

WaitXie
<http://blog.sina.com.cn/waitxie> [订阅] [手机订阅]

[首页](#) [博文目录](#) [图片](#) [关于我](#)

个人资料

正文

字体大小：大 中 小



ustcxxw


Qing


加好友
写留言

博客等级：
博客积分：720
博客访问：33,000
关注人气：16
荣誉徽章：

谁读书才能涨姿势？

新浪博客APP告诉你！





新浪博客客户端
扫一扫下载



卖得不贵，穿得高贵
简约 时尚 休闲

精彩图文

zz qemu源码架构 (2012-11-21 08:52:06) 转 载 ▼

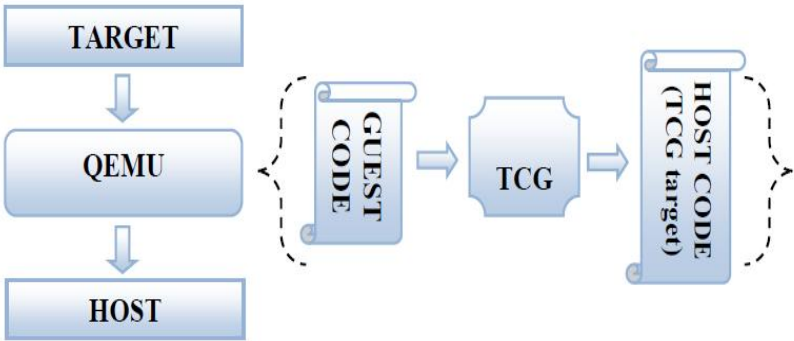
标签： 开源 虚拟机 育儿 分类： 开源工具

前言：本文主要概括了QEMU的代码结构，特别从代码翻译的角度分析了QEMU是如何将客户机代码翻译成TCG代码和主机代码并且最终执行的过程。并且在最后描述了QEMU和KVM之间联系的纽带。

申明：本文前面部分从qemu detailed study第七章翻译而来。

1.代码结构

如我们所知，QEMU是一个模拟器，它能够动态模拟特定架构的CPU指令，如X86，PPC，ARM等等。QEMU模拟的架构叫目标架构，运行QEMU的系统架构叫主机架构，QEMU中有一个模块叫做微型代码生成器（TCG），它用来将目标代码翻译成主机代码。如下图所示。



我们也可以将运行在虚拟cpu上的代码叫做客户机代码，QEMU的主要功能就是不断提取客户机代码并且转化成主机指定架构的代码。整个翻译任务分为两个部分：第一个部分是将做目标代码（TB）转化成TCG中间代码，然后再将中间代码转化成主机代码。

QEMU的代码结构非常清晰但是内容非常复杂，这里先简单分析一下总体的结构

1. 开始执行：

主要比较重要的c文件有：/vl.c/cpus.c, /exec-all.c, /exec.c, /cpu-exec.c.

QEMU的main函数定义在/vl.c中，它也是执行的起点，这个函数的功能主要是建立一个虚拟的硬件环境。它通过参数的解析，将初始化内存，需要的模拟的设备初始化，CPU参数，初始化KVM等等。接着程序就跳转到其他的执行分支文件如：/cpus.c, /exec-all.c, /exec.c, /cpu-exec.c.

2. 硬件模拟

所有的硬件设备都在/hw/ 目录下面，所有的设备都有独自的文件，包括总线，串口，网卡，鼠标等等。它们通过设备模块串在一起，在vl.c中的machine_init中初始化。这里就不讲每种设备是怎么实现的了。

3.目标机器

现在QEMU模拟的CPU架构有：Alpha, ARM, Cris, i386, M68K, PPC, Sparc, Mips, MicroBlaze, S390X and SH4.



爸爸2蒙古站花絮抢先看



张亮洗剪吹雷照



周慧敏依林闹小孩



周立波涉黄真相



王菲蔡依林闹翻



女星事业线PK



郑中基嫖娼染病

[查看更多>>](#)



炜盛厂家直销燃气模块

¥18.00/PCS

相关博文

博导引诱女学生开房步骤让人大开帝国良民

教师灌学生堕胎药（高清图组）微游戏

7.14早盘：周一走势与操盘占豪

徐小明：本周会不会是反弹终结徐小明

高中生：被30岁已婚男一吻征夏季紫罗兰

林毅夫、张维迎先生之争让人失叶檀

按摩强肾的6大技巧董路的健康快车

我舰船在钓鱼岛出大事了：船员客居据点

俄罗斯美女为何热衷夜店相亲木子李

揭秘十大当红绝色女星首次作品李守智

我们在QEMU中使用./configure 可以配置运行的架构，这个脚本会自动读取本机真实机器的CPU架构，并且编译的时候就编译对应架构的代码。对于不同的QEMU做的事情都不同，所以不同架构下的代码在不同的目录下。/target-arch/目录就对应了相应架构的代码，如/target-i386/就对应了x86系列的代码部分。虽然不同架构做法不同，但是都是为了实现将对应客户机CPU架构的TBs转化成TCG的中间代码。这个就是TCG的前半部分。

4.主机

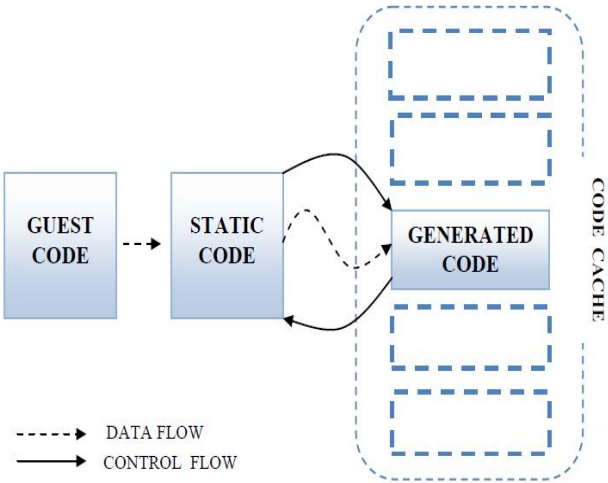
这个部分就是使用TCG代码生成主机的代码，这部分代码在/tcg/里面，在这个目录里面也对应了不同的架构，分别在不同的子目录里面，如i386就在/tcg/i386中。整个生成主机代码的过程也可以教TCG的后半部分。

5.文件总结和补充：

- /vl.c: 最主要的模拟循环，虚拟机机器环境初始化，和CPU的执行。
- /target-arch/translate.c 将客户机代码转化成不同架构的TCG操作码。
- /tcg/tcg.c 主要的TCG代码。
- /tcg/arch/tcg-target.c 将TCG代码转化生成主机代码
- /cpu-exec.c 其中的cpu-exec()函数主要寻找下一个TB（翻译代码块），如果没找到就请求得到下一个TB，并且操作生成的代码块。

2. TCG - 动态翻译

QEMU在 0.9.1版本之前使用DynGen翻译c代码.当我们需要的时候TCG会动态的转变代码，这个想法的目的是用更多的时间去执行我们生成的代码。当新的代码从TB中生成以后， 将会被保存到一个cache中，因为很多相同的TB会被反复的进行操作，所以这样类似于内存的cache，能够提高使用效率。而cache的刷新使用LRU算法。



编译器在执行器会从源代码中产生目标代码，像GCC这种编译器，它为了产生像函数调用目标代码会产生一些特殊的汇编目标代码，他们能够让编译器需要知道在调用函数。需要什么，以及函数调用以后需要返回什么，这些特殊的汇编代码产生过程就叫做函数的Prologue和Epilogue，这里就叫前端和后段吧。我在其他文章中也分析过汇编调用函数的过程，至于汇编里面函数调用过程中寄存器是如何变化的，在本文中就不再描述了。

函数的后端会恢复前端的状态，主要做下面2点：

1. 恢复堆栈的指针，包括栈顶和基地址。
2. 修改cs和ip，程序回到之前的前端记录点。

TCG就如编译器一样可以产生目标代码，代码会保存在缓冲区中，当进入前端和后端的时候就会将TCG生成的缓冲代码插入到目标代码中。

接下来我们就来看下如何翻译代码的：

客户机代码

超级萌娃王诗龄与20位当红明星
虫哥818

女人性高潮的7大杀手
健康之路-小米

更多>>

推荐资讯

初高中这样学 考不到600分就怪了
初中 高中正确学习方法 成绩提升

状元学习法：快速提高成绩！
百万家长推荐 教会孩子正确学习

写字难看？写一手漂亮字仅需21天
签字有面子,考试拿高分,孩子的榜

就读航空名校 毕业捧上金饭碗！
十大国办航空院校招生（初高中毕

新浪专业教育考试服务平台
出国留学、商学院、外语、教育等

推荐博文

写给儿子：十周岁生日信！
维尼小熊

宝贝异国友谊的烦恼事
promontory

婚姻需要经营
重庆人在纽约

暑假零食之开心果饼干
李子宝宝

夏日里像风一样的女子
零落妈妈

带五岁女儿游荷兰(原创)
闫晓苹

漂流瓶引来的可耻换女友事件
依恋妳

粗心奶爸独自带娃主妇忧思成疾
jimmy宝贝儿

老公竟然将怀孕小三领进门逼我让
哥比男模帅

“蜜罐娃”太胆小老妈要抓狂
我心依然dd



新妈妈如何调整自己的心.



做游戏老师撞疼孩子要不.



当海少首次遇上牌局



二年级：空气动力第二堂课

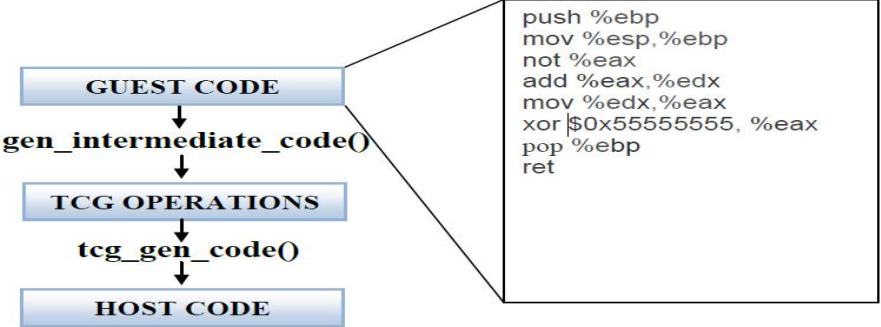


蜜月才刚开始的孕期生活

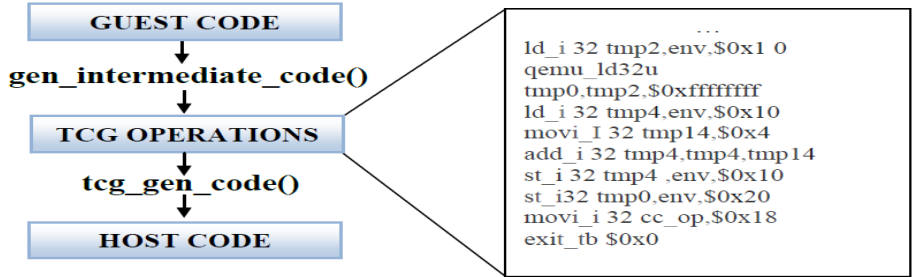


四年级下学期的收获和总.

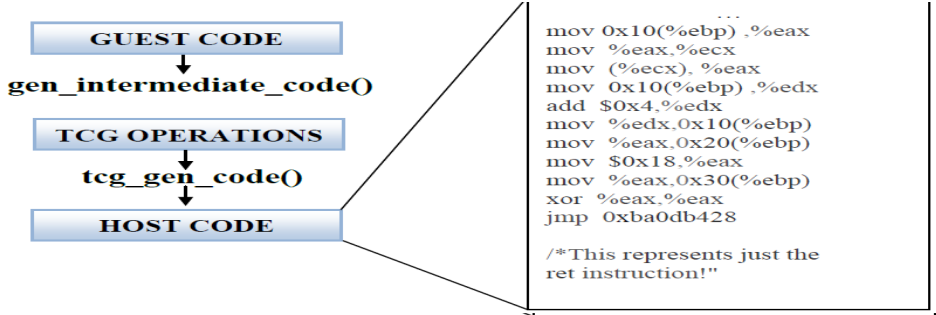
查看更多>>



TCG中间代码

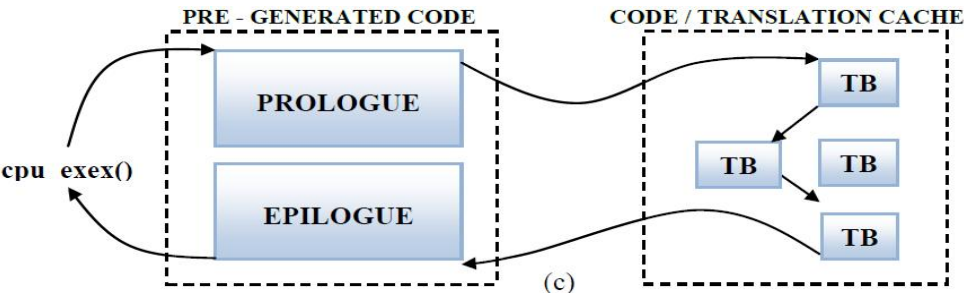


主机代码



3. TB链

在QEMU中，从代码cache到静态代码再回到代码cache，这个过程比较耗时，所以在QEMU中涉及了一个TB链。将所有TB连在一起，可以让一个TB执行完以后直接跳到下一个TB，而不用每次都返回到静态代码部分。具体过程如下图：



4. QEMU的TCG代码分析

接下来看看QEMU代码中到底怎么来执行这个TCG的，看看它是如何生成主机代码的。

main_loop(...){/vl.c} :

函数main_loop 初始化qemu_main_loop_start()然后进入无限循环cpu_exec_all()，这个是QEMU的一个主要循环，在里面会不断的判断一些条件，如虚拟机的关机断电之类的。

qemu_main_loop_start(...){/cpus.c} :

函数设置系统变量 qemu_system_ready = 1并且重启所有的线程并且等待一个条件变量。

cpu_exec_all(...){/cpus.c} :

推荐过这篇博文	
wzw0114	0分钟前
丁尼奥	6月10日
冬儿	4月14日
zhoutao_t...	4月12日
terenceli	4月4日
小缪	3月21日
wjwjwj	3月4日
zhaosj027	3月1日
dahai123	2月22日
有效证书	1月14日
随同个人	1月7日
define	11月16日



它是cpu循环，QEMU能够启动256个cpu核，但是这些核将会分时运行，然后执行qemu_cpu_exec()。

struct CPUState{target-xyz/cpu.h} :

它是CPU状态结构体，关于cpu的各种状态，不同架构下面还有不同。

cpu_exec(...){/cpu-exec.c}:

这个函数是主要的执行循环，这里第一次翻译之前说道德TB，TB被初始化为(TranslationBlock *tb)，然后不停的执行异常处理。其中嵌套了两个无限循环 find tb_find_fast() 和tcg_qemu_tb_exec()。

cantb_find_fast()为客户机初始化查询下一个TB，并且生成主机代码。

tcg_qemu_tb_exec()执行生成的主机代码

struct TranslationBlock {/exec-all.h}:

结构体TranslationBlock包含下面的成员：PC, CS_BASE, Flags（表明TB），tc_ptr（指向这个TB翻译代码的指针），tb_next_offset[2], tb_jump_offset[2]（接下去的Tb），*jmp_next[2], *jmp_first（之前的TB）。

tb_find_fast(...){/cpu-exec.c} :

函数通过调用获得程序指针计数器，然后传到一个哈希函数从 tb_jump_cache[]（一个哈希表）得到TB的所以，所以使用tb_jump_cache可以找到下一个TB。如果没有找到下一个TB，则使用tb_find_slow。

tb_find_slow(...){/cpu-exec.c}:

这个是在快速查找失败以后试图去访问物理内存，寻找TB。

tb_gen_code(...){/exec.c}:

开始分配一个新的TB，TB的PC是刚刚从CPUstate里面通过using get_page_addr_code()找到的

phys_pc = get_page_addr_code(env, pc);

tb = tb_alloc(pc);

ph当调用cpu_gen_code()以后，接着会调用tb_link_page()，它将增加一个新的TB，并且指向它的物理页表。

cpu_gen_code(...){/translate-all.c}:

函数初始化真正的代码生成，在这个函数里面有下面的函数调用：

gen_intermediate_code(){/target-arch/translate.c}->gen_intermediate_code_internal(){/target-arch/translate.c }->disas_insn(){/target-arch/translate.c }

disas_insn(){/target-arch/translate.c}

函数disas_insn() 真正的实现将客户机代码翻译成TCG代码，它通过一长串的switch case，将不同的指令做不同的翻译，最后调用tcg_gen_code。

tcg_gen_code(...){/tcg/tcg.c}:

这个函数将TCG的代码转化成主机代码，这个就不细细说明了，和前面类似。

#define tcg_qemu_tb_exec(...){/tcg/tcg.g}:

通过上面的步骤，当TB生成以后就通过这个函数进行执行。

next_tb = tcg_qemu_tb_exec(tc_ptr) :

extern uint8_t code_gen_prologue[];

#define tcg_qemu_tb_exec(tb_ptr) ((long REGPARAM*)(void *)) code_gen_prologue(tb_ptr)

通过上面的步骤我们就解析了QEMU是如何将客户机代码翻译成主机代码的，了解了TCG的工作原理。接下来看看QEMU与KVM是怎么联系的。

5. QEMU中的IOCTL

在QEMU-KVM中，用户空间的QEMU是通过IOCTL与内核空间的KVM模块进行通讯的。

1. 创建KVM

在/vl.c中通过kvm_init()将会创建各种KVM的结构体变量，并且通过IOCTL与已经初始化好的KVM模块进行通讯，创建虚拟机。然后创建VCPU，等等。

2. KVM_RUN

这个IOCTL是使用最频繁的，整个KVM运行就不停在执行这个IOCTL，当KVM需要QEMU处理一些指令和IO等的时候就会退出通过这个IOCTL退回到QEMU进行处理，不然就会一直在KVM中执行。

它的初始化过程：

vl.c中调用machine->init初始化硬件设备接着调用pc_init_pci，然后再调用pc_init1。

接着通过下面的调用初始化KVM的主循环，以及CPU循环。在CPU循环的过程中不断的执行KVM_RUN与KVM进行交互。

pc_init1->pc_cpus_init->pc_new_cpu->cpu_x86_init->qemu_init_vcpu->kvm_init_vcpu->ap_main_loop->kvm_main_loop_cpu->kvm_cpu_exec->kvm_run

3.KVM_IRQ_LINE

这个IOCTL和KVM_RUN是不同步的，它也是个频率非常高的调用，它就是一般中断设备的中断注入入口。当设备有中断就通过这个IOCTL最终调用KVM里面的kvm_set_irq将中断注入到虚拟的中断控制器。在kvm中会进一步判断属于什么中断类型，然后在合适的时机写入vmcs。当然在KVM_RUN中会不断的同步虚拟中断控制器，来获取需要注入的中断，这些中断包括QEMU和KVM本身的，并在重新进入客户机之前注入中断。

总结: 通过这篇文章能够大概的了解QEMU的代码结构，其中主要包括TCG翻译代码的过程以及QEMU和KVM的交互过程。

0

喜欢

分享：

阅读(267) | 评论 (8) | 收藏(0) | 转载(0) | 喜欢 ▼ | 打印 | 举报

已投稿到： 排行榜 圈子

前一篇：zz Linux内核如何进行读取和写入文件等操作

后一篇：zz@mitbbs 做Research的体会

评论 重要提示：警惕虚假中奖信息 [发评论]

合肥土鳖

你搞虚拟化？

2012-11-21 08:55 来自 合肥土鳖 的评论 回复(0)

Wait_Xie-ustc

回复 @合肥土鳖 :对的 qq有什么建议么？

2012-11-21 20:56 来自 Wait_Xie-ustc 的评论 回复(0)

合肥土鳖

木有。。。我只是用虚拟化软件，kvm xen之类的

2012-11-21 21:58 来自 合肥土鳖 的评论 回复(0)

Wait_Xie-ustc

reply @合肥土鳖 :你是做实验用?还是? 你知道怎么样在host上读取guest vm的文件么? 或者得到file指针?

2012-11-22 06:08 来自 Wait_Xie-ustc 的评论 回复(0)

合肥土鳖

回复 @Wait_Xie-ustc :我们是用libvirt库来对虚拟机进行相关操作的（创建 重启等），libvirt是个开源库支

持许多虚拟化软件，比如kvm xen openvz等

2012-11-22 08:49 来自 合肥土鳖 的评论 回复(0)

Wait_Xie-ustc

回复 @合肥土鳖 :libvirt 我看了一下。我问你的东西 你好像也没接触过去你们实验室有人弄这个么？

2012-11-22 09:40 来自 Wait_Xie-ustc 的评论 回复(0)

合肥土鳖

回复 @Wait_Xie-ustc :嗯，我做的项目是云计算的IaaS，我们实验室好像木有人弄这个。。guest vm在主机上是个镜像文件，然后把镜像文件mount到一个loop设备，然后去读vm内部文件？

2012-11-22 09:44 来自 合肥土鳖 的评论 回复(0)


Wait_Xie-ustc


reply @合肥土鳖 :嗯 就是一个镜像文件 想获取里面的文件结构。


2012-11-22 22:31 来自 Wait_Xie-ustc 的评论 回复(0)


发评论


wzw0114：您还未开通博客，点击一秒开通。




















☒ 分享到微博 ☐ 评论并转载此博文 ☐ 匿名评论

验证码： 请点击后输入验证码 收听验证码

发评论

以上网友发言只代表其个人观点，不代表新浪网的观点或立场。

< 前一篇

zz Linux内核如何进行读取和写入文件等操作

后一篇 >

zz@mitbbs 做Research的体会