

Оглавление

Вступление	11
Предисловие	14
Условные обозначения	16
Использование примеров кода	16
Благодарности	17
От издательства	19
Глава 1. Введение	20
История BPF	22
Архитектура.....	24
Резюме	26
Глава 2. Запуск программ BPF	27
Написание программ BPF	28
Типы программ BPF	31
Программы сокетной фильтрации.....	32
Программы kprobe	32
Программы трассировки	33
Программы XDP	33
Программы Perf Event.....	34
Программы для сокетов контрольных групп	34

Программы Cgroup Open Socket	35
Дополнительные программы для сокетов.....	35
Программы карт в соquete	36
Программы для устройств контрольных групп	36
Программы доставки сообщений через сокет.....	37
Программы для доступа к необработанным точкам трассировки	37
Адресные программы сокетов контрольных групп.....	37
Сокетные программы повторного использования портов	38
Программы разделения потока.....	38
Другие программы BPF.....	39
Верификатор BPF	39
Формат типа BPF	42
Оконечные вызовы BPF	42
Резюме.....	43
Глава 3. Карты BPF	44
Создание карт BPF	45
Соглашения ELF для создания карт BPF	46
Работа с картами BPF	47
Обновление элементов в карте BPF.....	47
Считывание элементов из карты BPF	50
Удаление элемента из карты BPF.....	52
Перебор элементов в карте BPF	53
Поиск и удаление элементов	55
Конкурентный доступ к элементам карты.....	56
Типы карт BPF	58
Карты хеш-таблиц	59
Карты массивов	60
Карты программных массивов	61
Карты массивов событий производительности	62
Хеш-карты для каждого процессора	64
Карты массивов для каждого процессора	64
Карты трассировки стека	64
Карты массива контрольной группы	64

Хеш-карты LRU и хеш-карты отдельных процессоров.....	65
Карты LPM Trie.....	66
Массив карт и хеш-карт.....	67
Карты устройств.....	67
Карты процессоров.....	68
Карты открытого сокета	68
Карты массива и хеша сокета.....	68
Карты сохранения sgrou и сохранения по ЦПУ	68
Карты переиспользования сокетного порта.....	69
Карты очередей.....	69
Карты стека.....	71
Виртуальная файловая система BPF	72
Резюме.....	75
Глава 4. Трассировка с помощью BPF	77
Зонды.....	78
Зонды ядра	79
Точки трассировки.....	82
Зонды пользовательского пространства.....	84
Статические точки трассировки пользовательского пространства	89
Визуализация данных трассировки.....	94
Флейм-графы	95
Гистограммы.....	101
События Perf.....	104
Резюме.....	107
Глава 5. Утилиты BPF	108
BPFTool	108
Установка.....	109
Вывод функциональных возможностей	109
Инспекция программ BPF.....	110
Инспекция карт BPF	115
Инспекция программ, подключенных к определенным интерфейсам	117
Загрузка команд в пакетном режиме	118

Отображение информации BTF	120
BPFTrace	120
Установка.....	121
Справочник по языку	121
Фильтрация	123
Динамическое отображение.....	124
kubectl-trace	125
Установка.....	125
Инспекция узлов Kubernetes.....	126
eBPF Exporter	127
Установка.....	127
Экспорт метрик из BPF	128
Резюме.....	129
Глава 6. Сетевое взаимодействие в Linux и BPF	131
BPF и фильтрация пакетов.....	132
Выражения tcpdump и BPF.....	133
Фильтрация пакетов для сырых сокетов.....	138
Классификатор управления трафиком на основе BPF	145
Терминология	146
Программа классификатора управления трафиком с использованием cls_bpf	150
Различия между управлением трафиком и XDP	156
Резюме.....	157
Глава 7. Express Data Path.....	158
Обзор программ XDP	159
Режимы работы	160
Пакетный процессор.....	162
XDP и iproute2 в качестве загрузчика.....	166
XDP и BCC.....	172
Тестирование программ XDP	175
XDP-тестирование с использованием фреймворка Python для тестирования модулей.....	176

Варианты использования XDP	182
Мониторинг	182
Миграция DDoS.....	182
Балансировка нагрузки.....	183
Брандмауэры	183
Резюме	184
Глава 8. Безопасность ядра Linux, его возможности и Seccomp	185
Возможности.....	185
Seccomp	189
Ошибки Seccomp.....	191
Пример фильтра BPF Seccomp	192
Ловушки BPF LSM.....	197
Резюме.....	198
Глава 9. Реальные способы применения	199
Режим God Mode от Sysdig eBPF	199
Flowmill.....	203
Об авторах	206
Об обложке.....	207