

深入理解JVM字节码



资深系统工程师、上市公司高级技术经理，掘金平台优秀作者撰写，多位行业专家联袂推荐
从原理和应用两个维度深入剖析字节码，揭示其在Java性能优化、软件破解、APM等各科应用领域的“黑科技”



深入理解 JVM字节码

Dive into JVM Bytecode

张亚 著



[深入理解JVM字节码_下载链接1](#)

著者:张亚

出版者:机械工业出版社

出版时间:2020-5

装帧:平装

isbn:9787111653721

这是一本揭示JVM字节码“黑科技”的著作，它从原理和应用两个维度深入剖析了JVM字节码。书中内容涉及JVM字节码的大部分应用场景，如Java性能优化、软件防护与破解、APM等，通过大量实战案例讲解了它在这些场景中的实操技巧。

本书共 12 章，从逻辑上分为两大部分。

第一部分：原理篇（第1~8章）

第1章详细剖析了class文件的内部结构；第2章介绍了字节码的概念以及Java虚拟机栈和栈帧的相关内容；第3章介绍了字节码的进阶知识，包括泛型擦除、synchronized关键字、反射的底层实现原理；第4章介绍了javac编译器的原理，以及javac编译的七大阶段和各阶段的作用；第5章从字节码的角度介绍Kotlin的常见语法糖、coroutine等原理；第6章介绍了ASM和Javassist这两个字节码操作工具；第7章介绍了Java Instrumentation的原理；第8章介绍了JSR 269插件化注解处理原理。

第二部分：应用篇（第9~12章）

第9章介绍了字节码在cglib、Fastjson等框架上的应用；第10章介绍了反编译、破解、防破解和逆向工程的相关内容；第11章介绍了APM的概况、分布式跟踪的基本原理等；第12章详细介绍了Android dex文件的组成结构，以及Android字节码指令与Java字节码指令的区别。

作者介绍:

张亚

资深后端工程师和Java工程师，CVTE（视源股份，股票代码：002841）高级技术经理，带领20多人的研发团队做教育相关的产品。

主要技术方向是JVM调优及故障诊断、TCP源码剖析、高并发系统设计，致力于后端底层技术细节的研究。独立实现了公司级全链路APM产品，在字节码、ASM、软件破解等方向有丰富的实战经验。

vim狂热爱好者，热衷分享，是掘金平台的优秀作者，在掘金上撰写过两本关于JVM和TCP底层原理的小册子。

目录: 前言

第1章 深入剖析 class 文件结构 1

1.1 初探 class 文件 1

1.2 class 文件结构剖析 3

1.2.1 魔数 4

1.2.2 版本号 6

1.2.3 常量池 7

1.2.4 Access flags 18

1.2.5 this_class、super_name、interfaces 19

1.2.6 字段表 20

1.2.7 方法表 23

1.2.8 属性表 25

1.3 使用 javap 查看类文件 30

1.4 小结 32

第2章 字节码基础 33

2.1 字节码概述 33

- 2.2 Java 虚拟机栈和栈帧 34
- 2.3 字节码指令 41
 - 2.3.1 加载和存储指令 41
 - 2.3.2 操作数栈指令 42
 - 2.3.3 运算和类型转换指令 45
 - 2.3.4 控制转移指令 46
 - 2.3.5 for语句的字节码原理 48
 - 2.3.6 switch-case底层实现原理 54
 - 2.3.7 String的switch-case实现的字节码原理 55
 - 2.3.8 ++i和i++的字节码原理 60
 - 2.3.9 try-catch-finally的字节码原理 63
 - 2.3.10 try-with-resources 的字节码原理 71
 - 2.3.11 对象相关的字节码指令 74
- 2.4 小结 77
- 第3章 字节码进阶 78
 - 3.1 方法调用指令 78
 - 3.1.1 invokestatic指令 79
 - 3.1.2 invokevirtual指令 79
 - 3.1.3 invokespecial指令 80
 - 3.1.4 invokeinterface指令 80
 - 3.1.5 invokedynamic指令 90
 - 3.2 Lambda 表达式的原理 95
 - 3.3 泛型与字节码 100
 - 3.4 synchronized 的实现原理 102
 - 3.5 反射的实现原理 106
 - 3.5.1 反射方法源码分析 107
 - 3.5.2 反射的inflation机制 109
 - 3.6 小结 110
- 第4章 javac 编译原理简介 111
 - 4.1 javac 源码调试 112
 - 4.2 javac 的七个阶段 114
 - 4.2.1 parse阶段 115
 - 4.2.2 enter阶段 116
 - 4.2.3 process阶段 118
 - 4.2.4 attr阶段 118
 - 4.2.5 flow阶段 121
 - 4.2.6 desugar阶段 122
 - 4.2.7 generate阶段 126
 - 4.3 小结 129
- 第5章 从字节码角度看 Kotlin语言 130
 - 5.1 Metadata 注解 130
 - 5.2 顶层方法 132
 - 5.3 object 单例 133
 - 5.4 扩展方法 134
 - 5.5 接口默认方法 135
 - 5.6 默认参数 137
 - 5.7 高级 for 循环 140
 - 5.8 data class 142
 - 5.9 多返回值 143
 - 5.10 协程的实现原理 144
 - 5.10.1 CPS 介绍 145
 - 5.10.2 suspend 关键字 146
 - 5.11 从字节码分析 Kotlin 编译器的bug 149
 - 5.12 小结 153

第6章 ASM 和 Javassist 字节码操作工具	154
6.1 ASM 介绍	154
6.1.1 ASM Core API核心类	156
6.1.2 ASM操作字节码示例	158
6.2 Javassist 介绍	169
6.2.1 Javassist核心API	169
6.2.2 Javassist操作字节码示例	170
6.3 小结	174
第7章 Java Instrumentation 原理	175
7.1 Java Instrumentation 简介	175
7.2 Instrumentation 与 -javaagent启动参数	176
7.3 JVM Attach API 介绍	180
7.3.1 JVM Attach API基本使用	181
7.3.2 JVM Attach API的底层原理	183
7.4 小结	190
第8章 JSR 269 插件化注解处理原理	191
8.1 JSR 269 简介	191
8.2 抽象语法树操作 API	193
8.2.1 Names介绍	193
8.2.2 JCTree介绍	193
8.2.3 TreeMaker介绍	198
8.2.4 自定义注解处理实战	202
8.3 JSR 269 在常用框架上的应用	207
8.3.1 案例一：ButterKnife	207
8.3.2 案例二：Lombok	209
8.4 小结	212
第9章 字节码的应用	213
9.1 cglib 动态代理原理分析	213
9.1.1 cglib核心API介绍	214
9.1.2 cglib原理分析	216
9.2 字节码在 Fastjson 上的应用	218
9.3 字节码在 Dubbo 上的应用	221
9.4 字节码在 JaCoCo 代码覆盖率上的应用	222
9.5 字节码在 Mock 上的应用	225
9.6 小结	227
第10章 软件破解和防破解	228
10.1 反编译	228
10.2 软件破解	229
10.2.1 破解方式一：直接修改class文件	230
10.2.2 破解方式二：javaagent无痛破解	232
10.3 软件防破解	234
10.3.1 自定义ClassLoader	234
10.3.2 JNI隐藏核心逻辑	237
10.3.3 基于JVMTI的加密方案	239
10.3.4 混淆	245
10.4 小结	250
第11章 全链路分布式跟踪与APM	251
11.1 全链路分布式跟踪介绍	251
11.1.1 什么是全链路分布式跟踪	252
11.1.2 OpenTracing基本术语	253
11.1.3 分布式跟踪的实现和上下文传递	254
11.2 见微知著之 APM	260
11.2.1 APM基本概念	260
11.2.2 APM的字节码注入实现	261

- 11.2.3 其他平台的APM实现 272
- 11.3 小结 273
- 第12章 Android字节码与 APM 274
- 12.1 dex 文件结构 274
 - 12.1.1 header 276
 - 12.1.2 string_ids 278
 - 12.1.3 type_ids 280
 - 12.1.4 proto_ids 281
 - 12.1.5 field_ids 282
 - 12.1.6 method_ids 283
 - 12.1.7 class_defs 284
 - 12.1.8 data 288
 - 12.1.9 link_data 288
- 12.2 Android字节码 288
 - 12.2.1 Android字节码概述 288
 - 12.2.2 常见的字节码指令介绍 289
- 12.3 Gradle 插件编写 295
 - 12.3.1 自定义Gradle插件 295
 - 12.3.2 独立的 Gradle 插件项目 296
- 12.4 Android字节码注入原理 297
 - 12.4.1 Transform API介绍 297
 - 12.4.2 字节码注入代码实现 299
- 12.5 小结 301
- • • • • [\(收起\)](#)

[深入理解JVM字节码 下载链接1](#)

标签

jvm

JVM

编程

计算机

最新版

评论

本以为几页劝退，没想到写的挺不错的，对invoke指令的描述简单明了，对kotlin的协程和cps也是见过的最简单清晰的解释。虽然内容有点杂，赞一个

对JVM底层知识的讲解很透彻，值得好好读一读！推荐

总体很不错,只是没有对技术进行分类和解释,技术之间的联系和区别有些困惑,对java本身理解更深入了,后面的分布式链路讲的有点简单,总体是很有诚意的一本书

结合实践，内容很干

之前看过掘金小册子，写的很系统，容易理解。决定再买本书研究一番。

厉害了

五星好评，值得推荐

7分吧。前面讲解jvm字节码基础知识还不错，后面的工具和应用章节有点一笔带过，太简略了

[深入理解JVM字节码_下载链接1](#)

书评

书的前面几章内容很详细，配图丰富，后面质量明显没有前面高。

从书中的几处错误看出本书的作者没有对相关的技术做非常深入的探究于理解。

.....

[深入理解JVM字节码_下载链接1](#)