

Александр Кенин

**САМОУЧИТЕЛЬ
СИСТЕМНОГО
АДМИНИСТРАТОРА**
3-е издание

Санкт-Петербург

«БХВ-Петербург»

2012

УДК 681.3.06
ББК 32.973.26-018.2
К35

Кенин А. М.

К35 Самоучитель системного администратора. — 3-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2012. — 512 с.: ил. — (Системный администратор)
ISBN 978-5-9775-0764-6

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

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

Для начинающих системных администраторов

УДК 681.3.06
ББК 32.973.26-018.2

Группа подготовки издания:

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

Подписано в печать 30.03.12.
Формат 70×100^{1/16}. Печать офсетная. Усл. печ. л. 41,28.
Тираж 2000 экз. Заказ №
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

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

Оглавление

Предисловие	1
Глава 1. Системное администрирование	3
Системный администратор	3
Регламент работы.....	4
Выбор операционной системы	5
Стоимость владения.....	6
Открытые стандарты.....	7
Конкурсы	7
Переход на новые версии программного обеспечения.....	8
Сертификация системных администраторов	8
Немного этики.....	9
О мистике	10
Глава 2. Выбор оборудования и программного обеспечения	11
Требования к оборудованию информационных систем	11
Выбор вендора	11
Сервисные контракты.....	12
Запасные элементы	12
Дополнительные требования к компьютерам.....	12
Выбор процессора.....	12
Выбор шасси	12
Выбор материнской платы	13
Выбор дисков	14
Выбор памяти	15
Совместимость компонентов	16
Дополнительные требования к коммутационному оборудованию.....	17
Дополнительные требования к аварийным источникам питания	18
Состав программного обеспечения типовой организации	18
Службы разрешения имен	19
Система авторизации, аутентификации и контроля доступа.....	19
Подключение Linux к домену (Kerberos)	19
Сервер Linux в качестве контроллера домена	22

Совместные документарные ресурсы	23
Учетная запись для анонимного доступа	23
Портальные решения	24
Поиск по сетевым ресурсам	24
Работа с Windows-ресурсами в Linux	25
Обозреватели Интернета	27
Защита хоста	28
Средства резервного копирования	29
Электронный офис	32
Электронная почта	34
Свободное программное обеспечение	37
Базовые сведения о работе в *nix-системах	39
Linux-мифы	39
Безопасность в Linux и Windows	40
Несколько моментов, о которых следует знать пользователям Linux	41
Структура папок Linux	43
Текстовый редактор vi	44
Выполнение команд с правами другого пользователя	45
Прикладные программы в Linux	46
Кроссплатформенный запуск программ	47
Установка Linux	47
Многовариантная загрузка	48
Тестирование Linux на виртуальной машине	48
Глава 3. Структура сети	49
Структурированные кабельные сети	49
Категории СКС	49
Волоконно-оптические сети	50
Сети 10G	51
Схема разъема RJ-45	52
Варианты исполнения СКС	53
Внимание: патч-корды	54
Составные линии	54
Прокладка силовых кабелей	54
Питание по сети Ethernet	55
Требования пожарной безопасности	56
Топология сети	56
Размеры сегментов сети на витой паре	56
Типовая структура сети предприятия	57
Уровни ядра, распределения и доступа	58
Топология каналов сети распределенного предприятия	59
Сеть управления	60
Документирование структуры каналов связи	61
Качество сетей связи предприятия	61
Тестирование кабельной системы	61
Тестирование качества передачи данных	63
Приоритезация трафика	63
Варианты приоритезации: QoS, ToS, DiffServ	64

Классификация, маркировка, приоритезация	66
Как работает приоритезация: очереди	66
Ограничение полосы пропускания трафика (Traffic shaping)	67
Беспроводные сети.....	68
Стандарты беспроводной сети.....	68
Проектирование беспроводной сети предприятия	69
Безопасность беспроводной сети.....	71
Шифрование трафика беспроводной сети	71
Аутентификация пользователей и устройств Wi-Fi	71
Безопасность клиента	72
Настройка транспортных протоколов.....	73
Протоколы	73
Модель OSI.....	74
Стек протоколов TCP/IP.....	75
Протоколы UDP, TCP, ICMP	76
IPv6.....	76
Параметры TCP/IP-протокола.....	77
IP-адрес	77
Групповые адреса.....	77
Распределение IP-адресов сети малого офиса	78
Маска адреса	79
Шлюз (Gateway, default gateway)	80
Таблицы маршрутизации.....	80
Автоматическое присвоение параметров IP-протокола	83
Порт.....	85
Протокол ARP	86
Имена компьютеров в сети TCP/IP	87
Настройка серверов WINS, DHCP, DNS.....	92
Установка и настройка WINS	92
Настройка DHCP.....	93
DNS	98
Глава 4. Информационные системы предприятия	111
Домашние сети.....	111
Одноранговые сети	112
Сеть с централизованным управлением.....	113
Управление локальными ресурсами.....	113
Возможность добавлять рабочие станции в домен	114
Удаление устаревших записей о компьютерах и пользователях	115
Изменения настроек системы при подключении ее к домену.....	116
"Кто кого": локальный или доменный администратор	116
Проблема аудитора	119
Методы управления локальной системой.....	119
Служба каталогов.....	121
Служба каталогов Windows (Active Directory)	122
Домены Windows	123
Подразделение.....	124
Лес	124

Сайты	125
Режимы совместимости доменов и леса	125
DN, RDN	126
Управление структурой домена предприятия	126
Создание нового домена	126
Особенности создания дополнительного удаленного контроллера в домене Windows	127
Создание контроллеров домена "только для чтения"	129
Удаление контроллера домена	129
Переименование домена	130
Утилиты управления объектами службы каталогов	130
Утилиты запросов командной строки службы каталогов	130
LDAP-управление	131
Подключаемся к каталогу по протоколу LDAP	131
Синтаксис поисковых запросов LDAP	132
Команда <i>ldifde</i>	134
Делегирование прав	135
Просмотр и восстановление удаленных объектов каталога	137
Учетные записи и права	137
Понятие учетной записи	137
Локальные и доменные учетные записи	138
Группы пользователей	140
Возможные члены групп. Области применения групп	141
Ролевое управление	142
Результирующее право: разрешить или запретить?	142
Разрешения общего доступа и разрешения безопасности	143
Наследуемые разрешения: будьте внимательны	144
Восстановление доступа к ресурсам	145
Обход перекрестной проверки	146
Изменение атрибутов объектов при операциях копирования и перемещения	146
Результирующие права и утилиты	147
Рекомендации по применению разрешений	147
Создание и удаление учетных записей	148
Дополнительные параметры учетной записи	150
Права учетной записи	150
Восстановление параметров безопасности по умолчанию	150
Автоматически создаваемые учетные записи	152
Учетная запись <i>Система</i>	154
Встроенные группы	155
Специальные группы	157
Рекомендации по использованию операции <i>Запуск от имени</i>	158
Глава 5. Работа в глобальной сети	159
Организация доступа к ресурсам Интернета	159
NAT	159
Реализация NAT средствами службы маршрутизации Windows	160
Реализация NAT при совместном использовании подключения к Интернету	161

Аппаратный NAT	164
Реализация NAT средствами Linux	164
Фильтрация трафика	164
Демилитаризованная зона	164
Межсетевой экран (брандмауэр)	165
Что может межсетевой экран и чего не стоит от него ожидать?	166
Учитываемые параметры фильтрации	166
Варианты организации межсетевых экранов	167
Intrusion Prevention Systems	168
Варианты межсетевых экранов	169
Аппаратные решения	170
Встроенный межсетевой экран Windows XP/7/Server 2003/2008	170
Программные комплексы	172
Фильтрация пакетов средствами операционной системы	172
Настройка параметров меж сетевого экрана при помощи групповой политики	173
Групповые политики меж сетевого экрана	173
Межсетевой экран Linux	175
Настройки запуска	175
Использование <i>iptables</i> в Ubuntu	177
Программы графического управления <i>iptables</i>	177
Принципы работы <i>iptables</i>	179
Создание правил меж сетевого экрана	180
Оптимизация доступа в Интернет	181
Прокси-сервер	182
Автообнаружение прокси-серверов	183
"Прозрачный" прокси	184
Настройка использования полосы пропускания	185
Блокировка рекламы, порносайтов и т. п.	186
Удаленная работа	187
Удаленное подключение пользователей	188
Прием входящих подключений	188
VPN	189
Удаленное подключение к Linux	193
OpenSSH-сервер	193
Подключение SSH-клиента	194
Использование графических утилит для подключения к Linux	194
Подключения филиалов	195
Туннель между Linux-системами	195
Постоянное подключение к серверу Windows	196
В случае разрыва канала	196
Карантин клиентов удаленного подключения	197
Контроллер домена только для чтения	199
DirectAccess	200
Терминальный доступ	202
Терминальные серверы от Microsoft	202
Терминальные клиенты	202
Режимы терминальных служб	203
Лицензирование терминальных служб	204

Особенности использования приложений на терминальном сервере	204
Безопасность терминальных сессий	205
Подключение к консоли терминального сервера	206
Подключение администратора к сессии пользователя	207
Публикация приложений в терминале	207
Веб-доступ к терминальному серверу	209
Шлюз терминалов	210
Создание локальных копий данных	210
BranchCache	211
Автономные файлы	212
Варианты синхронизации автономных файлов	213
Разрешение конфликтов	214
Удаление автономных файлов	214
Настройка автономных почтовых папок	214
Перенаправление папок хранения документов	215
Доступ из-за межсетевых экранов	215
Глава 6. Управление информационной системой	217
Инвентаризация	217
Построение топологии существующей СКС	217
Инвентаризация физических каналов связи	218
Учет компьютеров и программ	219
Контроль функционирования ПО	220
Управление с помощью групповых политик	220
Групповые политики в различных версиях операционных систем	221
К чему и как применяются групповые политики	222
Где хранятся и когда применяются групповые политики	223
Последствия отключений политик	224
Чем редактировать групповую политику	225
Начальные объекты групповой политики	227
Расширенное управление групповыми политиками	227
"Обход" параметров пользователя	229
Фильтрация объектов при применении групповой политики	229
Фильтрация при помощи WMI-запросов	230
Настройка параметров безопасности групповых политик	230
Предпочтения групповых политик	230
Рекомендации по применению политик	232
Некоторые особенности политики ограниченного использования программ	233
Варианты политик ограниченного использования	233
Опции настройки применения политик ограниченного использования программ	235
Когда ограничения не действуют	236
Последовательность применения политик ограниченного использования программ	236
Некоторые рекомендации применения политик ограниченного использования программ	237
Некоторые особенности политики установки программного обеспечения	238
Административные шаблоны	239

Утилиты группового управления.....	240
Средства поддержки пользователей.....	240
"Удаленный помощник".....	240
Утилиты подключения к рабочему столу.....	242
Средства автоматизации — сценарии.....	243
Использование командной строки.....	243
Сценарии Visual Basic.....	244
Intelligent Platform Management Interface.....	246
Windows Management Interface.....	246
WMI Query Language.....	248
Варианты применения WMI.....	249
Примеры.....	250
PowerShell.....	251
Отдельные утилиты администрирования третьих фирм.....	252
Утилиты от компании Sysinternals.....	252
Средства восстановления системы.....	253
Снифферы.....	253
DameWare NT Utilities.....	254
Ideal Administrator.....	254
Huena.....	254
Автоматизация установки программного обеспечения.....	254
Развертывание Windows 7 при помощи WAIK.....	255
Клонирование систем.....	255
Подводные камни процесса клонирования.....	256
Утилита <i>sysprep</i>	257
Дублирование жесткого диска.....	259
Образы клонируемого диска и их модификация.....	260
Клонирование компьютеров-членов домена.....	260
Подготовка программ для тихой установки.....	261
Файлы ответов (трансформаций).....	261
Использование ключей тихой установки.....	263
Административная установка.....	265
Глава 7. Мониторинг информационной системы.....	267
Основные способы контроля.....	267
Журналы системы и программ.....	267
Протокол SNMP.....	268
Контроль ответов служб.....	268
Мониторинг с использованием агентов.....	268
Simple Network Management Protocol.....	269
Простейшие варианты мониторинга.....	272
Контроль журналов Windows.....	272
Привязка задачи.....	273
Подписка на события.....	274
Создание собственных событий в журналах Windows.....	276
Настройка журналирования в syslog.....	276
Утилиты мониторинга.....	276
Microsoft System Center Operation Management.....	277

Вариант построения мониторинга на SCOM.....	277
Установка SCOM	279
Операции по настройке SCOM после установки	281
Импорт пакетов управления.....	281
Добавление контролируемых систем	282
Настройка оповещений SCOM	283
Немного о структуре объектов SCOM	283
Реагирование на события системы	285
<i>Nagios</i>	286
Установка <i>Nagios</i>	286
Немного о логике работы <i>Nagios</i>	287
Структура конфигурационных файлов <i>Nagios</i>	289
Описание команд <i>Nagios</i>	289
Службы <i>Nagios</i>	290
Описание контролируемых систем в <i>Nagios</i>	291
Описание временных параметров.....	292
Использование встроенных в <i>Nagios</i> команд контроля.....	292
Мониторинг серверов Windows в <i>Nagios</i>	295
Мониторинг Windows-систем на основе WMI	299
Мониторинг серверов Linux в <i>Nagios</i>	300
Мониторинг систем с использованием протокола SNMP	300
Мониторинг коммутационного оборудования	301
Использование собственных программ мониторинга	303
Построение графиков в <i>Nagios</i>	304
Настройка интерфейса <i>Nagios</i>	306
Глава 8. Виртуализация	307
Экономические аспекты виртуализации	307
Основные термины	308
Разработчики виртуальных решений	309
Распределение ресурсов в *nix	310
Особенности выбора ПО гипервизора	310
Какое ПО можно использовать в виртуальной среде	311
Особенности сетевых подключений виртуальных машин	312
Лицензирование программного обеспечения виртуальных машин.....	313
Создание виртуальных машин.....	313
Создание виртуальной машины путем чистой установки операционной системы.....	314
Клонирование виртуальной машины	315
Снятие образа физического сервера.....	315
Миграция между решениями различных вендоров.....	316
Некоторые замечания к параметрам виртуальных машин	317
Жесткие диски	317
Типы виртуальных дисков	317
Необходимость блочного доступа к виртуальному диску.....	318
Варианты подключения виртуального диска	318
Обслуживание файлов виртуального диска	318
Сохранение состояния виртуальной машины.....	319
Распределение вычислительных ресурсов.....	319
Оперативная память.....	319

Сервисные операции.....	320
Резервное копирование и антивирусная защита.....	320
Обмен данными.....	320
Копирование данных с хоста	320
Общие папки.....	320
Миграция виртуальных машин	321
Подключения к виртуальным машинам	322
Особенности выключения виртуальных машин.....	323
Виртуальные рабочие станции	323
Сравниваем с терминальными клиентами	323
Немного об экономике VDI	324
Структура VDI-решений.....	325
Некоторые особенности VDI-решений	326
Производительность виртуальных систем.....	327
Советы по оптимизации виртуальных систем	327
Некоторые дополнительные источники технической поддержки	328
Виртуализация в сетях передачи данных.....	329
Виртуальные частные сети.....	329
Варианты создания VLAN	329
Теги 802.1q	330
VLAN 1	331
Маршрутизация в сетях предприятий	331
Автоматизация настроек маршрутизации.....	332
DHCP-relay.....	333
Программная маршрутизация	333
Виртуальные маршрутизаторы	334
Глава 9. Безопасность	335
Человеческий фактор.....	335
Интернет-ресурсы, посвященные безопасности	336
Попытаемся разложить по полочкам	337
Что защищаем	337
Где защищаем.....	337
От чего защищаем.....	337
Как защищаем	339
Три "кита" безопасности	339
Типовые меры защиты информационной системы.....	340
Организационное обеспечение информационной безопасности	341
План обеспечения непрерывности функционирования информационной системы	341
Безопасность паролей	342
Rainbow-таблицы	344
Рекомендации по составлению сложного пароля	345
Технические пути решения проблемы	345
Блокировка учетной записи пользователя	345
Смарт-карты	346
Восстановление пароля администратора	348
Методы социальной инженерии	349

Меры защиты от внешних угроз.....	350
Физическая безопасность.....	350
Ограничения доступа к станциям.....	350
Межсетевые экраны.....	351
Ограничения подключения нового оборудования.....	351
Обеспечение сетевой безопасности информационной системы.....	352
Контроль проходящего трафика.....	352
Контроль устройств по MAC-адресам.....	353
Протокол 802.1x.....	354
Технология NAP.....	360
Обнаружение нештатной сетевой активности.....	361
Контроль состояния программной среды серверов и станций.....	362
Индивидуальная настройка серверов.....	362
Security Configuration Manager.....	363
Security Compliance Manager.....	363
Исключение уязвимостей программного обеспечения.....	364
Использование эксплойтов.....	364
Как узнать об обновлениях.....	364
Тестирование.....	368
Обновления операционных систем Linux.....	369
Индивидуальные обновления Windows-систем.....	369
Организация обновлений Windows-систем на предприятии.....	370
Обновление ПО с использованием специализированных средств.....	372
Установка обновлений через групповые политики.....	373
Защита от вредоносных программ.....	373
Особенности эксплуатации антивирусных программ.....	373
График обновлений баз.....	374
Внимательность пользователя.....	375
Лечение вирусов.....	375
Защита от вторжений.....	376
Программы-шпионы. "Троянские кони".....	376
Безопасность приложений.....	380
Средства контроля запуска программного обеспечения.....	381
Неизменность системы.....	382
Защита от утечки данных.....	382
Шифрование данных.....	382
Шифрование данных на устройствах хранения.....	383
Шифрование в Linux.....	385
Шифрование файловой системы Windows.....	386
Шифрование диска при помощи BitLocker.....	387
Шифрование почты.....	390
Шифрование в базах данных.....	392
Цифровые права документов.....	393
Стеганография.....	394
Анализ поведения пользователей.....	395
DLP-технологии.....	395
Анонимность работы в глобальной Сети.....	396
Скрытие своего IP-адреса.....	396

Защита от файлов слежения на компьютере.....	397
Использование наложенных сетей	399
Глава 10. Построение отказоустойчивой информационной системы	401
Территориальная распределенность	401
Центры обработки данных	401
Требования к помещениям ЦОД	402
Климат-контроль помещений ЦОД.....	402
Резервирование электроснабжения ЦОД.....	403
Системы пожаротушения ЦОД.....	403
Надежность системы электроснабжения	403
Надежность сетевой инфраструктуры.....	404
Отказоустойчивая топология сети передачи данных.....	404
Построение отказоустойчивой сети на основе протоколов второго уровня.....	405
Использование "агрегированных" каналов.....	407
Построение отказоустойчивой сети на основе протоколов третьего уровня.....	408
Время восстановления структуры сети	409
Серверные фермы	410
Отказоустойчивые решения приложений	411
DHCP-сервер	411
DNS-серверы	411
Oracle Real Application Cluster (RAC).....	412
Распределенная база 1С.....	412
Дублирование данных	412
Зеркалирование серверов баз данных	413
Репликация данных SQL-серверов	413
Снимки баз данных	414
Настройка клиентских подключений	414
Распределенная файловая система	414
Создание DFS	415
Репликация DFS	416
Поддержка DFS в Linux-системах	417
Кластерные решения	418
Кластер Microsoft	418
Veritas Cluster Server	421
Решения высокой доступности от Marathon.....	422
Распределенные каталоги.....	423
Репликация данных каталогов	424
Хозяева операций.....	424
Сервер глобального каталога (GC).....	425
Отказоустойчивые решения на виртуальных системах	426
Глава 11. Порядок настройки и определения неисправностей	427
Прежде чем начать.....	427
Пять девяток?	428
Будьте готовы к худшему.....	428
Запасные детали	429
Где найти помощь	429

Сбор информации об отказе	431
Анализ журналов системы	431
Средства просмотра журналов системы	432
Изменение детализации протоколирования	433
Централизованное ведение журналов	434
Установка триггеров на события протоколов.....	437
Настройка аудита событий безопасности	438
Утилиты от Sysinternals	438
Особенности отказов различных компонентов	439
Мониторинг отказоустойчивой структуры	439
Неисправности подсистемы передачи данных	439
Обнаружение неисправностей сетевой инфраструктуры	440
Диагностика IP-протокола	440
Проверка качества канала связи	445
Неисправности аппаратной части компьютера	451
Контроль жестких дисков.....	451
Проверка оперативной памяти.....	453
Контроль теплового режима работы системы.....	454
Ошибки программного обеспечения	455
Восстановление "упавших" систем	455
Восстановление из резервной копии	456
Восстановление загрузчика системы.....	457
Восстановление загрузки Windows 7/2008/Vista.....	457
Восстановление загрузки Windows XP/2003/2000	457
Восстановление загрузки Linux-систем	459
Если опции восстановления недоступны	460
Загрузка в специальных режимах	460
Загрузка Windows в безопасном режиме	461
Загрузка *nix-систем в однопользовательском режиме.....	461
Откат к предыдущим состояниям системы	461
Загрузка последней удачной конфигурации Windows	461
Загрузка конфигурации из точек восстановления Windows	462
Восстановление Windows путем переустановки	463
Восстановление удаленных данных	464
Корзины	464
Восстановление из теневых копий	464
Оптимизация настроек компьютера	466
Что такое "медленно"	466
Основные узкие места системы	467
Оценка производительности процессора	468
Оценка использования оперативной памяти	470
Оценка дисковой подсистемы.....	470
Оценка работы сетевого адаптера	474
Некоторые советы по анализу показаний производительности.....	476
Оптимизация приложений.....	477
Диагностика службы каталогов	477
Обнаружение неисправностей AD.....	478
Средства тестирования AD	478
Проверка разрешения имен.....	479

Глава 12. Плановые операции обслуживания	481
Ежедневные операции	481
Еженедельные операции	483
Плановые операции другой периодичности	483
План-отчет операций	484
Предметный указатель	487

Предисловие

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

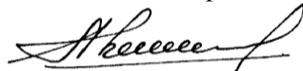
Занимаясь более 20 лет администрированием и развитием компьютерных систем, оказывая техническую поддержку, я постоянно сталкиваюсь с однотипными проблемами и вопросами пользователей и специалистов. И каждый раз я пытаюсь простыми и доходчивыми словами объяснить основы, на которых построена современная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

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

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

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

Ваш Александр Кенин



ГЛАВА 1



Системное администрирование

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

Системный администратор

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

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

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

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

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

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

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

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

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

Регламент работы

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

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

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

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

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

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

Выбор операционной системы

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

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

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

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

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

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

ПРИМЕЧАНИЕ

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

Стоимость владения

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

ПРИМЕЧАНИЕ

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

Открытые стандарты

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

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

Подобных примеров можно привести много.

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

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

ПРИМЕЧАНИЕ

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

Конкурсы

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

требования до такой степени, что они могут быть выполнены только определенной моделью оборудования¹. А можно сформулировать лишь основные, принципиальные требования проекта, рассмотреть полученные в итоге конкурса подходы к решению проблемы и выбрать оптимальный вариант.

Переход на новые версии программного обеспечения

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

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

ПРИМЕЧАНИЕ

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

Сертификация системных администраторов

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

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

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

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

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

ПРИМЕЧАНИЕ

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

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

Немного этики

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

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

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

О мистике

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

ГЛАВА 2



Выбор оборудования и программного обеспечения

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

Требования к оборудованию информационных систем

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

Выбор вендора

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

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

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

Сервисные контракты

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

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

Запасные элементы

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

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

Дополнительные требования к компьютерам

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

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

Выбор процессора

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

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

Выбор шасси

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

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

Выбор материнской платы

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

Sun(TM) Integrated Lights Out Manager - Mozilla Firefox

https://192.168.2.75/iPages/suntab.asp

User: root (Administrator) Server: SUNSP00144F6B6B9D

Sun™ Integrated Lights Out Manager

System Information System Monitoring Configuration User Management Remote Control Maintenance

Sensor Readings Event Logs Locator Indicator

Sensor Readings

View readings for temperature, voltage, or fan sensors.

Select a sensor type category:

All Sensors

Sensor Readings: 80 sensors

Status	Name	Reading	Low NR	Low CT	Low NC	High NC	High CT	High NR
Normal	mb.v_bat	2.928 Volts	2.4 Volts	2.592 Volts	2.888 Volts	3.392 Volts	3.6 Volts	3.7
Normal	mb.v_+3v3stby	3.252 Volts	2.595 Volts	2.785 Volts	2.992 Volts	3.598 Volts	3.788 Volts	3.5
Normal	mb.v_+3v3	3.338 Volts	2.595 Volts	2.785 Volts	2.992 Volts	3.598 Volts	3.788 Volts	3.5
Normal	mb.v_+5v	4.94 Volts	3.484 Volts	3.978 Volts	4.498 Volts	5.486 Volts	5.98 Volts	6.5
Normal	mb.v_+12v	12.222 Volts	8.946 Volts	9.954 Volts	10.962 Volts	12.978 Volts	13.986 Volts	14
Normal	mb.v_-12v	-12.204 Volts	-15.051 Volts	-14.029 Volts	-13.007 Volts	-11.036 Volts	-10.014 Volts	-9
Normal	mb.v_+2v5core	2.532 Volts	1.8 Volts	1.992 Volts	2.196 Volts	2.796 Volts	2.892 Volts	3
Normal	mb.v_+1v8core	1.84 Volts	1.1 Volts	1.3 Volts	1.5 Volts	2.1 Volts	2.3 Volts	2.5
Normal	mb.v_+1v2core	1.22 Volts	0.6 Volts	0.8 Volts	1 Volts	1.5 Volts	1.7 Volts	1.5
State Asserted	bp.power	2	-0.001	0	-0.001	-0.001	0	0

Refresh... Hide Thresholds

Готово 192.168.2.75 2.933s

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

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

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

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

Выбор дисков

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

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

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

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

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

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