякую всячину». Эту роль чаще всего видят пользователи, и поэтому она обычно ассоциируется с работой системного администратора. Пользователь редко видит другие, возможно, более важные должности, например людей, проектирующих инфраструктуру.

Ценность установщиков для компании заключается в их способности доводить работу до конца и видеть, что работа выполняется. Часто они являются последним и наиболее важным звеном в цепи разработки.

Когда установка выполняется в крупном масштабе, устанавливаемый объект обычно предварительно настраивается в каком-то центральном местоположении. Установщики обучены тому, как действовать в конкретных ситуациях, в которые они могут попасть, и имеют ресурс второго уровня, к которому они могут обратиться в неожиданной ситуации. В таком случае человек, который станет хорошим установщиком, – это тот, кому доставляет удовольствие встречаться с пользователями и помогать им и кто получает удовлетворение от многократного качественного выполнения одной и той же задачи. С другой стороны, при менее масштабной установке предполагается, что установщик будет более опытным человеком, потому что возможно больше неожиданных ситуаций.

Если вы установщик, важно быть дружелюбным и вежливым. Установщик – это публичное лицо организации; люди будут думать, что вся организация действует так, как вы.

A.1.2. Ремонтник

Все ломается. Некоторые рассматривают системного администратора как ремонтника. Точно так же, как люди звонят кому-то, когда ломается их посудомоечная машина, они звонят компьютерному ремонтнику, когда ломается их компьютер. Кроме того, системные администраторы ремонтируют более крупные и иногда более эфемерные вещи, например «Интернет» или «базу данных». Пользователя мало интересует, заключается ли реальная проблема в простом обрыве кабеля или она гораздо серьезнее.

Ценность ремонтников для компании заключается в их способности возвращать компанию к жизни, когда технологические проблемы блокируют бизнес. Ремонтники получают удовлетворение от осознания того, что они помогли одному человеку или целой компании. Они получают удовольствие от сложности хорошей загадки или секрета.

Если вы ремонтник, пользователям нужно знать, что вам не безразличны их проблемы. Им нужно ощущать, что их проблемы – важнейшие в мире.

А.1.3. Сотрудник поддержки

Сотрудник поддержки – это человек, который поддерживает работу ранее построенных систем. У сотрудников поддержки очень хорошо получается выполнять указания, данные им в виде письменной инструкции или посредством обучения. Они не стремятся улучшить систему, они хотят поддерживать ее такой, какая она есть.

Ценность поддерживающих сотрудников для компании заключается в том, что они вносят в среду стабильность. Такие люди не будут ничего ломать, пытаясь это улучшить или заменить. Также они не будут тратить весь день на чтение журналов о том, что можно поставить нового. Когда компании тратят деньги на установку какой-либо системы, им нужно будет поддерживать ее стабильность в течение времени, достаточного для того, чтобы она себя окупила, прежде чем заменять ее на что-то более новое.

Сотрудники поддержки получают удовлетворение от осознания того, что их работа является элементом большого дела, поддерживающим деятельность организации. Они склонны радоваться тому, что они не те люди, которым приходится выяснять, как проектировать и устанавливать следующее поколение систем, и даже могут презирать тех, кто хочет заменить их стабильную систему чем-то новым.

Если вы сотрудник поддержки, пользователям нужно от вас два противоположных качества: они хотят знать, что вы поддерживаете стабильность их мира, и желают, чтобы вы были гибким, если им нужна индивидуализация.

А.1.4. Предохранитель

Предотвращение проблем – задача, невидимая большинству пользователей, и выполняющий ее сотрудник ищет проблемы и устраняет их до того, как они станут видимыми. Предохранители выполняют закулисное планирование и профилактическое обслуживание, которое не позволяет проблемам появиться вообще. Хороший предохранитель отслеживает показатели для поиска тенденций, а также всегда должен быть в курсе событий, чтобы знать, какие проблемы могут возникнуть в дальнейшем.

Ценность предохранителя для компании заключается в предупреждении проблем, а это дешевле устранения проблем при их появлении.

Предохранители получают удовлетворение от осознания того, что их работа предотвратила проблемы, о возможном возникновении которых никто не знал. Их радость тайная. Они получают удовольствие от продумывания действий в долгосрочной перспективе, а не от успешного решения экстренной проблемы.

Типичные пользователи не подозревают о существовании такого человека, но их руководство знает. Руководство рассчитывает, что у этого человека те же самые приоритеты, что и у него.

А.1.5. Герой

Системный администратор может быть героем, совершающим свой ежедневный подвиг. Как пожарный, который выносит людей из горящего здания, герой получает лесть и похвалу. Сеть не работала, но теперь она работает. Демоверсия не была готова, но системный администратор работал все выходные, чтобы

провести сеть в эту часть здания. Герои получают удовлетворение от своей работы, когда их хвалят после ее выполнения.

Ценность героев для компании очень велика: руководство всегда поощряет героя. Забавно, но предохранители часто вынуждены бороться за подобное позитивное впечатление, несмотря на то что их вклад может быть не меньшим, а то и большим.

Герои получают удовлетворение от осознания того, что они обладают какими-то ключевыми знаниями, без которых компания не может жить. Роль героя – не из тех, которые предполагают здоровую жизнь вне работы. Они жертвуют ночами, выходными и отпусками, часто не замечая этого. Личная жизнь отходит на второй план. В конце концов герои выгорают и становятся мучениками, если руководство не находит какого-либо способа облегчить их напряжение.

Пользователи рассчитывают, что герой найдется всегда и везде. Они предпочли бы иметь дело только с героем, потому что эта эффектная суперзвезда стала кем-то, на кого они могут положиться. Однако пользователям нужно знать, что, если они получат желаемое, герой сгорит на работе. Для поиска новых героев требуется время.

A.1.6. Универсал

Этот человек приобрел репутацию сотрудника, который может решить любую проблему. Универсалы немного похожи на героев, но они более координированы и больше полагаются на инфраструктуру. Вместо того чтобы бегать и тушить пожары или ремонтировать сервер с трех дня в пятницу до трех ночи в воскресенье, этот человек является тем, к кому руководство пойдет при возникновении масштабных вопросов, где необходимы глубокие знания. Руководство знает, что универсал дойдет до корня проблемы, выяснит проблемы, лежащие в основе, и устранит их. Это может быть проблема инфраструктуры – настройка параметра базы данных – или проблема процесса – как обеспечить, чтобы у новых пользователей была общая конфигурация, – необходимость создать новую автоматизированную систему и практически все что угодно.

Ценность наличия универсала под рукой в том, что он может сделать то, что не могут сделать другие.

Как и герой, этот человек может сгореть на работе при злоупотреблении его работой, но когда он работает, он получает удовлетворение от осознания того, что его решение станет элементом стандартных процедур, которые будут использоваться в дальнейшем.

Пользователи рассчитывают, что, когда универсал согласится решить проблему, он доведет работу до конца и сможет предоставить точную оценку времени или, по крайней мере, периодические сообщения о состоянии, пока такую оценку дать нельзя.

A.1.7. Создатель инфраструктуры

Корпоративная сеть зависит от большого количества инфраструктур: DNS, директорий, баз данных, скриптов, коммутаторов и т. д. Типичный пользователь не видит ничего из этого, если не происходит сбой, объясняемый такими непонятными фразами, как «Была проблема с DNS-сервером».

Чем крупнее компания, тем ценнее становятся создатели инфраструктуры. Хорошая инфраструктура аналогична прочному фундаменту, на котором мож-

но построить дом. Вы можете построить дом на шатком фундаменте и укрепить его при помощи более сложных и дорогих проектов, но в долгосрочной перспективе дешевле начать с прочного фундамента. В небольших компаниях практически нет инфраструктуры. Более крупные компании выигрывают от амортизации расходов на качественную инфраструктуру по все более и более крупной пользовательской базе. Когда малые компании вырастают и становятся крупными, часто это происходит плавно из-за предусмотрительного найма системных администраторов с «большими планами» по инфраструктуре.

Создатели инфраструктуры получают удовлетворение от долгосрочного планирования, усовершенствования существующих систем, расширения крупных систем до огромных, а также от переделки старых систем и их замены на более новые. Создатели инфраструктуры гордятся своей способностью не только строить очень большие системы, но и создавать изящные способы перехода на них.

Если вы создатель инфраструктуры, у вас есть две группы пользователей. Основной массе пользователей нужно, чтобы компьютерная инфраструктура была надежной, а новая инфраструктура устанавливалась вчера. Другие ваши пользователи – это системные администраторы, чьи системы полагаются на инфраструктуру, которую вы строите. Системным администраторам нужна документация и инфраструктура, которая является надежной и простой для их понимания, и она нужна им *сейчас*, потому что, если вы не уложитесь в срок, их проекты тоже задержатся.

A.1.8. Создатель политики

Политики – основа информационных технологий. Они распространяют требования высших руководителей компании и определяют, как, когда и почему все нужно делать. Часто системных администраторов просят создавать политики в интересах своего руководства. Социальные проблемы невозможно решить технологическим путем. Некоторые социальные проблемы могут быть решены только при помощи письменной политики.

Ценность создателей политики для компании в том, что они решают некоторые проблемы и предотвращают возникновение новых. По мере роста компании распространение информации становится все более сложным и важным.

Создатели политик получают удовлетворение от осознания того, что их знания, навыки и личный опыт были внесены в политику, которая улучшила организацию. Кроме того, они получают удовольствие от того, что являются координаторами, которые могут получить признание многих различных сообществ.

Если вы создатель политики, пользователи рассчитывают, что вы будете учитывать их пожелания. Это нужно делать на начальном этапе процесса. Если спрашивать мнение людей после принятия основных решений, это лишает их влияния. Ваше желание слушать оценят.

A.1.9. Системный клерк

У системных клерков очень мало власти и ответственности по принятию решений. Таким системным администраторам дают указания, которые нужно выполнять, например «Создайте учетную запись для Фреда» или «Выделите IP-адрес». Если системный клерк – помощник системного администратора более высокого уровня, это может быть хорошим местом. На самом деле это прекрасный способ

начать карьеру. Однако мы видели системных клерков, находившихся под началом нетехнических руководителей, которых раздражало, что клерк не мог выполнять задачи за пределами своих нормальных обязанностей.

Ценность системных клерков для компании связана с выполнением задач, которые иначе отвлекали бы старших системных администраторов от более специализированных задач, и заменой отсутствующих системных администраторов. Кроме того, системный клерк является прекрасным кандидатом на должность более старшего системного администратора при ее освобождении. Клерк уже знает среду, а менеджер по подбору персонала знает клерка. Однако, если в среде нет старших системных администраторов, клерки часто являются «козлами отпущения» из-за плохой компьютерной среды, тогда как реальная проблема заключается в недостатке понимания руководством технической работы.

Клерк получает удовлетворение от хорошо сделанной работы, от обучения новым навыкам и от стремления к карьерному росту.

Если вы клерк, пользователям нужно немедленное выполнение их запросов, вне зависимости от того, являются ли они разумными. В главе 31 более подробно рассмотрено, как справиться с такой ситуацией.

Пример: компания, где были только системные клерки

Компании нужен баланс между старшими системными администраторами и клерками. В одной компании были только системные клерки. Их обучение включало зачаточные навыки работы с UNIX: выполнение резервного копирования, создание учетных записей, выделение IP-адресов и IP-подсетей, установку новых программ и добавление новых узлов. Клерки были жертвой синдрома «всегда можно добавить еще одного»: новые назначения слепо выполнялись по первому требованию без общего плана для повышения емкости. Например, новый узел мог быть добавлен в подсеть без какого-либо планирования емкости сети. Какое-то время это работало, но в конце концов привело к перегрузке подсетей.

Пользователи жаловались на медленные сети, но у клерков не было навыков проектирования сетей для устранения проблемы. Пользователи решали эту проблему сами, запрашивая частные подсети, чтобы получить собственный выделенный канал. Клерки неохотно выделяли новые IP-подсети, и пользователи подключали их к остальной сети при помощи маршрутизирующей подстанции с двумя сетевыми картами. Такие соединения были ненадежными, потому что узлы медленно маршрутизировали пакеты, особенно при перегрузке. Чем более перегруженными становились основные сети, тем больше создавалось выделенных подсетей. В конце концов медленная работа сети стала, главным образом, обусловлена медленными соединениями между этими частными участками. Вычислительные серверы компании тоже страдали от отсутствия планирования емкости. Пользователи устанавливали свои вычислительные серверы даже несмотря на то, что проблемы с быстродействием, с которыми они сталкивались, были, скорее всего, связаны с медленной маршрутизацией, обеспечиваемой рабочими станциями. Эти новые, быстрые серверы перегружали сеть с пропускной способностью 10 Мбит/с

особенно из-за того, что часто они были на порядок быстрее, чем узлы, которые выполняли маршрутизацию.

К тому времени, когда организация наняла старшего системного администратора, сеть представляла собой болото из ненадежных подсетей, плохо настроенных вычислительных серверов и древних файловых серверов. В сети было 50 подсетей на приблизительно 500 пользователей. Расчистка и модернизация сети заняла около двух лет.

А.1.10. Лаборант

Лаборант – это системный администратор узкоспециализированного оборудования. Например, в химической исследовательской компании лаборант может отвечать за небольшую сеть, которая объединяет все микроскопы и устройства мониторинга. В компании по производству телекоммуникационного оборудования лаборант может поддерживать все оборудование в помещении обеспечения совместимости протоколов, имея в наличии экземпляр каждой версии продукта, конкурирующие продукты и набор генераторов трафика. Лаборант несет ответственность за установку нового оборудования, интеграцию систем для специализированных проектов[1], а также должен достаточно хорошо разбираться в сфере деятельности пользователей, чтобы переводить их желания в задачи, которые ему нужно выполнить. У лаборанта обычно есть небольшая сеть или группа сетей, которая соединена с главной корпоративной сетью и зависит от нее по большинству служб; если он неглупый, он также заведет друзей в области корпоративных служб, чтобы советоваться с ними в технических вопросах.

Ценность лаборантов для компании состоит в том, что они позволяют исследователям сосредоточиться на проектировании экспериментов, а не на их выполнении. Кроме того, лаборанты ценны своими обширными знаниями технической информации.

Лаборант получает удовлетворение от вовремя завершенного эксперимента или презентации. Тем не менее, если он не получает непосредственных поздравлений от исследователей, с которыми работает, он может обидеться. Лаборантам следует помнить, что их исследователи благодарны вне зависимости от того, показывают они это или нет. Исследователи будут дольше работать с лаборантами, если последних приглашают на церемонии вручения наград, ужины и т. д.

Если вы играете роль лаборанта, пользователи хотят знать, можно ли что-то сделать, а не как это будет сделано. Они хотят, чтобы их требования были выполнены, хотя выяснить у них эти требования – ваша обязанность. В этой области могут сильно помочь навыки активного слушания.

А.1.11. Искатель продуктов

Искатель продуктов читает все технические журналы и обзоры, и когда кто-нибудь спрашивает: «Существует ли программное обеспечение для сжатия клипов?», он может посоветовать не только несколько систем сжатия клипов, но и способы, которыми можно определить, какой из них лучше всего подходит

[1] В большинстве лабораторий они все специализированные.

для конкретного приложения. Он также знает, где можно найти подобный продукт.

Ценность такого искателя для компании заключается в его способности быть в курсе последних новинок. Руководителям не нужно пристально следить за этим человеком, потому что они ужаснутся, обнаружив, что он проводит половину рабочего дня за чтением журналов и веб-сайтов. Руководители должны сравнить это с тем временем, которое искатель экономит всем другим.

Искатели продуктов получают удовлетворение, когда все используют правильные продукты. Эти люди могут раздражать других сотрудников группы, даже тех, кому они помогают, так как все хотят иметь время на то, чтобы «полазить» в Интернете и быть в курсе новинок, но у большинства людей (поневоле) другие приоритеты.

Если вы являетесь искателем продуктов, пользователям нужны краткие сводки, а не детали. Если вы будете описывать все детали, которые выяснили по данной теме, что подобно многочасовому чтению длинной и сумбурно написанной статьи, они будут вас избегать. Будьте немногословны.

A.1.12. Проектировщик решений

Проектировщики решений играют ключевую роль в компании. Вскоре после того, как они услышат, в чем заключается проблема, у них уже будет решение, лучшее, чем кто-либо мог ожидать. Это может относиться как к небольшим вопросам, таким как установка сервера электронного факса для упрощения процедуры отправки факсов, так и к крупным вопросам, например созданию электронной версии бухгалтерии. В отличие от искателей продуктов, проектировщики решений с большей долей вероятности создадут что-то с нуля или интегрируют несколько меньших продуктов.

Ценность проектировщиков решений для компании состоит в их способности устранять препятствия и упрощать бюрократические процессы.

Проектировщик решений получает удовлетворения от сознания того, что люди охотно используют его решения, поскольку это означает, что людям они нравятся.

Если вы являетесь проектировщиком решений, пользователям нужно, чтобы проблема была решена в соответствии с их видением, а не тем, что вы понимаете под проблемой или что сэкономит компании деньги. Например, если отчеты о затратах отсылаются факсом в главный офис, вы должны создать способ, позволяющий передавать данные в электронном виде, чтобы в главном офисе не приходилось перепечатывать все данные. Однако ваши клиенты не получат пользы от того, что вы сэкономите время сотрудникам главного офиса; им нужно просто упростить подготовку документа. Это можно решить созданием лучшего пользовательского интерфейса или системы, которая могла бы загружать их корпоративный кредитный счет с сайта провайдера службы. Ваших пользователей не будет интересовать, будет ли результат затем отправлен по факсу в главный офис для повторного ручного ввода.

A.1.13. Искатель специализированных решений

Искатель специализированных решений может в экстренной ситуации создать решение для, казалось бы, нерешаемой проблемы. Это человек, который может каким-то магическим путем установить безопасное соединение с Луной, чтобы

представить вашу большую презентацию ее обитателям. Такие люди могут знать о средствах больше, чем обычный человек, который пользуется этими средствами, возможно, благодаря их изучению. В отличие от героя, который возвращает ситуацию в нормальное русло, устраняя проблемы, этот человек создает решения.

Ценность искателя специализированных решений состоит в его способности находить решения несмотря на тот факт, что технология не является настолько гибкой, как того требуют некоторые особые ситуации, или на то, что ваша корпоративная сеть имеет слабые места, исправлением которых вы еще не занимались. Первое – это ситуация, которая со временем становится лучше. Второе показывает отсутствие должного технического управления.

Искатель специализированных решений получает удовлетворение, спасая ситуацию. Как и герой, искатель специализированных решений может «сгореть» на работе от перегрузок.

Если играете роль искателя специализированных решений, пользователи хотят, чтобы свершались чудеса, и не хотят напоминаний, что чрезвычайной ситуации можно было избежать за счет лучшего планирования, поскольку это редко относится к их ошибкам.

А.1.14. Искатель незатребованных решений

Некоторые системные администраторы занимаются тем, что внедряют решения, которые не были затребованы. Это может быть как хорошо, так и плохо. Одного системного администратора наградили за установку пользователям системы отправки факсов без использования бумаги, которую не просили ставить, но которая вскоре привела к серьезному повышению производительности. Она была основана на открытом программном обеспечении и использовала уже имеющийся в наличии модемный пул, так что реальная стоимость этой системы была нулевой. Этому же системному администратору однажды объявили выговор за то, что он слишком много времени проводил за «самодеятельными проектами», и заставили сосредоточиться на задачах, которые он должен решать.

Ценность для компании сотрудников, занимающихся незатребованными решениями, заключается в том, что обычно они находятся ближе к пользователям и в состоянии увидеть те их потребности, которые высшее руководство не увидело бы или не поняло. Кроме того, эти системные администраторы лучше осведомлены о новых продуктах, чем их менее технически продвинутые пользователи.

Люди на этой должности получают удовлетворение, когда обнаруживают, что их догадки о том, что может быть полезным, оказываются верными.

Если вы находитесь на этой роли, пользователи хотят, чтобы вы правильно угадывали то, что будет или не будет им полезно; очень важно регулярно, в определенное время, с ними разговаривать. Они будут беспокоиться, не скажутся ли эти новые проекты негативно на сроках выполнения непосредственно ваших проектов, а особенно их собственных. Руководство будет беспокоиться о стоимости вашего рабочего времени и любых материальных затратах, особенно когда незатребованная служба не используется.

A.1.15. Эксперт по вызову

Эксперт по вызову всегда может дать совет. Этот человек зарекомендовал себя как разбирающийся во всех или почти во всех аспектах системы. Иногда эксперт по вызову имеет узкую специализацию; в других случаях его знания являются всесторонними.

Ценность экспертов по вызову для компании заключается в том, что к этому человеку всегда можно обратиться, когда людям необходим совет – либо точное решение, либо просто хорошая начальная точка для исследований.

Эксперт по вызову получает удовлетворение от помощи людям и от гордости за занимаемую роль. Так как технологии стремительно развиваются, ему нужно время для расширения своих знаний, будь то чтение соответствующих журналов, участие в конференциях или эксперименты с новыми продуктами.

Если вы являетесь экспертом по вызову, вам следует напоминать людям, что можно работать и самостоятельно. В противном случае вы не справитесь со всеми взятыми обязательствами.

A.1.16. Преподаватель

Преподаватель учит пользователей работать с доступными службами. Преподаватель может отвлечься от процесса устранения неполадки с принтером, чтобы объяснить пользователю, как лучше пользоваться электронными таблицами, и часто пишет бóльшую часть пользовательской документации.

Преподаватель важен для компании, потому что результатом его работы является более эффективное использование рабочих инструментов. У преподавателя тесные взаимоотношения с пользователями, вследствие чего он знает, какие у людей есть проблемы. Он становится средством, через которое можно узнать о нуждах пользователей.

Преподаватель получает удовлетворение от осознания того, что его документацию используют и уважают и что люди работают лучше благодаря его трудам.

Если вы находитесь на роли преподавателя, пользователи хотят, чтобы вы разбирались в сфере их деятельности, в особенностях их работы и, самое важное, в том, что их не устраивает в средствах, которыми они пользуются. Они хотят, чтобы документация содержала ответы на вопросы, которые у них возникают, а не на те, которые важны по мнению разработчиков.

A.1.17. Блюститель политики

Блюститель политики – это человек, который говорит «нет», когда кто-то хочет сделать что-то, противоречащее политике, а также пресекает действия нарушителей. Блюститель политики одинаково зависит от двух факторов: от письменных правил и поддержки руководства. Правила должны быть записаны и опубликованы, чтобы все были о них осведомлены. Если правила нигде не записаны, действия блюстителя будут несостоятельными, так как ему придется создавать правила на ходу, а его коллеги могут иметь другое мнение по поводу того, что правильно, а что нет. Второй фактор – это поддержка руководства. Политика не имеет силы, если руководство меняет правила каждый раз, когда

кто-то просит сделать исключение. Руководителю не следует утверждать политику, а затем постоянно менять ее при просьбе сделать исключение. Зачастую блюститель политики обладает полномочиями отключить сетевой кабель, если нарушение создает глобальные проблемы, а связаться с нарушителем быстро невозможно. Если руководство не поддерживает решение блюстителя политики, он не сможет выполнять свою работу. Если руководство подтверждает политику, но затем разрешает исключение после отказа блюстителя, он потеряет влияние и желание или основания продолжать свою деятельность.

Ценность блюстителя политики для компании состоит в том, что политика компании приводится в исполнение. Если важную политику не осуществлять полностью, то смысл ее наличия теряется.

Блюститель политики получает удовлетворение, осознавая, что он старается удерживать курс компании в соответствии с направлением, установленным руководством, а также обеспечивая жесткое соблюдение правил по всей компании.

Если вы являетесь блюстителем политики, пользователи хотят просто выполнять свою работу и не понимают, почему так много препятствий (правил) мешают им это сделать. Вместо того чтобы говорить «нет», может быть правильнее выяснить, чего они хотят добиться, и помочь им достичь своих целей, не нарушая политики. Если вам не нравится играть эту роль, но приходится, вы можете попробовать потренировать уверенность в себе или почитать такие книги, как *«When I Say No I Feel Guilty»* (Smith 2000).

Политика с исключениями

У компании была политика безопасности, которая создавала множество лишней работы для всех, кто хотел ее соблюдать. Чтобы веб-сайт был доступен за границей брандмауэра, этот сайт приходилось дублировать снаружи, вместо того чтобы создать «брешь» в брандмауэре и предоставить внешним пользователям доступ к внутренней машине. Этот дублирующий сайт не мог соединяться с внутренней сетью компании. Если был необходим доступ к внутренней службе, например к базе данных, эту службу также приходилось дублировать. Сделать службу полностью независимой было очень сложно. Поэтому, когда блюститель политики отклонял запрос, сотрудники начинали плакаться руководству и обычно одобрялось исключение. В итоге в брандмауэре появилось столько брешей, что политика потеряла всякий смысл.

Блюститель политики предложил ее пересмотр, чтобы она попросту отражала поведение руководства: если затраты на дублирование, требующие нескольких рабочих часов, окупятся, то будут создаваться бреши в брандмауэре. Руководство было шокировано таким предложением, потому что это не соответствовало их предпочтениям по воплощению политики безопасности. Блюститель политики указал все исключения, которые сделало руководство. Хотя старые исключения остались в силе, после пересмотра политики руководство стало гораздо больше поддерживать блюстителя политики. Если руководство не собиралось поддерживать политику, то и блюстителю политики этого делать не следовало.

A.1.18. Перестраховщик

Кому-то в группе следует беспокоиться о том, что что-то может пойти не так. Когда предлагается решение, этот человек спросит: «А что произойдет при неудаче?» Конечно, этот человек не может определять все решения, иначе проекты никогда не будут завершены либо выйдут за пределы бюджета. Этого человека следует уравновесить оптимистом. Однако, если никто не следит за потенциальными опасностями, группа может построить «карточный домик».

Ценность для компании перестраховщика чувствуется только в чрезвычайных ситуациях. Половина системы отказала, но другая половина продолжает работать благодаря грамотно установленным средствам управления. Результатом работы этого человека может быть общая отказоустойчивость системы.

Этот человек получает удовлетворение от собственной уверенности в безопасности и стабильности.

Если вы находитесь на этой должности, люди вокруг вас могут устать от того, что вы постоянно требуете, чтобы они «пристегнули ремни». Важно воплощать свои решения в жизнь, а не просто высказывать свое мнение на каждом шагу. Никто не любит слушать жалобы наподобие «Этой неудачи не произошло бы, если бы люди меня послушали» или «В следующий раз вы не будете так просто меня игнорировать». Может быть лучше разделять ответственность, вместо того чтобы определять виноватых, и работать над последующим улучшением, вместо того чтобы тайно радоваться своей прозорливости: «В будущем нам будет необходимо написать скрипты, которые справляются с ситуацией переполнения дисков». Вежливый инструктаж с глазу на глаз гораздо более эффективен, чем публичные жалобы.

A.1.19. Осторожный проектировщик

Осторожный проектировщик долго планирует каждый шаг проекта, в котором он участвует. Он строит хорошие тестовые макеты и никогда не смущается, когда что-то идет не так, потому что уже выяснил, что делать.

Ценность осторожного проектировщика для компании состоит в том, что он выполняет важные задачи надежно и безукоризненно.

Этот человек получает удовлетворение от завершения задачи и осознания того, что она завершена должным образом, а также наблюдая, как первые пользователи используют ее без заминок. Он гордится своей работой.

Если вы играете эту роль, другие могут привыкнуть полагаться на то, что ваша работа безукоризненна. Вам часто дают задачи, в которых нельзя допускать ошибок. Продолжайте работать так, как вы всегда работали, и не позволяйте важности задач перевесить все другие факторы. Не забывайте, что ваша тщательная работа требует времени, а другие постоянно спешат и могут возмутиться, глядя на то, как вы работаете. Убедитесь, что вы развиваете талант прогнозирования того, как много времени вам понадобится, чтобы завершить задачу. Вы же не хотите, чтобы вас считали человеком, который не может выполнить задачу в срок.

А.1.20. Проектировщик пропускной способности

Проектировщик пропускной способности расширяет систему по мере ее роста. Этот человек замечает, когда что-либо переполняется, истощается или становится перегруженным. *Хорошие* проектировщики пропускной способности уделяют внимание структурам использования и знают об изменениях бизнеса, которые могут их затронуть. *Искусные* проектировщики пропускной способности устанавливают системы, которые проводят такой мониторинг автоматически и создают графики, которые предсказывают, когда пропускной способности будет недостаточно. Производители могут помочь проектировщикам пропускной способности, документируя данные, которые могут быть им полезны, такие как необходимое количество оперативной памяти и дискового пространства в зависимости от числа пользователей.

Ценность проектировщиков пропускной способности для компании заключается в том, что предотвращаются заторы трафика. Это еще одна роль, которая остается незамеченной, если работа выполнена должным образом. Человек также помогает компании правильно решить важную проблему. (Слишком часто мы видели, как подразделения пытались ускорить работу сервера, добавляя больше оперативной памяти, хотя реальной проблемой была перегруженная сеть, и наоборот.)

Проектировщик пропускной способности получает удовлетворение от осознания того, что проблемы были предотвращены и что люди принимают предупреждения к сведению, а также от определения реального источника проблем.

Если вы являетесь проектировщиком пропускной способности, пользователи хотят, чтобы у вас имелись точные данные и решения, которые не будут стоить денег. Оправдывать затраты – ваша работа. Как всегда, очень важно объяснить ситуацию на языке клиента.

А.1.21. Администратор бюджета

Администратор бюджета ведет счет деньгам, которые остались в бюджете, и помогает составить бюджет на следующий год. Этот человек знает, на что следует направить денежные затраты, когда это необходимо, и как можно растянуть бюджет пошире.

Ценность администратора бюджета для компании состоит в том, чтобы контролировать затраты на системное администрирование, обеспечивать финансирование задач, требующих выполнения, в пределах разумного – даже если они были неожиданными, – и предоставлять достоверные сведения, чтобы руководство могло произвести финансовое планирование на следующий год.

Администратор бюджета получает удовлетворение от того, что он не выходит за пределы бюджета и при этом справляется с финансированием дополнительных важных проектов, которые не были включены в бюджет.

Если вы являетесь администратором бюджета, пользователи хотят, чтобы вы оставались в пределах бюджета, готовили хороший бюджетный план на следующий год, точно определяли, какие проекты являются самыми важными, чтобы обеспечить финансирование всех приоритетных задач, и показывали, каким образом деньги, которые они позволили вам потратить, приносят им выгоду.

A.1.22. Адвокат пользователей

Адвокат пользователей может помочь человеку заявить о его потребностях. Он переводчик и лоббист, посредник между пользователем и его руководством. Адвокат не просто рекомендует решение, но и объясняет пользователю, как представить его идею руководителю, и присутствует при этом, на случай если человеку понадобится помощь.

Ценность адвоката пользователей для компании состоит в том, чтобы помогать пользователям получать то, что им нужно, несмотря на бюрократию и затруднения в общении.

Адвокат получает удовлетворение от осознания того, что он кому-то помог. Он также знает, что, взаимодействуя с руководством, он может представить свою группу системного администрирования в хорошем свете, и играет роль полезного координатора. Часто вы помогаете пользователю получить то, что он хочет, при помощи системы, а не обходя ее. Это особенно важно, если вы сами участвовали в создании этой системы.

Если вы являетесь адвокатом, пользователи хотят, чтобы вы поняли их, прежде чем начнете предлагать решения. Пользователи хотят, чтобы вы поняли их технические потребности, а также щепетильные вопросы, касающиеся расписаний и средств.

A.1.23. Технократ

Технократ – это сторонник новых технологий. Когда систему необходимо починить или заменить, он отдает предпочтение новой системе, даже если она еще не доведена до безупречного состояния. Он презирает тех, кто считает удобными старые системы, которые еще «достаточно хороши». Технократ может быть хорошим противовесом перестраховщику.

Ценность технократа для компании заключается в том, что он удерживает компанию от технического застоя.

Технократ получает удовлетворение от того, что погружен в море последних технологий, – можно сказать, от синдрома «новой игрушки».

Если вы технократ, пользователи хотят, чтобы вы сосредоточились на реальной ценности решения, а не бездумно отдавали предпочтение всему новому.

A.1.24. Продавец

Продавец не ограничен только лишь материальными аспектами. Он может продавать конкретную политику, новую службу или план. Он может продавать саму группу системного администрирования – либо высшему руководству, либо пользователям. Продавец занимается тем, что выясняет потребности пользователей, а затем убеждает их в том, что его товар отвечает их нуждам. Новые службы легче продать, если пользователи были вовлечены в процесс определения характеристик и выбора средств.

Ценность продавца для компании заключается в том, что он упрощает работу группы системного администрирования. Великолепная система, которая никогда не будет принята пользователями, бесполезна для компании. Великолепная политика, которая экономит компании деньги, бесполезна, если пользователи обходят ее, потому что не понимают ее преимуществ.

Продавец получает кратковременное удовлетворение от продажи, но для настоящего, длительного удовлетворения продавец должен развить взаимоотношения с пользователями и ощущать, что сильно помогает им.

Если вы являетесь продавцом, пользователи хотят, чтобы вы понимали и уважали их потребности. Они хотят, чтобы с ними разговаривали, а не указывали.

А.1.25. Контактер с поставщиком

Контактер с поставщиком поддерживает связь с одним или более поставщиками. Он может знать линию продуктов поставщика лучше, чем кто-либо еще в группе, и быть в курсе следующих продуктов. Он является ресурсом для других системных администраторов, таким образом сокращая время звонков продавцу производителя.

Ценность для компании контактера с поставщиком состоит в том, что это человек, который понимает и специализируется на потребностях компании по взаимодействию с поставщиком.

Контактер с поставщиком получает удовлетворение от того, что он является экспертом, которого все уважают, от того, что он первый узнает новости производителя, и от бесплатных обедов и футболок, которые он получает.

Если вы являетесь контактером с поставщиком, пользователи будут хотеть, чтобы вы знали все о производителе, непредвзято относились к конкурирующим производителям и жестко торговались при установке цен.

А.1.26. Провидец

Провидец смотрит на общую картину и имеет представление о направлении, по которому компании следует идти.

Ценность провидца для компании состоит в том, что он поддерживает сосредоточенность группы на том, что происходит.

Провидец получает удовлетворение, когда он оглядывается на много лет назад и видит, что в долгосрочной перспективе его работа очень важна. Все эти постепенные улучшения в итоге привели к выполнению основных задач.

Если вы являетесь провидцем, пользователи хотят знать, что произойдет в будущем и не хотят слишком сильно беспокоиться о долгосрочной перспективе. Репутация вашей группы в смысле способностей по выполнению плана влияет на возможность продавать ваши замыслы пользователям.

А.1.27. Мать

Мать опекает пользователей. Это сложно объяснить без примера. Один системный администратор каждое утро ходил по комнатам, останавливаясь у рабочего стола каждого человека, чтобы посмотреть, как идут дела. Он мог исправить мелкие неполадки и напомнить о более крупных проблемах текущего дня. Он отвечал на множество мелких вопросов по интерфейсу пользователя, которые, по мнению пользователя, были слишком несущественны, чтобы задавать их службе поддержки. Пользователи осуществляли большой переход (с X-терминалов на настольные эмуляторы X-терминалов), и такая материнская забота была как раз тем, что им было нужно. За эти утренние прогулки он отвечал на сотни вопросов и разрешал десятки проблем, которые в ином случае были бы

отправлены в службу поддержки. Пользователи привыкли к такому уровню обслуживания и скоро стали полагаться на его утренние визиты как на один из факторов, которые повышают продуктивность их деятельности.

Ценность матери для компании заключается в высокой степени поддержки, что может быть очень важно во времена больших перемен или при обслуживании нетехнических пользователей. Личностное общение также прибавляет уверенности в том, что нужды клиентов будут поняты точно.

Мать получает удовлетворение от человечности взаимоотношений, которые она развивает со своими клиентами.

Если вы являетесь матерью, пользователи хотят знать, что их срочные потребности выполнены, и станут уделять меньше внимания долгосрочной стратегии. Вы же должны не забывать о будущем и не слишком сильно погружаться в настоящее.

A.1.28. Наблюдатель

Наблюдатель следит за тем, насколько хорошо идут дела. Иногда наблюдатель использует устаревшие технологии, применяя те же службы, что и его пользователи. Хотя у системных администраторов может иметься собственный файловый сервер, этот человек хранит свои файлы на одном сервере с клиентами, чтобы он мог «почувствовать их боль». По мере того как этот человек становится более опытным, он автоматизирует мониторинг, а затем просматривает выходные данные системы мониторинга и тратит время на исправление неполадок, а не просто стирает предупреждения.

Ценность наблюдателя для компании состоит в том, что проблемы замечаются до того, как пользователи начинают жаловаться. Это может создать впечатление безотказно работающей сети.

Наблюдатель получает удовлетворение от того, что первым замечает проблему и решает ее до того, как пользователи о ней сообщат, а также от осознания, что проблемы были предотвращены посредством мониторинга характеристик пропускной способности.

Если вы являетесь наблюдателем, пользователи, скорее всего, не будут знать о вашем существовании. Если бы они знали, они бы захотели, чтобы ваше тестирование симулировало их реальную рабочую нагрузку и было сквозным. Например, недостаточно знать, что сервер электронной почты работает. Вы должны убедиться, что сообщение может быть отправлено, передано, доставлено и прочитано.

A.1.29. Координатор

У координатора отличные навыки общения. Он стремится превратить спонтанные дискуссии во встречи по принятию решений. Его часто просят провести совещание, особенно большое, на котором сложно поддерживать сосредоточенность на вопросе.

Координатор важен тем, что обеспечивает более спокойное протекание процессов. Он может и не предпринимать много мер, но помогает группам людей договориться о том, что необходимо сделать и кто будет это делать. Он делает совещания эффективными и живыми.

Координатор получает удовлетворение от вида людей, пришедших к согласию в своих целях, и от проявления инициативы для достижения этих целей.

Если вы являетесь координатором, другие члены вашей группы хотят, чтобы вы координировали все их переговоры. Важно учить других людей быть координаторами и создавать среду, в которой все имели бы хорошие навыки общения.

А.1.30. Пользователь/системный администратор

Иногда пользователь одновременно является и системным администратором, возможно, потому, что у пользователя есть какие-то определенные обязанности, которые требуют привилегированного доступа, либо он ранее был системным администратором и сохранил некоторые из этих обязанностей.

Ценность пользователя/системного администратора для компании заключается в том, что он может подменить других системных администраторов, когда они находятся в отпуске. В действительности в ситуациях, когда есть только один системный администратор, очень полезно обучить кого-либо из пользователей вопросам, связанными с ежедневными операциями, чтобы он смог заменить системного администратора на время отпуска. Может быть очень полезно иметь дополнительного человека, который умеет менять ленты в системе резервного копирования, создавать учетные записи пользователей и решать десять самых распространенных проблем.

Пользователь/системный администратор получает удовлетворение от своей роли, если он имеет доступ системного администратора или привилегированного пользователя. Кроме того, он может получать своего рода «боевую надбавку» за обучение смежной профессии.

Если вы являетесь пользователем/системным администратором, основная группа системного администрирования хочет знать, что вы не мешаете их планам, соблюдаете правильные процедуры и следуете тем же этическим правилам, что и они. Другие пользователи хотят знать, что вы сможете решить многие проблемы, если вас об этом попросят.

А.1.31. Помощник пользователей

Системный администратор, помогающий пользователям, видит свою работу в том, чтобы концентрироваться на запросах живых пользователей, а не на технических процессах, в которых он участвует. Он рассматривает свою работу как помощь пользователям в работе с системой, которая довольно статична. Основные изменения в системе исходят от внешних сил, таких как группа программирования систем.

Системный администратор, помогающий пользователям, важен для компании как всегда доступный живой представитель всей группы системного администрирования. Многие пользователи никогда не видят заднюю линию поддержки.

Системный администратор, помогающий пользователям, получает удовлетворение от личных взаимоотношений, которые он развивает, и от теплого чувства, вызванного осознанием, что он помог реальному живому человеку.

Если вы являетесь системным администратором, поддерживающим пользователей, последние хотят, чтобы их задачи выполнялись в соответствии с их расписанием. Если они обнаруживают, что ситуация экстренная, они ожидают, что вы все бросите и придете им на помощь.

A.1.32. Навигатор по политике

Навигатор по политике понимает правила и нормы бюрократической системы и может помочь остальным проходить через них или в обход них. Навигатор может помочь кому-либо пройти через бюрократический процесс или обойти политику без ее нарушения.

Навигатор по политике важен для группы системного администрирования, так как помогает быстрее выполнять задачи, когда приходится иметь дело с бюрократической системой и когда необходимо обойти систему, не подвергая ее риску нарушения.

Навигатор по политике получает удовлетворение от осознания, что его связи и знания способствовали выполнению проекта.

Если вы являетесь навигатором по политике, ваши пользователи хотят, чтобы задачи были выполнены, вне зависимости от того, остаетесь ли вы в пределах норм системы. Это может поставить вас в трудное положение, когда пользователю кажется, что легче нарушить политику или работать в обход системы.

A.2. Отрицательные роли

В следующих разделах описаны некоторые отрицательные роли, которых вам следовало бы избегать.

A.2.1. Экстремал

Иногда, системный администратор может быть настолько увлеченным новой технологией, что ищет пути испытать ее на пользователях до того, как она будет разработана до состояния готовности. Вместо того чтобы быть на переднем крае, он держит компанию *на острие технологий*. В таком случае получается, что пользователи всегда страдают от недостатков новых, еще не отработанных служб.

A.2.2. Консерватор

Противоположностью экстремала является сотрудник, который оттягивает использование любой новой технологии. У этого человека, стремящегося уйти от риска, всегда есть любимое оправдание, например неудовлетворенность планом отмены изменений. Он доволен текущей версией операционной системы, текущим дистрибутивом операционной системы, текущей маркой компьютера, количеством каналов связи и типом сетевой топологии. Этот человек не замечает отсутствия обновления технологий и проблем, к которым это приводит. По иронии судьбы раньше этот человек всегда был на передовых позициях, но теперь погряз в рутине. Он может быть тем самым человеком, который отказался от мэйнфреймов и осваивал UNIX или смеялся над пользователями рабочих станций, которые не переходили на персональные компьютеры. Однако это время прошло, он нашел что-то, с чем ему удобно, и теперь сам стал таким человеком, над которым посмеялся бы много лет назад.

A.2.3. Паникер

Этот человек беспокоится о том, что еще не происходит и с большой долей вероятности никогда не произойдет. Почти все системное администрирование свя-

зано с управлением рисками, но этот человек считает, что любой риск неприемлем. Этот человек замедляет проекты и не дает им сдвинуться с мертвой точки. Он предсказывает гибель или неудачу без каких-либо фактов, подтверждающих это. Иногда он просто испытывает дискомфорт от своей неспособности что-то контролировать или от недостатка обучения. Порой этот человек будет тратить много рабочего времени, трудясь над проблемами, которых вы даже не видите, и игнорировать более срочные задачи. Самая большая опасность этого человека в том, что, когда он действительно будет прав, его проигнорируют.

A.2.4. Ковбой

Ковбой приступает к устранению неполадок в системах или разработке новых служб без должного планирования, размышлений о последствиях или разработки плана отмены изменений. Он не думает о том, чтобы предварительно спросить своего руководителя или посоветоваться с пользователями. Он не проверяет должным образом результаты своего труда, чтобы убедиться, что все работает, и уходит домой, никому не сообщая об этом. Он считает себя исключительно талантливым и производительным и думает, что другие пытаются поставить на его пути слишком много бюрократических препятствий и что они недооценивают его таланты. Ковбой ничего не документирует и просто знает, что он бесценен для компании.

Ковбой

В компании среднего размера, производящей аппаратное обеспечение для компьютеров, должность старшего системного администратора занимал ковбой. Его руководство привлекло группу консультантов, чтобы перепроектировать сеть и построить план перехода от старой сети к новой. План был подтвержден, оборудование заказано, расписание составлено и согласовано с клиентами, и планы по тестированию были созданы совместно с пользователями. Когда пришло новое оборудование, ковбой задержался на работе, выкинул все старое оборудование и установил новое. Он не использовал новую архитектуру; он игнорировал все пункты из плана перехода, касающиеся несвязанных задач, которые нужно было решить в процессе перехода; он также не стал утруждать себя проведением тестирования. На следующий день, когда люди пришли на работу, многие из них обнаружили, что у них нет сетевого соединения, – среди них были генеральный директор, целый отдел поддержки пользователей, цепь руководства ковбоя и многие инженеры. Служба поддержки и остальная группа системного администрирования не имели ни малейшего понятия, что произошло, потому что он никому ничего не сказал и даже не удосужился придти на работу в этот день вовремя – в конце концов, он же задержался вчера на работе! Он был все еще горд тем, что сделал, и совершенно не испытывал стыда, потому что считал план перехода и тестирование излишней тратой времени и денег. Он наслаждался, показывая, что смог сделать все это сам за несколько часов, в то время как консультантам для этого потребовалось гораздо больше времени. Он не обратил внимания на стоимость того большого перебоя, который он вызвал, и вреда, нанесенного репутации группы системного администрирования.

A.2.5. Раб, козел отпущения или швейцар

Иногда системные администраторы играют роль рабов, козлов отпущения или швейцаров. Рабы – это сотрудники, которые выполняют все требования без вопросов, даже если они могли бы предложить лучшее решение, взглянув внимательнее на картину в целом. Иногда другие люди используют системных администраторов как козлов отпущения. Их обвиняют во всем плохом, что происходит. Системных администраторов обвиняют в том, что проект запаздывает, даже если пользователи не сообщали им о своих потребностях. Иногда системные администраторы рассматриваются как швейцары: люди, которые не представляют никакой ценности для бизнеса компании, а являются неквалифицированными рабочими, от которых одни расходы. Все три роли связаны с проблемами руководства, которое не понимает задачи системного администрирования в своей собственной организации. Однако обязанность системных администраторов – исправить такое положение вещей, улучшая взаимодействие и работая над заметностью своей группы в организации.

A.3. Групповые роли

Некоторые групповые роли должны присутствовать в группе системного администрирования, за исключением мученика.

A.3.1. Сквозной эксперт

Сквозной эксперт понимает используемую технологию с самых нижних до самых верхних уровней. Он крайне важен для решения неясных задач, таких как масштабные отказы. Неясные задачи, как правило, являются результатом нескольких одновременных сбоев или неизвестных взаимодействий между различными областями, их решение требует знаний во всех областях. Масштабные отказы затрагивают множество подсистем и требуют глубокого понимания общей архитектуры для выявления реальной проблемы.

A.3.2. Посторонний

Во время продолжительного сбоя системные администраторы, работающие над проблемой, иногда оказываются в ситуации, аналогичной творческому тупику писателей. Они начинают ходить по кругу, не способные сдвинуть ситуацию с мертвой точки. Роль, которая тут лучше всего подходит, – это посторонний, который привнесет свежее видение ситуации. Если попросить кого-либо объяснить то, что происходит в данный момент, люди обычно находят решение. Иногда роль этого человека заключается в том, чтобы убедить остальных попросить помощи извне или передать проблему в вышестоящие органы либо службу поддержки производителя. В другом случае роль этого человека может состоять в том, чтобы просто определить, что пришло время сдаться: есть план отмены и его нужно применить.

A.3.3. Специалист по уровням

Это человек, который определяет, на каком уровне нужно решать конкретную задачу. Люди зачастую склонны думать, что те или иные проблемы можно решить на их уровне. Техники полагают, что им нужно усерднее работать. Про-

граммисты думают, что им необходимо внедрить новое программное обеспечение, чтобы решить проблемы. Однако важную роль играет человек, который понимает устройство всех уровней, включая руководство, и может подсказать, на каком из них лучше всего решить проблему. После недель, проведенных в попытке решить проблему, этот человек заявит, что дешевле и, возможно, эффективнее будет просто обратиться на верхний уровень руководства, чтобы сказать, что данный метод невыполним. Может быть лучше найти ближайшего по старшинству руководителя в структуре организации, который имеет более высокую должность, чем два спорящих пользователя, и попросить его решить эту проблему. Кроме того, скорее всего, это тот человек, который напомнит вам старый афоризм Интернета: «Технологии не могут решить социальные проблемы», и приступит к поиску замены политики.

А.3.4. Мученик

Мученик считает, что никто не выполняет так много работы, как он. Возмущенный тем фактом, что никто, кроме него, не работает так долго, и недовольный отсутствием друзей или финансового успеха, он не может понять, как другие люди могут «сделать это», когда они делают для этого так мало. Этот человек проводит много времени, оплакивая проблемы мира – по большей части его мира. Это может случиться в результате простого морального и физического истощения или низкой самооценки.

Моральное и физическое истощение происходит, когда человек не устанавливает равновесие между работой и отдыхом. К сожалению, в современной интенсивной жизни некоторые люди вырастают, не понимая необходимости отдыха. Они считают, что они всегда должны быть «в работе». Эта крайняя степень рабочей этики может быть секретом их успеха, но без духовного эквивалента профилактического ремонта она ведет к моральному и физическому истощению. В этом случае более усердный труд только делает ситуацию хуже. Людям, которые достигли этого предела, может не помочь даже длительный отдых; и они могут стать еще более раздраженными, если им нечего делать.

Самооценка – это то, что мы обретаем (или не обретаем), когда мы молоды. Теоретики познания считают, что наше душевное состояние – грусть или радость – это показатель не того, плохие или хорошие события с нами происходят, а того, как мы на них реагируем (Burns 1999b). Мы можем быть недовольны какими-либо хорошими событиями, если наша самооценка была повреждена до такой степени, что в любой ситуации мы чувствуем собственную никчемность. Когда такое происходит, мы превращаем хорошие новости и события в повод для беспокойства: «Ему понравилась моя работа над тем проектом! Что если я не смогу каждый раз оправдывать эти ожидания? Что если мои коллеги станут мне завидовать и обидятся на меня?» Для помощи людям в такой ситуации существуют различные терапии (Burns 1999a).

А.3.5. Выполняющий монотонную работу

Некоторые типы личностей имеют склонность к монотонной работе. Этих людей следует ценить, так как они решают неотложные задачи. Невозможно переоценить важность автоматизации, но некоторые процессы нельзя автоматизировать, например физическую доставку новых машин, или они недостаточно монотонны, чтобы автоматизация была финансово эффективна. Эта роль очень важна

для группы. Этот человек может взять на себя монотонную работу, освободив от нее более квалифицированных сотрудников. Эти маленькие задачи часто являются отличной тренировкой для задач более высокого уровня.

A.3.6. Общественный директор

Общественный директор повышает моральный дух группы, находя причины для совместных торжеств; дни рождения, юбилеи, дни приема на работу – это лишь малая их часть. Общение людей в нерабочей обстановке может способствовать созданию сплоченного коллектива. Ключ успеха на этой должности – быть уверенным в том, что люди не будут чувствовать принуждения и что вы не перегибаете палку, подвергаясь риску того, что вашему начальнику подобная деятельность покажется пустой тратой времени.

> **Ежемесячное празднование дня рождения**
>
> В одной группе системного администрирования было принято устраивать каждый месяц коллективный обед. Люди, у которых в этот месяц был день рождения, не должны были платить и были ответственны за организацию обеда в следующем месяце. Эта традиция была важна для сплочения коллектива. По некоторым причинам эта традиция была приостановлена на год. Чтобы заново начать этот процесс, группа устроила обед для всех, «у кого был день рождения за последние 12 месяцев», а руководитель оплатил весь счет.

A.3.7. Мистер Перерыв

Во время чрезвычайной ситуации очень важно присутствие кого-то, кто замечает, что люди очень устали, и убеждает их сделать перерыв. Люди могут считать, что задача слишком важна, чтобы прекратить работу над ней, но этот человек видит бесполезность вымученных попыток и настаивает на перерыве, который всех освежит. Том часто исчезал и возвращался с пиццами и напитками. Часто, отвлекаясь на некоторое время от проблемы, люди смогут посмотреть на нее по-другому и найдут лучшие решения.

Есть и другие роли, которые могут существовать в группе системного администрирования, но мы считаем, что перечисленные выше заслуживают особого упоминания.

A.4. Заключение

Мы надеемся, что после прочтения этого приложения вы посмотрите на себя свежим взглядом и найдете свое отражение в одной или нескольких ролях. Теперь вы будете осознавать то, что вас мотивирует и чем вы подходите вашей группе.

Это может помочь вам понять, что вы играете множество ролей в своей организации и, возможно, особую роль в своей группе. Вы носите разные шляпы.

Примеряя каждую шляпу, вы можете осознать свое значение для компании, свою мотивацию и ожидания пользователей от вас.

Может быть, вы узнали что-то хорошее или плохое про себя. Возможно, вы нашли что-то новое в себе или подтвердили чувства, которые у вас уже были. Это может побудить вас стремиться к улучшениям в своей жизни. В следующий раз, когда вы будете рассуждать о смене работы, вы, возможно, уделите больше времени размышлениям о ролях, которые вам хотелось бы играть или которые подходят к вашим навыкам, и сравнить их с ролями, которые вас просят играть на новом месте. Не беспокойтесь, если вы чувствуете, что вам нравится любая роль. Может быть, это ваша судьба, а возможно, когда у вас будет больше опыта и знаний, вы добьетесь большей ясности в ваших чувствах на этот счет.

Возможно, это приложение заставило вас осознать, что ваша организация нуждается в одной из описанных здесь ролей. Может быть, вы заметили, что в вашей группе системного администрирования чего-то не хватает. Возможно, вам следует попробовать чаще брать эту роль на себя, призывать к этому других или искать нужные навыки, когда вы будете в следующий раз нанимать кого-то на работу. Вы можете обнаружить, что в вашей организации слишком много людей играют одну и ту же роль, а это означает, что вам необходимо лучшее равновесие. Может быть, это приложение помогло вам заметить, что какой-то человек играет отрицательную роль и требуется провести с ним инструктаж, чтобы изменить положение вещей.

Возможно, это приложение заставило вас осознать, что все люди в вашей группе играют слишком много ролей, либо играют недостаточное количество ролей, либо роли не сбалансированы.

Мы очень надеемся, что эта часть книги помогла вам понять, что люди в вашей группе не такие, как вы. Теперь вы можете ценить их за ту значимость, которую они имеют для группы. Сильная группа включает людей с разными навыками и с различным опытом; каждый привносит что-то уникальное. Эти отличия не разобщают группу, а, напротив, делают ее сильнее. Поэтому группа должна осознавать эти отличия и уделять время их оценке, вместо того чтобы стараться их сгладить.

Задания

1. На каких ролях вы хотели бы себя видеть? (Не стесняйтесь.) Вы часто находитесь на этих ролях? Какие незнакомые роли вас привлекают?
2. На каких ролях вы видели себя в начале вашей карьеры? Как они отличаются от ролей, на которых вы находитесь сейчас?
3. На каких ролях вы видите себя в будущем?
4. Какие перемены в своей жизни вы хотели бы осуществить, чтобы вы могли лучше соответствовать своей роли или переходу на новые роли?
5. Какие роли вам не нравятся? Почему? Как они отличаются от ролей, которые вы на данный момент занимаете?
6. Определите, какая роль соответствует каждому человеку из вашей группы. Если вам кажется, что это может повредить вашей дружбе, попросите своих коллег сделать то же самое и поделитесь списками ролей. Сколько стоит курс терапии?

7. Психологи и руководители знают, что других людей нельзя изменить; им необходимо увидеть необходимость перемен самим и захотеть измениться самим. Заставила ли эта глава вас осознать, что кто-то в вашей группе играет отрицательную роль и нуждается в некоторых изменениях личности? Как вы можете помочь этому человеку увидеть необходимость перемен? Этот человек – вы?
8. Каких ролей недостает в вашей группе? Как вы можете развить эти роли в вашей группе?
9. Это приложение не содержит полный список ролей. Какие роли, по вашему мнению, следует добавить в этот список? Какое значение они имеют для организации или группы или почему они относятся к отрицательным ролям? Что относится к мотивирующим факторам этих ролей? Чего пользователи от них ожидают?

B

Сокращения

AC	Переменный ток (Alternating Current)
ACL	Список контроля доступа (Access Control List)
AICPA	Американский институт дипломированных общественных бухгалтеров (American Institute of Certified Public Accountants)
AoE	Интерфейс ATA через Ethernet (ATA over Ethernet)
ASP	Провайдер приложений либо ASP-страница (Application Service Provider или Active Server Page)
ATA	Интерфейс ATA (Advanced Technology Attachment)
ATM	Асинхронный режим передачи (Asynchronous Transfer Mode)
ATS	Автоматический переключатель (Automatic Transfer Switch)
AUP	Политика допустимого использования (Acceptable-Use Policy)
AUSCERT	Австралийская команда экстренной компьютерной помощи (Australian Computer Emergency Response Team)
BGP	Протокол пограничной маршрутизации (Border Gateway Protocol)
CA	Центр сертификации (Certification Authority)
CAD	Автоматизированное проектирование (Computer-Aided Design)
CAP	Колумбийский протокол Appletalk (Columbia Appletalk Protocol)
CDP	Непрерывная защита данных (Continuous Data Protection)
CD-ROM	Компакт-диск (Compact Disk Read-Only Memory)
CEO	Главный исполнительный директор (Chief Executive Officer)
CERT	Команда экстренной компьютерной помощи (Computer Emergency Response Team)
CFO	Главный финансовый директор (Chief Financial Officer)
CGI	Общий шлюзовой интерфейс (Common Gateway Interface)
CIAC	Группа реагирования на нарушения информационной безопасности (Computer Incident Advisory Capability)
CIFS	Общая межсетевая файловая система (Common Internet File System)
CIO	Главный информационный директор (Chief Information Officer)
CMS	Система управления контентом (Content Management System)

Colo	Колокейшн-центр (Colocation Center)
CNAME	Общее имя (DNS-запись) (Common NAME (DNS record))
COO	Главный операционный директор (Chief Operating Officer)
CPU	Центральный процессор (Central Processing Unit)
CSE	Специалист по поддержке пользователей (Customer Support Engineer)
CSU/DSU	Устройство обслуживания каналов/Устройство обработки данных (Channel Service Unit/Data Service Unit)
CTO	Главный технический директор (Chief Technology Officer)
DAD	Плотность доступа к диску (Disk Access Density)
DAS	Накопитель с прямым подключением (Directly Attached Storage)
DC	Постоянный ток (Direct Current)
DHCP	Протокол динамической конфигурации сетевого узла/Протокол DHCP (Dynamic Host Configuration Protocol)
DLT	Цифровая лента с дорожечной записью (Digital Linear Tape)
DNS	Служба доменных имен (Domain Name Service)
DoS	Отказ в обслуживании (Denial of Service)
DR	Аварийное восстановление (Disaster Recovery)
DSL	Цифровая абонентская линия (Digital Subscriber Line)
EAP	Программа помощи сотрудникам (Employee Assistance Program)
EDA	Автоматизация проектирования электроники (Electronic Design Automation)
EIGRP	Улучшенный протокол внутренней маршрутизации между шлюзами (Enhanced Interior Gateway Routing Protocol)
EPO	Экстренное выключение питания (Emergency Power Off)
ERP	Планирование ресурсов предприятия (Enterprise Resource Planning)
ESD	Электростатический разряд (Electrostatic Discharge)
ETR	Оценка продолжительности восстановления (Estimated Time to Repair)
ETSI	Европейский институт телекоммуникационных стандартов (European Telecommunication Standards Institute)
EU	Евросоюз (European Union)
FAA	Федеральное управление гражданской авиации США (Federal Aviation Administration)
FAQ	Часто задаваемый вопрос (Frequently Asked Question)
FC	Стандарт ANSI на передачу данных (Fibre Channel)
FC-AL	Высокоскоростная последовательная шина (Fibre Channel-Arbitrated Loop)
FCC	Федеральная комиссия связи США (Federal Communications Commission)

FDDI	Распределенный интерфейс передачи данных по оптоволоконным каналам (Fiber-Distributed Data Interface)
FTP	Протокол передачи файлов (File Transfer Protocol)
GUI	Графический интерфейс пользователя (Graphical User Interface)
HBA	Адаптер главной шины (Host Bus Adapter)
HHA	Портативное устройство аутентификации (Handheld Authenticator)
HTML	Язык гипертекстовой разметки (HyperText Markup Language)
HTTP	Протокол передачи гипертекста (HyperText Transfer Protocol)
HVAC	Система отопления, вентиляции и кондиционирования воздуха (Heating, Ventilation, Air Conditioning)
ICS	Система управления в чрезвычайной ситуации (Incident Command System)
I/O	Ввод/вывод (Input/Output)
ICMP	Протокол управляющих сообщений в Интернете (Internet Control Message Protocol)
IDF	Промежуточный распределительный щит (Intermediate Distribution Frame)
IDS	Система обнаружения вторжений (Intrusion Detection System)
IEEE	Институт инженеров по электротехнике и радиоэлектронике (Institute of Electrical and Electronic Engineers)
IETF	Рабочая группа по стандартам Интернета (Internet Engineering Task Force)
IMAP	Протокол доступа к сообщениям в Интернете (Internet Message Access Protocol)
IP	Интеллектуальная собственность (Intellectual Property)
IP	Интернет-протокол (Internet Protocol)
IS	Информационные системы (Information Systems)
ISDN	Цифровая сеть с интеграцией услуг (Integrated Service Digital Network)
ISO	Международная организация по стандартизации (International Organization for Standardization)
ISP	Интернет-провайдер (Internet Service Provider)
IT	Информационные технологии (Information Technology)
ITIL	Библиотека инфраструктуры информационных технологий (Information Technology Infrastructure Library)
KVM	Клавиатура, дисплей, мышь (Keyboard, Video, Mouse)
LAN	Локальная вычислительная сеть (Local Area Network)
LDAP	Облегченный протокол доступа к каталогам (Lightweight Directory Access Protocol)
LOPSA	Союз профессиональных системных администраторов (League of Professional System Administrators)

LPDP	Протокол демона линейного принтера (Line Printer Daemon Protocol)
LISA	Системное администрирование крупных систем (Large Installation System Administration)
MAC	Управление доступом к среде (Media Access Control)
MAN	Городская сеть (Metropolitan Area Network)
MAPI	API приложений электронной почты, распространяется под лицензией производителя, не путать с IMAP
MDA	Агент доставки электронной почты (Mail-Delivery Agent)
MDF	Основной распределительный щит (Main Distribution Frame)
MIB	Информационная база управления (Management Information Base)
MIDI	Цифровой интерфейс музыкальных инструментов (Musical Instrument Digital Interface)
MIL-SPEC	Военные стандарты (U.S. Military Specifications)
MIS	Информационные системы управления (Management Information Systems)
MONET	Оптическая сеть, поддерживающая несколько длин волн (Multiwavelength Optical Network)
MPEG	Экспертная группа по вопросам движущегося изображения (Moving Picture Experts Group)
MPLS	Мультипротокольная коммутация по меткам (Multi Protocol Label Switching)
MRTG	Устройство учета трафика по нескольким маршрутизаторам (Multirouter Traffic Grapher)
MS-SMS	Служба управления системой от Майкрософт (Microsoft's System Management Service)
MTA	Агент передачи электронной почты (Mail Transport Agent)
MTU	Максимальный размер пакета (Maximum Transmission Unit)
MTTR	Среднее время восстановления (Mean Time to Repair)
MUA	Пользовательский почтовый агент (Mail User Agent)
MX	Обмен почтой (Mail Exchanger)
NAS	Сетевое устройство хранения данных (Network-Attached Storage)
NAT	Преобразование сетевых адресов (Network Address Translation)
NCD	Сетевые вычислительные устройства (Network Computing Devices)
NDA	Соглашение о неразглашении (Non-Disclosure Agreement)
NEBS	Система построения сетевого оборудования (Network Equipment Building System)
NFS	Сетевая файловая система (Network File System)
NIC	Сетевой адаптер (PC-совместимая Ethernet сетевая карта) (Network Interface Card (PC Ethernet network card))
NIS	Сетевая информационная служба (Network Information Service)

NNTP	Сетевой протокол передачи новостей (Net News Transfer Protocol)
NOC	Центр управления сетью (Network Operations Center)
OEM	Производитель оригинального оборудования (Original Equipment Manufacturer)
OLTP	Средства оперативной обработки транзакций (Online Transaction Processing)
OPS	Операций в секунду (Operations Per Second)
OS	Операционная система (Operating System)
OSHA	Закон о технике безопасности и гигиене труда (Occupational Safety and Health Administration)
OSI	Модель взаимодействия открытых систем (Open Systems Interconnection)
OSPF	Открытый протокол предпочтения кратчайшего пути (Open Shortest Path First)
OTP	Одноразовый пароль (One-Time Password)
PAM	Подключаемый модуль аутентификации (Pluggable Authentication Module)
PARIS	Программируемая служба автоматической удаленной установки (Programmable Automatic Remote Installation Service)
PC	Персональный компьютер (Personal Computer)
PCMIA	Люди не могут запомнить промышленные сокращения (People Can't Memorize Industry Acronyms)
PDA	Карманный персональный компьютер (Personal Digital Assistant)
PDU	Распределительный щит питания (Power-Distribution Unit)
PIN	Персональный идентификационный номер (Personal Identification Number)
POP	Почтовый протокол (Post Office Protocol)
POPI	Защита конфиденциальной информации (Protection of Proprietary Information)
POP3	Почтовый протокол, версия 3 (Post Office Protocol, version 3)
PPP	Протокол соединения точка–точка (Point-to-Point Protocol)
PR	Связи с общественностью (Public Relations)
QA	Контроль качества (Quality Assurance)
QPS	Запросов в секунду (Queries Per Second)
QoS	Качество обслуживания (Quality of Service)
RADIUS	Служба удаленной аутентификации звонящего (Remote Authentication Dial-In User Service)
RAID	Избыточный массив недорогих жестких дисков (Redundant Array of Inexpensive Disks)
RAM	Оперативная память (Random Access Memory)
RAS	Сервер с удаленным доступом (Remote Access Server)
RCS	Система управления версиями (Revision Control System)

RF	Радиочастота (Radio Frequency)
RFC	Документ, описывающий набор сетевых протоколов (Request for Comments)
RIP	Протокол информации о маршрутизации (Routing Information Protocol)
RMA	Возврат (некачественных или неисправных изделий) производителю (Returned Merchandise Authorization)
ROI	Окупаемость инвестиций (Return on Investment)
RPC	Удаленный вызов процедур (Remote Procedure Call)
RTT	Время двойного оборота (Round-Trip Time)
RSS	Очень простое приобретение информации, формат (Really Simple Syndication)
SA	Системный администратор (System Administrator)
SAGE	Гильдия системных администраторов (System Administrator's Guild)
SAN	Сеть хранения данных (Storage-Area Network)
SANS	Системное администрирование, сеть и безопасность (System Administration, Network, and Security)
SAS-70	Положение о стандартах аудита № 70 (Statement of Auditing Standards, № 70)
SATA	Последовательный интерфейс ATA (Serial ATA)
SCCS	Система управления исходным кодом (Source Code Control System)
SCSI	Интерфейс малых компьютерных систем (Small Computer Systems Interface)
SCM	Управление конфигурацией программного обеспечения (Software Configuration Management)
SEC	Комиссия по торговле ценными бумагами США (Securities and Exchange Commission)
SID	Идентификатор безопасности (Security ID)
SLA	Соглашение об уровне обслуживания (Service-Level Agreement)
SMB	Блок сообщений сервера, формат сетевых сообщений (Server Message Block)
SME	Специалист в конкретной области (Subject Matter Expert)
SMTP	Простой протокол передачи электронной почты (Simple Mail Transfer Protocol)
SNMP	Простой протокол управления сетью (Simple Network Management Protocol)
SOA	Запись о сервере, хранящем эталонную информацию о домене в DNS (Start of Authority)
SONET	Синхронная оптическая сеть (Synchronous Optical Network)
SQL	Язык структурированных запросов (Structured Query Language)
SSH	Безопасный командный процессор (Secure Shell)

SSL	Уровень защищенных сокетов (Secure Sockets Layer)
STP	Протокол связующего дерева (Spanning Tree Protocol)
SUID	Задать идентификатор пользователя (Set User ID)
TCP	Протокол управления передачей (Transmission Control Protocol)
TDD	Разработка через тестирование (Test-Driven Development)
TFTP	Простой протокол передачи данных (Trivial File Transfer Protocol)
TLS	Безопасность на транспортном уровне, сетевой протокол (Transport Layer Security)
TTL	Время жизни (Time to Live)
UCE	Нежелательная коммерческая электронная почта, спам (Unsolicited Commercial Email)
UDP	Протокол пользовательских датаграмм (User Datagram Protocol)
UID	Идентификатор пользователя (User Identificator)
UPS	Источник бесперебойного питания (Uninterruptible Power Supply)
USB	Универсальная последовательная шина (Universal Serial Bus)
URL	Унифицированный указатель ресурса (Uniform Resource Locator)
UUCP	Протокол обмена файлами в сети машин UNIX (UNIX-to-UNIX Copy Protocol)
VIF	Виртуальный интерфейс (Virtual Interface)
VLAN	Виртуальная локальная сеть (Virtual LAN)
VPN	Виртуальная частная сеть (Virtual Private Network)
VRRP	Протокол избыточной виртуальной маршрутизации (Virtual Router Redundancy Protocol)
WAN	Глобальная сеть (Wide Area Network)
WAFL	Файловая система «с записью повсюду» (Write Anywhere File Layout)

Список литературы

Adams, S. 2000. *The Dilbert Principle*. Boxtree. *www.Dilbert.com*.

Albitz, P., C. Liu and M. Loukides, eds. 1998. DNS and BIND. O'Reilly.

Allen, D. 2002. *Getting Things Done: The Art of Stress-Free Productivity*. Penguin.

Allen, J. R. 1999. Driving by the rear-view mirror: Managing a network with cricket. *First Conference on Network Administration (NETA'99)*, USENIX, Santa Clara, Calif., pp. 1–10.

Anonymous. 1997. The backhoe, natural enemy of the network administrator. *www.23.com/backhoe/*.

Archer, B. 1993. Towards a POSIX standard for software administration. *Systems Administration (LISA VII) Conference*, USENIX, Monterey, Calif., pp. 67–79.

Beck, R. 1999. Dealing with public Ethernet jacks – switches, gateways and authentication. *Proceedings of the 13th Systems Administration Conference LISA (SAGE/USENIX)*, p. 149.

Bent, Jr., W. H. 1993. System administration as a user interface: An extended metaphor. *Systems Administration (LISA VII) Conference*, USENIX, Monterey, Calif., pp. 209–212.

Bentley, J. and B. Kernigan. 1991. A system for algorithm animation. *Computing Systems*, Vol. 4, USENIX, pp. 5–30.

Berkowitz, H. C. 1998. Designing Addressing Architectures for Routing and Switching. Macmillan Technical Publishing. ISBN: 1578700590.

Berkowitz, H. C. 1999. *Designing Routing and Switching Architectures*. Macmillan Technical Publishing. ISBN: 1578700604.

Berliner, B. 1990. CVS II: Parallelizing software development. *USENIX Conference Proceedings*, USENIX, Washington, D. C., pp. 341–352.

Bernstein, D. J. 1997. VERP: Variable envelope return paths. *http://cr.yp.to/proto/verp.txt*.

Black, D. P. 1999. *Building Switched Networks: Multilayer Switching, QoS, IP Multicast, Network Policy, and Service-Level Agreements*. Addison-Wesley.

Black, U. D. 2000. *IP Routing Protocols: RIP, OSPF, BGP, PNNI and Cisco Routing Protocols. Prentice Hall*. ISBN: 0130142484.

Black, U. D. 2001. *MPLS and Label Switching Networks*. Prentice Hall.

Blanchard, K. H. 1993. *The One Minute Manager*. Berkley Pub Group.

Blanchard, K. H., W. Oncken and H. Burrows. 1989. *The One Minute Manager Meets the Monkey*. Morrow.

Bolinger, D. 1995. *Applying RCS and SCCS*. O'Reilly.

Braden, R. T. 1989. RFC 1123: Requirements for Internet hosts – application and support. See also STD0003. Updates RFC 822 (Crocker 1982). Updated by RFC 2181 (Elz and Bush 1997). Status: Standard.

Brutlag, J. D. 2000. Aberrant behavior detection in time series for network monitoring. *Fourteenth Systems Administration Conference (LISA'00)*, USENIX, New Orleans.

Burgess, M. 2000. *Principles of Network and System Administration*. Wiley.

Burns, D. D. 1999a. *The Feeling Good Handbook*. Avon.

Burns, D. D. 1999b. *Feeling Good: The New Mood Therapy*. Avon.

Chalup, S. R. et al. 1998. Drinking from the fire(walls) hose: Another approach to very large mailing lists. *Twelfth Systems Administration Conference (LISA'98)*, USENIX, Boston, p. 317.

Chapman, D. B. 1992. Majordomo: How I manage 17 mailing lists without answering"-request" mail. *Systems Administration (LISA VI) Conference*, USENIX, Long Beach, Calif., pp. 135–143.

Chapman, R. B. and K. R. Andrade. 1997. *Insourcing After the Outsourcing: MIS Survival Guide*. AMACOM. ISBN: 0814403867.

Cheswick, W. R. and S. M. Bellovin. 1994. *Firewalls and Internet Security: Repelling theWily Hacker*. Addison-Wesley.

Colyer, W. and W. Wong. 1992. Depot: A tool for managing software environments. *Systems Administration (LISA VI) Conference*, USENIX, Long Beach, Calif., pp. 153–162.

Comer, D. 2005. *Internetworking with TCP/IP*, Vol. 1. Prentice Hall.

Cox P. and T. Sheldon. 2000. *Windows 2000 Security Handbook*. McGraw-Hill Professional Publishing. ISBN: 0072124334.

Crispin, M. 1996. RFC 2060: Internet message access protocol – Version 4, rev. 1. Obsoletes RFC1730. Status: Proposed standard.

Crittenden, J. 1995. The Simpsons: [episode 2F10] And Maggie Makes Three, TV episode. *www.snpp.com/episodes/2F10.html*.

Crocker, D. 1982. RFC 822: Standard for the format of ARPA Internet text messages. See also STD0011. Obsoletes RFC 733. Updated by RFC 1123 (Braden 1989), RFC 1138, RFC 1148, RFC 1327, RFC 2156. Status: Standard.

Curtin, M. 1999a. Electronic snake oil. Vol. 24, USENIX, pp. 31–38.

Curtin, M. 1999b. Snake Oil Warning Signs: Encryption Software to Avoid. *http://www.interhack.net/people/cmcurtin/snake-oil-faq.html*.

Dagenais, M. et al. 1993. LUDE: A distributed software library. *Systems Administration (LISA VII) Conference*, USENIX, Monterey, Calif., pp. 25–32.

Darmohray, E. T., ed. 2001. *Job Descriptions for System Administrators*, rev. and expanded ed. USENIX for/SAGE. *www.sage.org/pubs/8 jobs*.

Davis, C. P. et al. 1996. RFC 1876: A means for expressing location information in the domain name system. Updates RFC 1034, RFC 1035. Status: Experimental.

Denning, D. E. 1999. *Information Warfare and Security*. Addison-Wesley. ISBN: 0201433036.

Dijker, B. L. 2000. Sage computing policies website. *http://www.usenix.org/sage/publications/policies*.

Dodge, J. 1999. Maybe Ascend should have bought Lucent. *ZDNet eWeek*. *www.zdnet.com/eweek/stories/general/0,11011,385015,00.html*.

Elz, R. and R. Bush. 1996. RFC 1982: Serial number arithmetic. Updates RFC 1034, RFC 1035. Status: Proposed standard.

Elz, R. and R. Bush. 1997. RFC 2181: Clarifications to the DNS specification. Updates RFC 1034, RFC 1035, RFC 1123. Status: Proposed standard.

Epp, P. V. and B. Baines. 1992. Dropping the mainframe without crushing the users: Mainframe to distributed UNIX in nine months. *Systems Administration (LISA VI) Conference*, USENIX, Long Beach, Calif., pp. 39–53.

Epps, A., D. G. Bailey and D. Glatz. 1999. NFS and SMB data sharing within a heterogeneous environment: A real world study. *2nd Large Installation System Administration of Windows NT Conference*, USENIX, Seattle, Washington, pp. 37–42.

Evard, R. 1997. An analysis of UNIX system configuration. *Eleventh Systems Administration Conference (LISA '97)*, USENIX, San Diego, p. 179.

Feit, S. 1999. *Wide Area High Speed Networks*. Pearson Education. ISBN: 1578701147.

Fine, T. A. and S. M. Romig. 1990. A console server. *LISA IV Conference Proceedings*, USENIX, Colorado Springs, CO, pp. 97–100.

Finke, J. 1994a. Automating printing configuration. *LISA VIII Conference Proceedings*, USENIX, San Diego, CA, pp. 175–183.

Finke, J. 1994b. Monitoring usage of workstations with a relational database. *LISA VIII Conference Proceedings*, USENIX, San Diego, CA, pp. 149–157.

Finke, J. 1995. Sql 2 html: Automatic generation of HTML database schemas. *Ninth Systems Administration Conference (LISA '95)*, USENIX, Monterey, CA, pp. 133–138.

Finke, J. 1996. Institute white pages as a system administration problem. *10th Systems Administration Conference (LISA'96)*, USENIX, Chicago, IL, pp. 233–240.

Finke, J. 1997. Automation of site configuration management. *Eleventh Systems Administration Conference (LISA '97)*, USENIX, San Diego, California, p. 155.

Finke, J. 2000. An improved approach for generating configuration files from a database. *Proceedings of the 14th Systems Administration Conference LISA (SAGE/USENIX)*, p. 29.

Fulmer, K. L. 2000. *Business Continuity Planning: A Step-by-Step Guide with Planning Forms*. Rothstein Associates.

Fulmer, R. and A. Levine. 1998. Autoinstall for NT: Complete NT installation over the network. *Large Installation System Administration of Windows NT Conference*, USENIX, Seattle, p. 27.

Furlani, J. L. and P. W. Osel. 1996. Abstract yourself with modules. *Tenth Systems Administration Conference (LISA' 96)*, USENIX, Chicago, pp. 193–203.

Garfinkel, S. 1994. *PGP: Pretty Good Privacy*. O'Reilly. ISBN: 1565920988.

Garfinkel, S. and G. Spafford. 1996. *Practical UNIX and Internet Security*. O'Reilly and Associates, Inc. ISBN: 1565921488.

Gay, C. L. and J. Essinger. 2000. *Inside Outsourcing*. Nicholas Brealey. ISBN: 1857882040.

Glickstein, B. 1996. GNU stow. *www.gnu.org/software/stow/stow.html*.

Group Staff Outsource 1996. Outsourcing. South-Western Publishing Company. ISBN: 0538847514.

Guichard, J. and I. Pepelnjak. 2000. *MPLS and VPM Architectures: A Practical Guide to Understanding, Designing and Deploying MPLS and MPLS-Enabled VPNs.* Cisco Press.

Guth, R. and L. Radosevich. 1998. IBM crosses the Olympic finish line. *InfoWorld. http://archive.infoworld.com/cgi-bin/displayArchive.pl?/98/06/e01-06.79.htm.*

Halabi, S. and D. McPherson. 2000. *Internet Routing Architectures. Cisco Press.* ISBN: 157870233X.

Harlander, D. M. 1994. Central system administration in a heterogeneous unix environment: Genuadmin. *LISA VIII Conference Proceedings*, USENIX, San Diego, CA, pp. 1–8.

Harris, D. and B. Stansell. 2000. Finding time to do it all. *USENIX. www.conserver.com/consoles/.*

Heiss, J. 1999. Enterprise rollouts with jumpstart. *Thirteenth Systems Administration Conference (LISA '99)*, USENIX, Seattle.

Hemmerich, C. 2000. Automating request-based software distribution. *Fourteenth Systems Administration Conference (LISA '00)*, USENIX, New Orleans.

Hogan, C. Formula 1 Racing: "Science in the fast lane". *Nature* 481 (Oct. 14, 2000: *http://EverythingSysadmin.com/p/a*).

Horowitz, M. and S. Lunt. 1997. RFC 2228: FTP security extensions. Updates RFC 959 (Postel and Reynolds 1985). Status: Proposed standard.

Houle, B. 1996. Majorcool: A web interface to majordomo. *Tenth Systems Administration Conference (LISA '96)*, USENIX, Chicago, pp. 145–153.

Hume, A. 1988. The file motel – an incremental backup system for unix. *USENIX Conference Proceedings*, USENIX, San Francisco, pp. 61–72.

Hunter, T. and S. Watanabe. 1993. Guerrilla system administration: Scaling small group systems administration to a larger installed base. *Systems Administration (LISA VII) Conference*, USENIX, Monterey, Calif., pp. 99–105.

Jennings, R. W. and J. Passaro. 1999. *Make It Big in the $100 Billion Outsource Contracting Industry*. Westfield Press. ISBN: 096543110X.

Johnson, S. 1991. *The One Minute Sales Person*. Avon Books. ISBN: 0380716038.

Kantor, B. and P. Lapsley. 1986. RFC 977: Network news transfer protocol: A proposed standard for the stream-based transmission of news. Status: Proposed standard.

Katcher, J. 1999. NetApp Tech Report 3070: Scalable infrastructure for Internet business. *www.netapp.com/tech library/3070.html.*

Keagy, S. 2000. *Integrating Voice and Data Networks*. Cisco Press.

Kercheval, B. 1999. *DHCP: A Guide to Dynamic TCP/IP Network Configuration*. Prentice Hall.

Kernighan, B. W. and R. Pike. 1999. *The Practice of Programming.* Addison-Wesley. ISBN: 020161586X.

Knight, S. et al. 1998. RFC 2338: Virtual router redundancy protocol. Status: Proposed standard.

Koren, L. and P. Goodman. 1992. *The Haggler's Handbook: One Hour to Negotiating Power*. Norton.

Kovacich, G. 1998. *The Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program*. Butterworth-Heinenmann. ISBN: 0750698969.

Kubicki, C. 1992. Customer satisfaction metrics and measurement. *Systems Administration (LISA VI) Conference*, USENIX, Long Beach, Calif., pp. 63–68.

Kubicki, C. 1993. The system administration maturity model – SAMM. *Systems Administration (LISA VII) Conference*, USENIX, Monterey, Calif., pp. 213–225.

Kuong, J. F. 2000. *Application Service Provisioning*. Management Advisory Publications. ISBN: 0940706490.

Lakein, A. 1996. *How to Get Control of Your Time and Your Life*. New American Library.

Lear, E. et al. 1994. RFC 1627: Network 10 considered harmful (some practices shouldn't be codified). Obsoleted by BCP0005, RFC1918 Rekhter et al. 1996. Status: Informational.

Leber, J. 1998. *Windows NT Backup and Restore*. O'Reilly.

Lee, D. C. 1999. *Enhanced IP Services for Cisco Networks: A Practical Resource for Deploying Quality of Service, Security, IP Routing, and VPN Services*. Cisco Press.

Lemon, T. and R. E. Droms. 1999. *The DHCP Handbook: Understanding, Deploying, and Managing Automated Configuration Services*. MacMillan.

Levitt, A. M. 1997. *Disaster Planning and Recovery: A Guide for Facilities Professionals*. Wiley.

Levy, E. (n. d.). *Bugtraq.www.securityfocus.com/frames/?content=/forums/bugtraq/intro.html*.

Libes, D. 1990. RFC 1178: Choosing a name for your computer. See also FYI0005. Status: Informational.

Limoncelli, T. A. 1998. Please quit. *USENIX*, p. 38.

Limoncelli, T. A. 1999. Deconstructing user requests and the nine step model. *Proceedings of the 13th Systems Administration Conference LISA (SAGE/USENIX)*, p. 35.

Limoncelli, T. A. 2005. Time Management for System Administrators. O'Reilly.

Limoncelli, T. A. and C. Hogan. 2001. The Practice of System and Network Administration. Addison-Wesley.

Limoncelli, T. et al. 1997. Creating a network for Lucent Bell Labs Research South. *Eleventh Systems Administration Conference (LISA '97)*, USENIX, San Diego, p. 123.

Limoncelli, T. A. et al. 1998. Providing reliable NT desktop services by avoiding NT server. *Large Installation System Administration of Windows NT Conference*, USENIX, Seattle, p. 75.

Lions, J. 1996. *Lion's Commentary on UNIX 6th Edition, with Source Code*. Peer-to-Peer Communications. ISBN: 1-57398-013-7.

Liu, C. 2001. The ties that BIND: Using BIND name servers with Windows 2000. *Linux Magazine*. *www.linux-mag.com/2001-03/toc.html*.

Locke, C. et al. 2000. *The Cluetrain Manifesto : The End of Business as Usual*. Perseus Press.

MacKenzie, R. A. 1997. *The Time Trap*. AMACOM.

Maggiora, P. L. D. et al. 2000. *Performance and Fault Management*. Cisco Press.

Maniago, P. 1987. Consulting via mail at andrew. *Large Installation System Administrators Workshop Proceedings*, USENIX, Philadelphia, pp. 22–23.

Marcus, J. S. 1999. *Designing Wide Area Networks and Internetworks: A Practical Guide*. Addison-Wesley. ISBN: 0201695847.

Mathis, M. 2003. The case of raising the Internet MTU. *Cisco200307. http://www.psc.edu/mathis/MTU/index.html*.

Mauro, J. and R. McDougall. 2000. *Solaris Internals: Core Kernel Architecture*. Prentice Hall PTR/Sun Microsystems Press. ISBN: 0130224960.

McKusick, M. K. et al. 1996. *The Design and Implementation of the 4.4BSD Operating System*. Addison-Wesley. ISBN: 0201549794.

McLaughlin III, L. 1990. RFC 1179: Line printer daemon protocol. Status: Informational.

McNutt, D. 1993. Role-based system administration or who, what, where, and how. *Systems Administration (LISA VII) Conference*, USENIX, Monterey, Calif., pp. 107–112.

Menter, E. S. 1993. Managing the mission critical environment. *Systems Administration (LISA VII) Conference*, USENIX, Monterey, Calif., pp. 81–86.

Miller, A. and A. Donnini. 2000. Relieving the burden of system administration support through support automation. *Fourteenth Systems Administration Conference (LISA '00)*, USENIX, New Orleans.

Miller, A. R. and M. H. Davis. 2000. *Intellectual Property, Patents, Trademarks and Copyright in a Nutshell*. West/Wadsworth. ISBN: 0314235191.

Miller, M. and J. Morris. 1996. Centralized administration of distributed firewalls. *Tenth Systems Administration Conference (LISA'96)*, USENIX, Chicago, IL, pp. 19–23.

Moran, J. and B. Lyon. 1993. The restore-o-mounter: The file motel revisited. *USENIX Conference Proceedings*, USENIX, Cincinnati, pp. 45–58.

Morgenstern, J. 1998. O*rganizing from the Inside Out: The Foolproof System for Organizing Your Home, Your Office and Your Life*. Owl Books.

Moy, J. T. 2000. OSPF: *Anatomy of an Internet Routing Protocol*. Addison-Wesley.

Myers, J. and M. Rose, 1996. RFC 1939: Post Office Protocol – version 3. See also STD 0053. Obsoletes RFC 1725. Updated by RFC 1957, RFC 2449. Status: Standard.

Mylott, T. R., III. 1995. *Computer Outsourcing : Managing the Transfer of Information Systems*. Prentice Hall. ISBN: 013127614X.

Nelson, B. 2005. 1001 *Ways to Reward Employees*. 2d ed. Workman.

Neumann, P. 1997. *Computer-Related Risks*. Addison-Wesley. ISBN: 020155805X.

Niksic, H. 1998. GNU wget. *www.gnu.org/software/wget/wget.html*.

Norberg, S. and D. Russell. 2000. *Securing Windows NT/2000 Servers for the Internet: a Checklist for System Administrators*. O'Reilly. ISBN: 1565927680.

Northcutt, S. 1999. *G4.1 – Computer Security Incident Handling: Step-by-Step*. SANS Institute.

Oetiker, T. 1998a. MRTG – the multi router traffic grapher. *Twelfth Systems Administration Conference (LISA '98)*, USENIX, Boston, p. 141.

Oetiker, T. 1998b. SEPP – software installation and sharing system. *Twelfth Systems Administration Conference (LISA '98)*, USENIX, Boston, p. 253.

Ondishko, D. 1989. Administration of department machines by a central group. *USENIX Conference Proceedings*, USENIX, Baltimore, MD, pp. 73–82.

Osterman, M. 2000. The Impact of Effective Storage Technology on Exchange TCO. *http://www.cnilive.com/docs pub/html/stor00.html*.

Oppliger, R. 2000. *Secure Messaging with PGP and S/MIME*. Artech House. ISBN: 158053161X.

Peacock, D. and M. Giuffrida. 1988. Big brother: A network services expert. *USENIX Conference Proceedings*, USENIX, San Francisco, pp. 393–398.

Pepelnjak, I. 2000. *EIGRP Network Design Solutions*. Cisco Press.

Perlman, R. 1999. *Interconnections, Second Edition: Bridges, Routers, Switches, and Internetworking Protocols*. Addison-Wesley. ISBN: 0201634481.

Phillips, G. and W. LeFebvre. 1998. *Hiring System Administrators*. USENIX for SAGE, the System Administrator's Guild, Short Topics in System Administration #5.

Pildush, G. D. 2000. *Cisco ATM Solution: Master ATM Implementation of Cisco Networks*. Cisco Press.

Postel, J. and J. K. Reynolds. 1985. RFC 959: File transfer protocol. Obsoletes RFC 0765. Updated by RFC 2228 (Horowitz and Lunt 1997). Status: Standard.

Powell, P. and J. Mason. 1995. Lprng – an enhanced printer spooler system. *Ninth Systems Administration Conference (LISA '95)*, USENIX, Monterey, Calif., pp. 13–24.

Powers, D. P. and D. Russell. 1993. *Love Your Job!*. O'Reilly.

Preston, W. C. 1999. *UNIX Backup and Recovery*. O'Reilly.

Rekhter, Y. et al. 1994. RFC 1597: Address allocation for private internets. Obsoleted by BCP0005, RFC1918 Rekhter et al. 1996. Status: Informational.

Ressman, D. and J. Valdés. 2000. Use of cfengine for automated multi-platform software and patch distribution. *Fourteenth Systems Administration Conference (LISA '00)*, USENIX, New Orleans.

Ringel, M. F. and T. A. Limoncelli. 1999. Adverse termination procedures or how to fire a system administrator. *Proceedings of the 13th Systems Administration Conference LISA (SAGE/USENIX)*, p. 45.

Rothery, B. and I. Robertson. 1995. *The Truth About Outsourcing*. Ashgate Publishing Company. ISBN: 0566075156.

Schafer, P. 1992a. bbn-public – contributions from the user community. *Systems Administration (LISA VI) Conference*, USENIX, Long Beach, Calif., pp. 211–213.

Schafer, P. 1992b. Is centralized system administration the answer?. *Systems Administration (LISA VI) Conference*, USENIX, Long Beach, Calif., pp. 55–61.

Schreider, T. 1998. *Encyclopedia of Disaster Recovery, Security & Risk Management*. Crucible Publishing Works.

Schwartz, K. L., L. Cottrell and M. Dart. 1994. Adventures in the evolution of a highbandwidth network for central servers. *Eighth Systems Administration Conference (LISA VIII)*, USENIX, San Diego, California.

Shapiro, G. N. and E. Allman, 1999. Sendmail evolution: 8.10 and beyond. *FREENIX Track: 1999 USENIX Annual Technical Conference*, USENIX, Monterey, Calif., pp. 149–158.

Small, F. 1993. Everything possible. In particular, the title song.

Smallwood, K. 1992. SAGE views: Whither the customer?. *USENIX*, pp. 15–16.

Snyder, G. et al. 1986. sudo. *www.courtesan.com/sudo*.

SPIE. 2002. Optical security and counterfeit deterrence techniques IV. *Proceeding of SPIE*, Vol. 4677. *http://everythingsysadmin.com/p/h*.

Spurgeon, C. E. 2000. *Ethernet: The Definitive Guide*. O'Reilly. ISBN: 1565926609.

Stern, H. 1991. *Managing NFS and NIS*. O'Reilly.

Stevens, W. R. 1994. *TCP/IP Illustrated, Volume 1: The Protocols*. Addison-Wesley.

Stewart, J. W. 1999. B*GP4 Inter-Domain Routing in the Internet*. Addison-Wesley.

Stoll, C. 1989. *The Cuckoo's Egg*. Doubleday.

Thomas, T. M. 1998. *OSPF Network Design Solutions*. Cisco Press.

Valian, P. and T. K. Watson. 1999. NetReg: An automated DHCP registration system. *Thirteenth Systems Administration Conference (LISA '99)*, USENIX, Seattle.

van den Berg, S. R. 1990. procmail. *www.procmail.org*.

Vegesna, S. 2001. *IP Quality of Service*. Cisco Press.

Viega, J., B. Warsaw and K. Manheimer. 1998. Mailman: The GNU mailing list manager. *Twelfth Systems Administration Conference (LISA '98)*, USENIX, Boston, p. 309.

Williams, O. D. 1998. *Outsourcing: A CIO's Perspective. CRC Press St*. Lucie Press. ISBN: 1574442163.

Williamson, B. 2000. *Developing IP Multicast Networks: The Definitive Guide to Designing and Deploying Cisco IP Multicast Networks*. Cisco Press. ISBN: 1578700779.

Wood, C. C. 1999. *Information Security Policies Made Easy*. Baseline Software. ISBN: 1881585069.

Yeong, W., T. Howes and S. Kille. 1995. RFC 1777: Lightweight directory access protocol. Obsoletes RFC 1487. Status: Draft standard.

Zwicky, E. D., S. Simmons and R. Dalton. 1990. Policy as a system administration tool. *LISA IV Conference Proceedings*, USENIX, Colorado Springs, pp. 115–124.

Алфавитный указатель

Б

В

Г

Д

Е

Ж

З

И

К

Л

M

Н

О

П

Р

С

Т

У

Ф

Х

Ц

Ч

Ш

Э

Ю

Я