



АЛЕКСАНДР КЕНИН

Практическое руководство СИСТЕМНОГО АДМИНИСТРАТОРА

2-е издание

Задачи системного администратора

Эксплуатация сети передачи данных

Решения на основе технологий Windows и Linux

Рекомендации по установке, настройке и оптимизации основных служб

Секреты оптимальной и безопасной работы в Интернете

Обеспечение работы мобильных пользователей

Защита информации и отказоустойчивость

Мониторинг информационных систем

СИСТЕМНЫЙ
АДМИНИСТРАТОР

УДК 004
ББК 32.973.26-018.2
К33

Кенин А. М.

К33 Практическое руководство системного администратора. — 2-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2013. — 544 с.: ил. — (Системный администратор)

ISBN 978-5-9775-0874-2

Практическое руководство к действию для системных администраторов, создающих и эксплуатирующих информационные системы офиса. Параллельно рассмотрены решения на основе технологий Windows и Linux. Приведены рекомендации по установке, настройке и оптимизации основных служб информационной системы, организации работы системного администратора, развертыванию операционных систем Windows и Linux (Ubuntu), программ корпоративной работы, мониторинга состояния серверов. Особое внимание уделено вопросам обеспечения безопасности и надежности. Даны конкретные советы по настройке основных сетевых служб, обеспечению распределенной работы в Интернете. Описана технология разрешения проблем в работе операционной системы и прикладных программ и их совместная тонкая настройка.

Второе издание доработано с учетом выхода новых версий ПО и появления новых технологий.

Для системных администраторов

УДК 004
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>Екатерина Капалыгина</i>
Редактор	<i>Анна Кузьмина</i>
Компьютерная верстка	<i>Ольги Сергиенко</i>
Корректор	<i>Зинаида Дмитриева</i>
Дизайн серии	<i>Инны Тачиной</i>
Оформление обложки	<i>Марины Дамбиевой</i>

Подписано в печать 30.04.13.
Формат 70×100^{1/16}. Печать офсетная. Усл. печ. л. 43,86.
Тираж 1500 экз. Заказ №
"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

Первая Академическая типография "Наука"
199034, Санкт-Петербург, 9 линия, 12/28

ISBN 978-5-9775-0874-2

© Кенин А. М., 2013
© Оформление, издательство "БХВ-Петербург", 2013

Оглавление

Предисловие	1
Глава 1. Системный администратор	3
Квалификационные требования к системным администраторам	3
Начинающий системный администратор	3
"Младший" системный администратор	4
Системный администратор	4
Опытный системный администратор	5
Дополнительные требования	5
Сертификация системных администраторов	6
Планирование рабочего дня	6
Выделяйте время на перспективные проекты	6
Работа с пользователями	7
Обучение системного администратора	7
Реализация изменений в информационной системе	8
Планирование изменений	8
Планирование момента изменений и продолжительности операций	9
Системный администратор как продавец ИТ-технологий	10
Учитывать человеческие особенности	11
Быть в курсе	11
Ошибки администратора	12
Инструкции и контрольные листы	12
Полномочия системного администратора	12
Если в организации внедряется новая система	13
Особенности организации рабочего места администратора	14
Программное оснащение рабочего места администратора	16
Загрузочный диск	16
Комплект переносных утилит	17
Отдельные утилиты	19
Глава 2. Готовим компьютер к эксплуатации	23
Паспорт компьютера	23
Установка операционной системы	25
Live-версии операционных систем	25

Live-версии Windows.....	25
Live-версии Linux-систем.....	26
Установка Windows	26
Автоматизация установки.....	26
Установка с USB-носителя	27
Режим Windows Core.....	28
Установка Linux-систем	31
Настройка локализованной консоли	32
Настройка сетевых параметров	32
Настройка синхронизации времени	33
Многовариантная загрузка.....	34
Требования к сосуществованию двух ОС.....	34
Установка двух ОС на один компьютер	37
Восстановление двойной загрузки в Windows	37
Кроссплатформенный доступ	39
Удаленный доступ к Linux	39
Перенаправление графического вывода с Linux-систем	43
Подключение к рабочему столу Linux	43
Запуск Windows-программ на Linux	44
Клонирование систем	45
Учитывайте уникальные параметры системы.....	45
Дублирование жесткого диска.....	46
Утилита <i>sysprep</i>	46
Модификация образов диска	47
Установка виртуальных систем.....	47
Создание виртуальной машины путем чистой установки операционной системы.....	47
Клонирование виртуальной машины	48
Снятие образа физического сервера.....	48
Миграция между решениями различных вендоров	49
Использование неизменной конфигурации системы.....	49
Настройка серверов.....	50
Security Configuration Manager.....	50
Security Compliance Manager.....	51
Установка обновлений прошивок оборудования.....	51
Установка обновлений безопасности.....	51
Когда устанавливать обновления	52
Нужно ли устанавливать все обновления?	53
Настройка установки обновлений с сервера интрасети	54
Установка обновлений в Linux	56
Ускорение запуска программ.....	57
Регулировка приоритетов приложения	57
Проблемы совместимости ПО разных версий Windows	59
Установка программ Windows из сети.....	60
Особенности установки через групповые политики.....	60
Публикация и назначение приложений.....	60
Установка на компьютер и для пользователя.....	61
Подготовка ZAP-файла	61

Установка программ в Linux.....	62
Установка приложений из репозитория.....	62
Переконвертация пакетов.....	64
Установка программ Linux из исходных кодов.....	64
Виртуализация приложений.....	66
Использование опубликованных приложений. RemoteApp.....	67
Тихая установка программ.....	69
Переупаковка.....	70
Файлы ответов (трансформаций).....	71
Службы системы.....	71
Установка служб Windows.....	71
Установка демонов в Linux.....	72
Запуск программ по времени.....	73
Настройка расписания запуска программ в Windows.....	73
Выполнение заданий по расписанию в Linux.....	74
Глава 3. Сетевая инфраструктура.....	77
Строение сети передачи данных.....	77
Размеры сегментов сети.....	77
Выбор типа коммутаторов.....	78
Топология сети передачи данных.....	79
Ищем точку подключения компьютера.....	80
Контроль подключения к СКС.....	82
Предварительные настройки для использования протокола 802.1x.....	84
Настройка компьютера.....	85
Настройка домена Windows.....	85
Настройка сервера RADIUS.....	85
Настройка политики доступа на основе протокола 802.1x.....	86
Настройка коммутатора для работы с протоколом 802.1x.....	88
Технология NAP.....	89
Настройка протокола IP.....	90
Протоколы UDP, TCP, ICMP.....	90
Протокол IPv6.....	91
Параметры TCP/IP-протокола.....	91
IP-адрес.....	91
Групповые адреса.....	92
Распределение IP-адресов сети малого офиса.....	92
Маска адреса.....	93
Шлюз.....	94
Таблицы маршрутизации.....	95
Назначение адресов при совместном использовании подключения к Интернету.....	96
Порт.....	96
Имена компьютеров в сети TCP/IP.....	97
Проверка каналов связи.....	98
Диагностика линий связи.....	98
Диагностика IP-протокола.....	100
Служба автоматического назначения параметров IP-адреса.....	105
Адресация APIPA.....	105

Серверы DHCP	106
Настройка серверов DHCP в Windows.....	106
Установка и настройка сервера DHCP в Ubuntu	108
Обслуживание DHCP-сервером других сегментов сети.....	109
Статическое разрешение имен.....	110
Серверы DNS	111
Основные понятия DNS	111
Основные типы записей DNS	113
Разделение DNS	114
Одинаковые имена локального домена и домена Интернета.....	114
Различные имена локального домена и домена Интернета	116
Установка сервера DNS.....	116
Установка DNS в Windows Server	117
Установка и настройка сервера DNS в Ubuntu.....	118
Динамическое обновление DNS	120
Обслуживание и диагностика неисправностей DNS-сервера	123
Глава 4. Обеспечение доступа в Интернет	127
Подключение к Интернету с использованием аппаратного маршрутизатора.....	127
Network Address Translator	129
Подключение к Интернету в Windows.....	130
Использование службы маршрутизации и удаленного доступа	130
Совместное использование интернет-подключения	130
Публикация компьютеров в Интернете при совместном использовании	
подключения	131
Ограничения совместного использования подключения к Интернету	132
Подключение к Интернету с помощью Microsoft TMG Server.....	132
Поиск причин запрета трафика.....	134
Подключение к Интернету с использованием серверов Ubuntu.....	134
Настройка <i>ufw</i>	135
Межсетевой экран <i>iptables</i>	135
Последовательность обработки пакета (таблицы).....	136
Использование <i>iptables</i> в Ubuntu	137
Правила <i>iptables</i>	138
Команды	138
Параметры	139
Опции	139
Настройка NAT	140
Очистка всех правил <i>iptables</i>	142
Назначение политик по умолчанию	142
Пример настройки <i>iptables</i>	142
Пользовательские цепочки команд	143
Некоторые полезные функции <i>iptables</i>	144
Отладка <i>iptables</i>	145
Блокировка попыток перебора паролей.....	145
Настройка VPN-подключения к интернет-провайдеру	146
Прокси-сервер.....	149
Автообнаружение прокси-серверов	150
Установка и настройка прокси-сервера	151

Дополнительные настройки прокси-сервера.....	152
Как создавать собственные настройки.....	153
Настройка использования полосы пропускания	154
Блокировка рекламы, порносайтов и т. п.	155
Улучшение эффективности использования кэша прокси-сервера	156
Аутентификация доступа в Интернет	158
"Прозрачный" прокси-сервер	159
Анализ журналов работы прокси-сервера	159
Антивирусная проверка HTTP-трафика	161
Глава 5. Средства управления.....	165
Управление с помощью групповых политик	165
К чему и как применяются групповые политики	166
Где хранятся и когда применяются групповые политики	168
Последствия отключений политик	169
Чем редактировать групповую политику.....	169
Средства удаленного администрирования сервера.....	169
Назначение и удаление политики.....	172
Начальные объекты групповой политики.....	172
Расширенное управление групповыми политиками	172
"Обход" параметров пользователя	174
Фильтрация объектов при применении групповой политики	175
Фильтрация при помощи WMI-запросов.....	175
Настройка параметров безопасности групповых политик	175
Предпочтения групповых политик.....	176
Особенности предпочтений групповых политик	176
Клиенты предпочтений групповых политик	177
Общие свойства параметров групповых политик	177
Нацеливание на уровень элемента	179
Параметры, настраиваемые предпочтениями групповой политики.....	181
Регулярные выражения	185
Используемые символы. Метасимволы	185
Модификаторы.....	187
Комментарии.....	187
Поиск с учетом окружающего текста	187
Средства тестирования	188
Удаленное управление в режиме консоли.....	189
Запуск удаленного процесса через WMI	192
Запуск команд с использованием PsExec.....	192
Коммерческие утилиты	193
Использование WinRM в сценариях	193
PowerShell.....	193
Запуск PowerShell	194
Профиль пользователя	197
Консоль PowerShell.....	198
Безопасность сценариев	199
Удаленное выполнение команд PowerShell.....	201
Импорт расширений	202

Асинхронное выполнение заданий.....	204
Как получить подсказку в PowerShell	204
Конвейеры	206
Условные операторы, регулярные выражения, циклы	206
Функции.....	207
Переменные.....	208
Акселераторы типов	208
Диски PowerShell	209
PowerShell и WMI	211
PowerShell и Visual Basic.....	212
PowerShell и ADSI.....	212
Несколько советов по созданию собственных сценариев	212
Комментируйте сценарии.....	213
Не забывайте, что результат выполнения запроса — объект.....	213
Используйте примеры	214
Узнайте свойства объектов	214
Отображайте весь вывод	215
Семь раз проверьте, потом выполняйте.....	215
Предусматривайте обработку ошибок	216
Windows Management Interface	216
Глава 6. Доменная организация информационной системы.....	221
Домены Windows	221
Структура домена Windows	221
Функциональные уровни.....	223
Хозяева операций.....	223
Сервер глобального каталога (GC).....	224
Создание нового домена	225
Создание домена на серверах Windows	225
Настройка Ubuntu в качестве контроллера домена.....	226
Серверы Linux в качестве контроллеров домена	227
Настройка контроллера домена на сервере корпоративной почты Zimbra	227
Настройка параметров аутентификации	234
Добавление новых членов домена.....	237
Добавление Windows-систем	237
Модификация настроек Windows-систем при добавлении их в домен	239
Добавление Linux-систем в домен Windows	239
Диагностика службы каталогов.....	241
Обнаружение неисправностей AD	241
Средства тестирования AD	242
Проверка разрешения имен	244
Снимки службы каталогов	245
Создание снимков службы каталогов	246
Монтирование снимков службы каталогов	246
Публикация данных снимков.....	247
Удаление снимков.....	248
Службы Active Directory облегченного доступа к каталогам	249
Контроллер домена только для чтения	249
Особенности установки RODC.....	250

Особенности кэширования учетных данных.....	251
Настройка предварительных паролей.....	252
Коррекция состава учетных записей кэширования на RODC.....	252
Сброс паролей кэшированных учетных записей RODC.....	252
Известные проблемы использования RODC.....	253
Глава 7. Управление учетными записями.....	255
Понятие учетной записи.....	255
Локальные и доменные учетные записи.....	257
Создание и удаление учетных записей.....	258
Создание учетных записей в Windows.....	258
Создание учетных записей в Linux.....	259
Регулирование членства в группах в Linux.....	260
Автоматически создаваемые учетные записи.....	261
Учетная запись <i>Система</i>	263
Настройка отдельных параметров паролей.....	264
Настройка отличающихся политик паролей в Windows Server 2008.....	264
Настройка правил смены пароля в Linux.....	266
Блокировка учетных записей.....	266
Группы пользователей.....	267
Встроенные группы Windows.....	268
Специальные группы Windows.....	269
Возможные члены групп. Области применения групп.....	270
Контроль состава групп.....	271
Запуск команд от имени другого пользователя.....	272
Эскалация прав <i>Администратора</i> в Windows.....	272
Запуск от имени другого пользователя в Windows.....	273
Запуск от имени другого пользователя в Linux.....	273
Предоставление дополнительных прав командой <i>sudo</i>	273
Кто работает на компьютере.....	275
Права учетной записи.....	275
Традиционные способы назначения прав доступа.....	275
Разрешения общего доступа и разрешения безопасности.....	276
Порядок проверки прав доступа.....	277
Правила записи прав доступа.....	278
System ACL.....	280
Коды типов пользователей в SDDL.....	280
Права доступа в Linux.....	282
Типы прав доступа в Linux.....	282
Команды назначения прав доступа Linux.....	283
Особенности назначения прав доступа к папкам Linux.....	283
Специальные атрибуты файлов Linux.....	284
Особое внимание к учетной записи оператора резервного копирования.....	285
Изменение атрибутов объектов при операциях копирования и перемещения.....	285
Результирующие права и утилиты.....	286
Рекомендации по применению разрешений.....	287
Назначение прав на выполнение операций.....	288
Обход перекрестной проверки.....	289

Утилиты для работы с параметрами безопасности.....	289
Стандартные графические утилиты	289
Назначение прав доступа при помощи групповых политик	289
Специализированные утилиты.....	290
Утилита <i>icacls</i>	290
Пример замены разрешений одного пользователя на другого	291
Пример поиска файлов, доступных конкретному пользователю	292
Пример замены явных прав на наследованные	292
Утилита <i>takeown</i>	292
Утилита <i>SubInAcl</i>	292
Ролевое управление	292
Сервисные операции управления ролями.....	294
Восстановление параметров безопасности по умолчанию (графический режим).....	294
Восстановление параметров безопасности по умолчанию (командная строка).....	295
Восстановление доступа к ресурсам	296
Удаление неактивных учетных записей.....	296
Сброс пароля администратора сервера.....	297
Сброс пароля администратора Windows.....	297
Сброс пароля учетной записи root.....	299
Изоляция приложений.....	300
Контроль приложений Windows	300
Безопасная среда исполнения Linux.....	301
Глава 8. Почтовая система предприятия	305
Варианты почтового обслуживания.....	305
Бесплатные почтовые серверы Интернета.....	305
Облачное почтовое обслуживание	305
Размещение почтового сервера у провайдера	306
Собственный почтовый сервер.....	306
Протоколы для работы с почтовыми ящиками.....	306
Корпоративные почтовые системы.....	308
Сервисы корпоративной почты	308
Почтовый сервер Microsoft Exchange.....	309
Zimbra Collaboration Suite	310
Возможности совместной работы в ZCS	310
Установка Zimbra.....	311
Требования к операционной системе.....	311
Установка пакета ZCS	312
Настройка безопасного доступа к почте.....	314
Администрирование ZCS	314
Резервное копирование Zimbra.....	317
Особенности пользовательских почтовых ящиков Zimbra	318
Настройка взаимодействия с доменом Windows	319
Совместная работа Zimbra и Microsoft Exchange	320
Миграция с Microsoft Exchange	320
Почтовый клиент Zimbra.....	320
Особенности настройки фильтрации спама в ZCS	321
Трассировка сообщений в Zimbra	322
Поиск неисправностей ZCS	323

Глава 9. Организация корпоративных ресурсов.....	325
Требования к качеству обслуживания	325
Политики общих ресурсов	325
Объемы и сроки хранения. Возможности восстановления	326
Производительность	326
Поиск информации. Карточка документа.....	326
Контроль объемов и типов документов	327
Варианты организации корпоративных ресурсов.....	327
FTP-сервер.....	327
Установка FTP-сервера	328
Установка собственного FTP-сервера Windows	329
Установка vsftp	330
Использование распределенной файловой системы.....	331
Создание DFS в Windows-системах	332
Репликация DFS в домене Windows	333
Репликация папок в рабочих группах	335
Настройка DFS в Ubuntu	335
Ограничение предоставляемых файловых ресурсов	336
Настройка квотирования в Windows	336
Квотирование на уровне файловой системы	336
Квотирование общих папок	337
Блокировка записи в папки по типам файлов в Windows.....	338
Настройка квотирования в Ubuntu	339
Запрет записи на сетевые ресурсы Ubuntu по типам файлов	341
Корпоративные порталы	341
Особенности порталов.....	342
Установка Liferay на сервере Ubuntu	343
Портальные решения от Microsoft.....	345
Где найти помощь по SharePoint	346
Установка портала Windows	347
Подготовка операционной системы.....	347
Запуск мастера установки технологии.....	348
Запуск мастера настройки продуктов и технологий	349
Установка обновлений	349
Административная настройка параметров портала	349
Создание и редактирование страниц узла	351
Используйте возможности штатных элементов SharePoint	352
Установка поискового сервера по общим ресурсам.....	353
Настройка автоматических оповещений об изменениях документов на чужих серверах.....	354
Глава 10. Обеспечение работы мобильных пользователей	355
Терминальный доступ.....	355
Терминальные серверы Linux.....	356
Терминальные серверы от Microsoft.....	356
Особенности установки ПО на сервере терминалов.....	357
Безопасность при работе с терминальным сервером.....	358
Удаленные приложения	360
Веб-доступ к терминальному серверу. Шлюз терминалов	362

Некоторые особенности работы в режиме терминального доступа.....	363
Командная строка управления терминальными сессиями	363
Технологии доставки виртуального рабочего стола.....	364
Удаленное подключение пользователей к внутренней сети предприятия.....	365
Безопасное объединение локальных сетей офисов.....	366
Подключение офисов через виртуальную сеть провайдера.....	366
Подключение с использованием VPN-серверов Windows	367
Фильтрация VPN-трафика	368
В случае разрыва канала при доменной организации офиса.....	369
Подключение удаленных клиентов с помощью VPN-серверов Linux	369
Подключение "офис — офис" на основе технологии SSH.....	372
Облачные ресурсы.....	376
Управление оборудованием по Интернету.....	377
Intelligent Platform Management Interface	377
Управление оборудованием по сети IP.....	379
Синхронизация данных в офисах.....	380
Кэширование информации на компьютерах филиала	380
Синхронизация папок DFS.....	381
Синхронизация с помощью утилит	382
Утилиты синхронизации файлов и папок	382
Синхронизация данных со сменным носителем	383
Автономные файлы	384
Разрешение конфликтов.....	385
Удаление автономных файлов.....	385
Настройка автономных почтовых папок	386
Перенаправление папок хранения документов	386
Доступ к локальной системе из-за межсетевое экрана.....	387
Глава 11. Мониторинг информационной системы.....	389
Зачем нужен мониторинг?	389
Системы мониторинга.....	389
Агентный и безагентный способы мониторинга.....	390
Какие параметры системы обычно контролируют	390
Простейший вариант мониторинга по журналам	391
Log Parser.....	391
Централизованная обработка журналов Windows	392
Syslog — системный журнал в Linux	394
Nagios.....	394
Установка Nagios в Ubuntu из репозитория.....	395
Установка Nagios из исходных кодов	395
Подготовка операционной системы.....	395
Установка пакета net-snmp.....	396
Установка собственно Nagios и базового набора плагинов	397
Настройка модуля построения графиков	398
Настройка почтового клиента.....	400
Первичное подключение к Nagios.....	400
Немного о логике работы Nagios.....	401
Активная и пассивная проверки	401

Программы агентов Nagios	401
Терминология Nagios	402
Мониторинг серверов Windows.....	412
NSClient++	412
Стили команд: протоколы NSClient и NPPE	415
Контроль счетчиков Windows.....	415
Мониторинг журналов событий Windows	416
Использование WMI для мониторинга Windows-систем	417
Мониторинг серверов Linux	418
Установка плагина NRPE из исходных кодов.....	418
Установка плагина NRPE из репозитория	419
Установка демона NRPE из репозитория	419
Использование прокси-NRPE	420
Мониторинг с использованием протокола SNMP	420
Плагины, использующие SNMP-протокол	422
Обработка SNMP-трапов	423
Мониторинг коммутационного оборудования	427
Использование собственных программ мониторинга	430
Автоматическое реагирование на сбои в работе контролируемых систем.....	431
Глава 12. Защита информации	433
Опасности, которые нужно учитывать	433
Причины рисков	434
Порядок организации работ по защите информации	435
Примерные мероприятия по обеспечению защищенности информации	435
Проактивность мер защиты	435
Резервное копирование	436
Теневые копии	436
Системы цифровой защиты документов.....	438
DLP-решения.....	438
Антивирусная защита	439
Восстановление данных с жестких дисков	439
Глава 13. Построение отказоустойчивой системы	441
Общие требования к надежной системе	441
Территориальная распределенность	442
Надежность системы электроснабжения.....	442
Обеспечение климатических условий эксплуатации.....	444
Обеспечение отказоустойчивой среды передачи данных	444
Отказоустойчивая топология сети передачи данных.....	444
Построение отказоустойчивой сети на основе протоколов второго уровня	445
Использование протоколов остовного дерева.....	445
Использование стандарта MSTP	446
Построение отказоустойчивой сети на основе протоколов третьего уровня	447
Кластеры коммутационного оборудования.....	447
VRRP.....	447
Время восстановления структуры сети.....	448
Обеспечение резервированного доступа в Интернет.....	449

Построение отказоустойчивых сетевых служб	450
Настройка систем аутентификации	450
Отказоустойчивый DHCP-сервер	450
Дублирование DNS-сервера	453
Дублирование данных	454
Репликация файловых данных в DFS	454
Репликация данных средствами СХД	455
Зеркалирование серверов баз данных	455
Снимки баз данных	456
Настройка клиентских подключений	456
Сетевая балансировка	457
Кластерные решения	458
Кластер Microsoft	458
Veritas Cluster Server	460
Территориально распределенные кластеры Microsoft	461
Решения высокой доступности от Marathon	461
Отказоустойчивые решения на виртуальных системах	463
Глава 14. Порядок настройки и определения неисправностей.....	465
Где найти помощь?	465
Неисправность не может не возникнуть	466
Общие рекомендации по процедуре решения проблем	466
Имейте план действий	467
Обеспечьте доступность специалистов службы поддержки	467
Формализуйте процесс	467
Обеспечьте запасные детали	469
Обдумайте заранее свои действия	469
Поиск неисправностей	470
Информация о надежности системы	470
Монитор ресурсов и производительности	471
Мастер диагностики Windows	472
Анализатор соответствия рекомендациям	473
Средства диагностики Windows Server 2008 R2	475
Fix it	475
Анализ журналов системы	476
Средства просмотра журналов системы	477
Централизованное ведение журналов	478
Изменение детализации протоколирования	481
Установка триггеров на события протоколов	481
Удаленная помощь пользователю	482
Удаленный помощник	482
Подключение к рабочему столу Windows	484
Средство записи действий по воспроизведению неполадок	485
Конкурентные RDP-сессии рабочей станции	486
Интерфейсы удаленного управления	486
Особенности отказов различных компонентов	487
Обнаружение неисправностей кабелей передачи данных	487
Признаки неисправности кабельной подсистемы	488

Диагностика IP-протокола	489
Оценка качества аудио- и видеопотоков.....	491
Мониторинг отказоустойчивой структуры.....	493
Неисправности аппаратной части компьютеров.....	493
Действия при подозрении на неисправность оборудования	493
Проверка оперативной памяти	494
Контроль жестких дисков	495
Контроль теплового режима работы системы.....	496
Резервирование узлов компьютера	496
Ошибки программного обеспечения.....	497
Выяснение причин катастрофических ошибок в программном обеспечении.....	497
Порядок работ по оптимизации системы	500
Оценка производительности компонентов системы.....	500
Оценка производительности процессора.....	501
Оценка использования оперативной памяти	502
Оценка дисковой подсистемы	503
Оценка работы сетевого адаптера	505
Углубленный анализ производительности системы	505
Варианты оптимизации компьютера.....	512
Если не справляется процессор	512
Если дисковая подсистема недостаточно быстра	512
Когда не справляется сетевой адаптер.....	513
Дополнительные средства, используемые при анализе показателей производительности	514
Logman.exe	514
Relog.exe	514
Iometer.....	514
PAL.....	516
Утилиты настройки параметров дисковой подсистемы Linux.....	517
Предметный указатель	519

ГЛАВА 1



Системный администратор

Не подлежит сомнению, что ведущая роль в управлении информационной системой принадлежит системным администраторам. При том, что в нашей стране часто не формализованы требования к этой профессии.

Квалификационные требования к системным администраторам

Каждая организация имеет свою уникальную информационную систему и предъявляет к соискателям на должность системного администратора различные требования. Тем не менее можно выделить некоторые типовые параметры.

Во-первых, информационные системы бывают различной сложности. Принято классифицировать их по размеру — по числу компьютеров. В малых организациях число компьютеров составляет не более 10—15 единиц, в больших — более сотни. Понятно, что уровень требований к системному администратору будет разным в случае большой или средней организации.

ПРИМЕЧАНИЕ

Критерии размеров организаций различны для реалий нашей страны и западных компаний. Обычно размер компании в нашей стране, определяемый по числу компьютерных систем, соответствует меньшему уровню западной фирмы. Это следует учитывать, например, оценивая рекомендации по выбору программного обеспечения и т. п.

Во-вторых, по степени подготовленности можно выделить несколько уровней системных администраторов.

Начинающий системный администратор

Обычно от такого специалиста требуется точное выполнение указаний руководителя (опытного администратора). Большею частью начинающему системному администратору поручается взаимодействие с конечными пользователями.

Поэтому требования к нему могут быть сформулированы так:

- умение взаимодействовать с пользователями;
- углубленное знание операционной системы рабочей станции (настройка прав пользователя, знание особенностей структуры домашних папок, умение вылечить систему от последствий вирусной атаки и аналогичные компетенции).

"Младший" системный администратор

Будем называть такого специалиста *младшим* администратором только для того, чтобы отличать его от начинающего системного администратора. В принципе, этот уровень соответствует начальной степени подготовки администратора, которую он может приобрести примерно за 2—3 года работы.

Такой администратор может сопровождать небольшую информационную систему либо работать в качестве помощника администратора крупной организации.

В дополнение к требованиям, изложенным для начинающего администратора, для этого уровня добавляются следующие критерии:

- понимание особенностей функционирования сетевой инфраструктуры (знание основ маршрутизации, умение добавлять станции в домен, предоставлять в пользование и подключаться к общим ресурсам, диагностировать сетевые проблемы и т. д.);
- фундаментальные знания операционной системы и практические навыки работы (обслуживание баз, разбиение дисков, создание и мониторинг логических массивов, резервное копирование и восстановление операционных систем и прикладного ПО и т. п.);
- умение составлять сценарии управления на одном из языков программирования.

Системный администратор

Этот "базовый" уровень должен соответствовать следующим требованиям:

- умение самостоятельно организовывать свой рабочий день;
- качественное сопровождение пользователей (умение общаться, решать проблемы и т. п.);
- умение проводить обучение сотрудников, готовить необходимые презентации;
- практический опыт настройки основных программных систем (почтовой системы, межсетевых экранов, параметров безопасности, различных вариантов разворачивания систем и т. п.);
- фундаментальное знание операционной системы;
- умение устранять сбои в работе системы (выявлять узкие места, производить отладку в случае необходимости, пользоваться снифферами и т. п.);
- умение составлять и отлаживать сценарии на основных языках. Умение модифицировать (приспосабливать) сценарии управления к потребностям собственной системы.

Опытный системный администратор

Администратор данного уровня должен:

- уметь общаться с сотрудниками, с представителями смежных организаций, с вендорами, уметь готовить презентации;
- быстро и полностью решать проблемы в информационной системе;
- уметь выделять задания, выполнение которых можно автоматизировать, и реализовывать соответствующие алгоритмы;
- глубоко понимать операционную систему и принципы сетевого взаимодействия;
- программировать на основных языках управления, иметь опыт составления собственных программ.

Опытный системный администратор должен уметь управлять сложной информационной системой (в том числе распределенной, с большим числом мобильных пользователей). Он должен быть способен выполнять роль технического руководителя для других системных администраторов, программистов и т. д.

Как правило, для такого специалиста требуется не менее чем 5-летний опыт работы в области системного администрирования.

Дополнительные требования

Вы не могли не заметить, что в качестве требований были указаны, в общем-то, общие характеристики, предъявляемые к должности. Понятно, что в каждой организации требования к вакансии системного администратора обычно конкретизируются по следующим позициям.

- Знание конкретных операционных систем.** Это могут быть различные выпуски Windows, клоны Linux, операционные системы Oracle Solaris, HP AIX, Red Hat и пр., которые эксплуатируются в организации. Часто от претендентов при приеме на работу требуются только базовые навыки с последующей обязанностью досконального изучения в ходе эксплуатации.
- Умение специального программирования.** Например, от администратора может потребоваться умение устранить ошибку (или отладить сценарий) в 1С.
- Опыт сетевого администрирования.** Может потребоваться знание сетей Novell, умение настройки протоколов маршрутизации (OSPF, BGP и т. п.), наличие опыта работы с протоколом PPP и т. п.
- Особые требования по информационной безопасности.** Например, настройка межсетевых экранов конкретных вендоров, умение разворачивать систему PKI, опыт настройки аутентификации по смарт-картам, знание основ шифрования данных и цифровой защиты документов и т. п.
- Требования по умению документировать.** От администратора может потребоваться умение описывать информационную систему, составлять инструкции для пользователей и т. п.

- ❑ **Опыт работы с базами данных.** Часто от администратора требуются навыки администрирования баз данных (резервное копирование и восстановление данных, экспорт информации, управление пользователями, назначение прав, настройка параметров производительности и т. д.).
- ❑ **Знание оборудования.** Как правило, от администратора требуется знание оборудования (опыт работы с ним), которое эксплуатируется в конкретной организации (например, конкретной линейки серверов, источников аварийного питания, модемов, маршрутизаторов и т. д.).

Сертификация системных администраторов

Подтверждением профессионализма администратора являются *сертификаты*, которые он может получить от тех или иных организаций. Для получения сертификата обычно требуется сдача некоторого числа экзаменов и наличие опыта работы по данному направлению. Хотя формально опыт работы и не проверяется, но, не имея его, сдать экзамен достаточно сложно.

Сертификаты бывают различными. Имеются сертификаты от вендоров (Sun/Oracle, Red Hat, Microsoft, Hewlett-Packard и др.), от организаций (например, от сообщества системных администраторов — SAGE) и др.

Традиционно наличие сертификата рассматривается кадровыми службами как дополнительный аргумент в пользу соискателя. Хотя в последнее время — по данным анализа зарубежных организаций — большинство сертификатов начинает терять свою значимость для технических руководителей. Не в малой степени этому способствуют такие случаи, когда сертификат системного инженера одного из ведущих вендоров получают 13-летние подростки, подготовленные только к ответам на тестовые вопросы.

Планирование рабочего дня

Рабочее время администратора расходуется на три основные группы задач:

- ❑ анализ состояния информационной системы;
- ❑ реагирование на события системы и обращения пользователей;
- ❑ плановые работы (расширение сети, установка новых служб, обновление программных комплексов и т. п.).

Выделяйте время на перспективные проекты

Реализация проектов требует вдумчивости и сосредоточения. Оперативная работа отвлекает от проектов, поэтому необходимо найти способ выделить время на решение стратегических задач. Если функции системного администратора возложены на нескольких специалистов, то можно так распределить обязанности, что один администратор будет заниматься обслуживанием пользователей, а другой — работать над проектом. Потом можно поменяться функциями.

Если численность специалистов не позволяет выделить специалиста для проектов, то нужно постараться так организовать работу с обращениями, чтобы высвободить хотя бы несколько часов. Для этого можно, например, предусмотреть для системного администратора "творческое время", в течение которого его можно отвлекать только для решения критических проблем, а остальные обращения будут поставлены в очередь и т. п.

Периодически анализируйте распределение своего времени. Например, если вы заметите, что значительная часть времени расходуется на поддержание функционирующего оборудования, то не лучше ли выйти к руководству с предложением об обновлении, которое будет обосновано реальными цифрами расхода времени?

Работа с пользователями

По тому, как системный администратор общается с пользователями, во многом оценивается его работа со стороны, в том числе и руководителями предприятия. По решению проблем пользователя судят о работе администратора со стороны. Пользователь не может, например, знать, что в этот момент есть другие важные проблемы, также требующие срочного разрешения. Пользователь должен ощутить внимание со стороны администратора к своему вопросу и остаться уверенным в том, что для решения его проблемы будут "брошены все силы".

Ни в коем случае нельзя разговаривать с пользователем так, чтобы акцентировать внимание на его незнании компьютера и простейших операций. Кроме сиюминутного чувства вашего превосходства такой способ общения существенно усложнит взаимодействие и только затянет решение проблемы.

Обучение системного администратора

Основную часть информации системный администратор сегодня черпает из Интернета, на специализированных форумах, в онлайн-базе знаний. Однако не следует пренебрегать и традиционными формами обучения, которые часто проводятся как подготовка по тому или иному курсу вендора.

Такие очные формы обучения полезны тем, что дают более общий взгляд на продукт, позволяют ознакомиться со всеми функциями программного обеспечения, а не только с теми, которые используются на практике в данной организации. Кроме того, преподаватели часто рассказывают об особенностях продукта, ошибках и ограничениях, о которых не пишут в рекламных документах и не сообщают на бесплатных презентациях. На таких курсах традиционно развернуты полигоны, где можно протестировать различные возможности программного обеспечения или оборудования.

Конечно, такой курс будет и не лишним с точки зрения соответствующей строчки в резюме.

Реализация изменений в информационной системе

Информационная система не может быть застывшей. Изменения в нее вносятся как по результатам исправления ошибок, так и в процессе планового развития. Традиционно процесс изменений включает в себя:

- планирование изменений;
- тестирование (если возможно);
- их реализацию;
- работу с изменениями, сбор информации о поведении системы;
- анализ информации, поиск и устранение ошибок в случае нестабильной работы.

Планирование изменений

Идеальным случаем является ситуация, когда изменения в системе являются штатными: они планируются заранее, тестируются по возможности и только после этого внедряются.

Если изменения касаются большинства систем, то их можно охарактеризовать уже как *критические*, поскольку их реализация может существенно осложнить функционирование бизнес-процессов.

Весь процесс изменений должен тщательно протоколироваться: от составления плана до фиксации всех операций. Часто бывает, что в случае возникновения проблем в работе администраторы предпринимают различные шаги по исправлению ошибок. Если к успеху не приводят одни настройки, то осуществляют другие и т. д. Выполненные настройки по исправлению забываются, считается, что они не повлияли на работу; ищутся новые исправления. В результате через некоторое время уже невозможно определить, какие операции повлияли на результат, и не удастся полностью отказаться от промежуточных настроек системы.

Поэтому надо взять за правило документировать каждый свой шаг: что сделано, почему, записать ссылки на использованные статьи базы знаний и т. п.

Другой важный совет: не менять сразу много за один раз. Лучше провести несколько операций изменения, чем совместить их все. Это может не только много раз сэкономить время администратора, но и когда-нибудь нарушить работу системы на длительный срок.

Конечно, план внедрения специфичен для каждой организации. Но можно отметить необходимость следующих позиций:

- организация тестирования изменений на полигоне (провести обновления и проверить корректность работы всей системы);
- подготовка плана отмены изменений;
- выбор времени для изменений;
- организация оповещения пользователей;
- отключение пользователей;

- осуществление обновлений;
- проверка корректности работы;
- подключение пользователей;
- проверка корректности работы;
- документирование проведенных операций, доработка шаблона плана внедрения изменений по выявленным проблемам.

Обратите внимание, что после внедрения изменений на следующий день администратор обязательно с самого утра должен быть доступен для пользователей, поскольку не исключена возможность выявления ошибок на этапе начала работы в системе. Кроме того, недоступность администратора в такой ситуации косвенно будет характеризовать его заинтересованность в успешном функционировании информационной системы.

Планирование момента изменений и продолжительности операций

Реализуемые изменения не должны мешать работе организации в случае возникновения проблем. В зависимости от критичности планируемых изменений время их внедрения может выбираться во время обеда, перед началом рабочего дня, в ночное время или выходные дни. При этом любые изменения системы должны быть исключены в периоды плановых отчетов, на время проведения (и подготовки) серьезных совещаний и т. п.

О планируемых изменениях пользователи должны быть предупреждены заблаговременно. Можно озвучить планируемые операции на совещаниях у руководителей подразделений, оповестить конечных пользователей по электронной почте и т. п. Не следует относиться к оформлению оповещений формально: например, если изменения проводятся часто, то сотрудники вряд ли будут читать сам текст письма, они обратят внимание только на его тему. Поэтому уже по ней должно быть понятно, кого коснутся изменения. А в самом тексте следует объяснять, зачем проводятся эти изменения и кого и как предупредить о возражениях (например, если у подразделения на этот период запланированы важные мероприятия).

Планируя внедрение изменений, обязательно нужно готовить планы откатов изменений. Следует учитывать, что ошибки могут быть замечены и через некоторое время. Например, если планируется внесение изменения в бухгалтерскую программу, то ошибки в формировании квартальных отчетов могут быть обнаружены в худшем случае через три месяца. И вам необходимо иметь возможность восстановить исходный вариант отчетов и внести в него все операции за эти три месяца.

Время на реализацию изменений должно быть запланировано (запрошено) с запасом и включать в себя не только время на непосредственное изменение, но и запас на откат в случае неудачи, некоторый период на анализ ситуации и т. п.

При оценке периода операции следует учесть все факторы. Например, если обновление требует перезагрузки сервера, то следует предусмотреть время для штатного закрытия программ, сохранения данных, для периода тестирования оборудования

при старте системы и т. п. Если обновление предполагается установить на все системы с последующей перезагрузкой, то должна быть учтена и последовательная очередность выключения и включения систем (сначала должны выключаться файловые серверы, в последнюю очередь — серверы аутентификации и оборудование, обеспечивающее подключение к другим сетям, включение следует выполнять в обратной последовательности). Возможны и другие ситуации, которые нужно учитывать. Например, включение системы хранения данных (СХД) с одновременной раскруткой большого количества жестких дисков приводит к большой нагрузке на источники питания. А это может вызвать просадку напряжения и, возможно, сбои в работе другого оборудования. Поэтому резонно выделить некоторый период времени на включение СХД, во время которого не включать никакого другого оборудования.

Системный администратор как продавец ИТ-технологий

Системный администратор не является лицом, распределяющим финансовые ресурсы. Обычно на предприятиях подобные решения принимаются ИТ-директорами, в подчинении у которых находятся системные администраторы. Объективно как финансовые руководители, так и ИТ-директора не разбираются в тонкостях информационной системы и часто основывают свои решения на советах тех людей, которым они доверяют, например, сына, любящего посещать компьютерные клубы, или друга, которого считают специалистом ИТ. Или, что еще хуже, с позиций поддержки фирм, в которых работают родственники и знакомые. Без реального представления проблем, которые решаются при работе информационных систем.

Системным администраторам нужно приспосабливаться к такой ситуации. Без поддержки финансовых руководителей, ИТ-директоров, без нахождения компромиссов развитие ИТ-структуры будет неоптимальным. Системные администраторы должны поддерживать руководителей, обучать их, чаще посвящать в свои проблемы. Пытаться донести проблемы до руководителя в понятных ему терминах.

Системное администрирование обычно рассматривается только с точки зрения расходования бюджета. Но в тот момент, когда руководитель начинает понимать эффективность своих решений на практике и может оценить экономический эффект от работы системного администратора, а это происходит в случае ухудшения показателей основного бизнеса из-за проблем с работой инфраструктуры, служб и т. п., работа системных администраторов уже развалена, и службу приходится воссоздавать заново.

Чтобы не доводить информационную систему до критических показателей, системному администратору надо становиться *продавцом информационных технологий*. Он должен искать аргументы для обоснования выделения средств на поддержание и развитие системы. Желательно при этом опираться на независимые цифры. Например, на стоимость внешних контрактов, на количество обращений, зафиксиро-

рованных службой поддержки, на планы роста числа пользователей, отраженные в бизнес-планах предприятия, и т. д. Для этого нужно знать и свою статистику (например, количество предотвращенных сетевых атак), и тенденции в мире, решения у конкурентов... Если говорить коротко, то нужно показать, что конкретное вложение средств в ИТ-структуру отвечает *интересам руководителя*.

На практике используются два варианта финансирования: централизованное (содержание группы администраторов) и финансирование за счет отдельных проектов. Каждый вариант имеет свои преимущества и недостатки, но в любом случае требуются тщательно проработанные уровни обслуживания и контроль качества (чтобы при лучшем обслуживании группе системных администраторов выделялось больше средств, а руководители бизнеса в случае дополнительного финансирования могли ожидать улучшения качества обслуживания).

Учитывать человеческие особенности

Деятельность администратора по управлению системой не должна ухудшать комфортность работы пользователей. Поверьте, что через некоторое время пользователи все равно найдут способ, как обойти введенные администратором ограничения. А поскольку такие обходные пути менее безопасны и потенциально более рискованны, то они могут привести и к более серьезным отказам. Формально нарушение в таких случаях будет сделано самими пользователями, но первопричиной его фактически явится ваша политика.

Поэтому лучше так регулировать правила и ограничения, чтобы обеспечить необходимый уровень безопасности и надежности без существенных изменений принятой практики (если, конечно, такое возможно).

Быть в курсе

Системный администратор (руководитель группы администраторов) не должен замыкаться в проблемах информационной системы. Он должен знать приоритеты бизнеса и соответствующим образом планировать свою работу, в том числе заранее вносить предложения по изменению структуры (по созданию новых рабочих мест, в части организации работы сотрудников на дому, подключения филиалов и т. п.). Должны быть налажены отношения со специалистами юридической и кадровой служб предприятия.

Следует выделять время на участие в конференциях и семинарах. Обязательно подписаться на различные специализированные рассылки. И, естественно, не забывать и о самообразовании.

И не заблуждайтесь, считая, что все знают, например, о ваших планах модернизации информационной системы. Или о планируемых настройках. Чаще рассказывайте людям о своих намерениях, пытайтесь сделать пользователей своими сторонниками. Ну а если не можете перебороть себя, то хотя бы публикуйте минимальный объем информации на корпоративном сайте.

Ошибки администратора

От ошибок никто не застрахован. Не нужно скрывать их, как и не стоит наказывать подчиненных администраторов за неверные действия. Жестко придерживайтесь только одного правила: о возникновении проблемы должны быть оперативно проинформированы заинтересованные лица.

Чаще советуйтесь. Мнение собеседника, даже если он не является специалистом по данной проблеме, может подтолкнуть вас к решению совершенно с неожиданной стороны.

Старайтесь фиксировать все свои действия по настройке системы и соответствующие указания начальников. Если сомневаетесь в чем-то (например, в каком-то указании начальника), попытайтесь получить письменное подтверждение (по электронной почте и т. п.).

Инструкции и контрольные листы

Инструкции позволяют описать последовательность выполнения операций (например, по установке операционной системы в конфигурации конкретного отдела) и добиться идентичности результатов работы для различных специалистов. Удобно, если инструкции будут снабжены контрольными листами (обычно их принято называть *check*-листами), в которых будут последовательно перечислены все необходимые шаги. После изучения инструкции даже не совсем опытному администратору для выполнения операций достаточно будет только использовать контрольные листы, чтобы не пропустить какой-либо важный шаг в настройке системы.

Кроме того, заполненный контрольный лист является хорошим вариантом отчетности о выполненной работе. Особенно использование контрольных листов важно при выполнении серьезных изменений. Сам факт наличия контрольного листа уже будет свидетельствовать о том, что к предстоящим операциям была проведена серьезная подготовка.

Полномочия системного администратора

Фиксация полномочий и обязанностей системного администратора поможет снять многие претензии и оговорить условия выполнения специальных работ.

Так, желательно зафиксировать в соответствующих документах следующие параметры:

- четко определить обязанности, например, указать, что администраторы не поддерживают чужое ПО, самостоятельно установленное пользователем;
- распределить обязанности (если поддержку системы выполняют несколько специалистов): кто отвечает за установку ПО, кто решает проблемы сети, кто поддерживает пользователей данного подразделения и т. п.;
- определить особенности поддержки мобильных пользователей, работ на выставках, организуемых предприятием, и т. п.;