

QEMU设备模拟

原创 tycoon1988 最后发布于2015-04-18 20:34:10 阅读数 1732 ☆ 收藏

备模拟目的

我们好像不会干一件事而毫无目的，就算不停刷微信朋友圈也是为了打发你无聊的时间。

其实最装B的回答是：设备模拟的目的就是模拟设备。这话是屁话，不过也能说明些什么，确实是模拟设备，用软件的方式提供硬件设备具备的功能。对于和PC机交互的硬件设备，主要要干两件事，一是提供IRQ中断，二是响应IO输入输出。IO包括PIO/MMIO/DMA等（DMA算不算IO，不知道，反正不是CPU直接访问的）。以i8254.c实现的pit为例，主要提供了IRQ注入和PIO响应，见初始化函数pit_initfn：

```
1 static const MemoryRegionOps pit_ioport_ops = {
2     .read = pit_ioport_read,
3     .write = pit_ioport_write,
4     .impl = {
5         .min_access_size = 1,
6         .max_access_size = 1,
7     },
8     .endianness = DEVICE_LITTLE_ENDIAN,
9 };
10
11 static int pit_initfn(PITCommonState *pit)
12 {
13     PITChannelState *s;
14
15     s = &pit->channels[0];
16     /* the timer 0 is connected to an IRQ */
17     //这里有个irq_timer，用于qemu_set_irq提供中断注入
18     s->irq_timer = qemu_new_timer_ns(vm_clock, pit_irq_timer, s);
19     qdev_init_gpio_out(&pit->dev.qdev, &s->irq, 1);
20
21     memory_region_init_io(&pit->iports, &pit_ioport_ops, pit, "pit", 4);
22     qdev_init_gpio_in(&pit->dev.qdev, pit_irq_control, 1);
23     return 0;
24 }
```

这里的pit_ioport_ops，主要注册GUEST操作系统读写PIO时候的回调函数。

模块注册

QEMU要模拟模块那么多，以程序员的喜好，至少得来一套管理这些模拟设备模块的接口，以示设计良好。

QEMU将被模拟的模块分为了四类：

```
1 typedef enum {
2     MODULE_INIT_BLOCK,
3     MODULE_INIT_MACHINE,
4     MODULE_INIT_QAPI,
5     MODULE_INIT_QOM,
6     MODULE_INIT_MAX
7 } module_init_type;
```

• BLOCK

比如磁盘IO就属于BLOCK类型，e.g: block_init(bdrv_qcow2_init); block_init(iscsi_block_init);

• MACHINE

PC虚拟machine_init(pc_machine_init); XEN半虚拟化machine_init(xenpv_machine_init); MIPS虚拟machine_init(mips_machine_init);

• QAPI

QEMU GUEST AGENT模块里面会执行QAPI注册的回调

• QOM

QOM树大枝多，儿孙满堂，应该是这里面最复杂的一个，我们重点介绍。

e.g:

```
1 ObjectClass->PCIDeviceClass //显卡type_init(cirrus_vga_register_types), 网卡type_init(rtl8139_register_types)
2 IDEDeviceClass //IDE硬盘或CD-ROM type_init(ide_register_types)
3 ISADeviceClass //鼠标键盘type_init(i8042_register_types), RTC时钟type_init(pit_register)
4 SysBusDeviceClass //MMIO IDE(IDE设备直接连接CPU bus而不是连接IDE controller)type_init(mmio_ide_register_types)
5 //X86 CPU架构
```

CPUClass -



注册QOM设备的时候，使用QEMU提供的宏，type_init宏进行注册：

```
1 #define type_init(function) module_init(function, MODULE_INIT_QOM)
2 #define module_init(function, type) \
3     static void __attribute__((constructor)) do_qemu_init_## function(void) { \
4         register_module_init(function, type); \
5     }
```

这和写Linux驱动类似，一般写在一个模块实现文件的最底部，以pit为例，写的是type_init(pit_register_types)展开后为：

```
1 static void __attribute__((constructor)) do_qemu_init_pit_register_types(void)
2 {
3     register_module_init(pit_register_types, MODULE_INIT_QOM);
4 }
```

那么，这个do_qemu_init_pit_register_types何时调用？

在gcc里面，给函数加上__attribute__((constructor))，表示此函数需要在main开始前自动调用，测试调用顺序是：全局对象构造函数 -> __attribute__((constructor)) -> main -> 全局对象析构函数 -> __attribute__((destructor))。

调用register_module_init就是将pit_register_types回调函数插入util/module.c里定义的init_type_list[MODULE_INIT_QOM]链表内。

```
1 void register_module_init(void (*fn)(void), module_init_type type)
2 {
3     ModuleEntry *e;
4     ModuleTypeList *l;
5     e = g_malloc0(sizeof(*e));
6     e->init = fn; //init指针被设置为fn
7     l = find_type(type);
8     QTAILQ_INSERT_TAIL(l, e, node);
9 }
```

通过下面main函数的部分代码可以看出，模块初始化顺序是QOM->MACHINE->BLOCK，至于QAPI，在这个流程里没看到。

```
1 void main()
2 {
3     module_call_init(MODULE_INIT_QOM); //初始化设备
4     qemu_add_opts //初始化默认选项
5     module_call_init(MODULE_INIT_MACHINE); //初始化机器类型
6     machine = find_default_machine(); //这里对machine赋值，下面还会通过参数更改machine
7     vtp_script_execute(g_qemu_start_hook_path, g_fairsched_string, TYPE_START); //开机启动脚本的调用
8     深度分析启动参数
9     bdrv_init_with_whitelist -> bdrv_init -> module_call_init(MODULE_INIT_BLOCK); //初始化BLOCK设备
10    machine->init(&args); //初始化machine
11
12    qemu_run_machine_init_done_notifiers(); //初始化成功回调通知
13    qemu_system_reset(VMRESET_SILENT); //system reset 启动运行
14    if (loadvm) {
15        load_vmstate(loadvm);
16    } else if (loadstate) {
17        load_state_from_blockdev(loadstate);
18    }
19
20    resume_all_vcpus();
21    main_loop(); //进入主循环
22 }
```

在main函数进来的时候，首先调用module_call_init(MODULE_INIT_QOM);

```
1 void module_call_init(module_init_type type)
2 {
3     ModuleTypeList *l;
4     ModuleEntry *e;
5     l = find_type(type);
6     QTAILQ_FOREACH(e, l, node) {
7         e->init(); //这里，就是调用刚才注册的回调，例如，对于kvm-pit来说，调用的是pit_register
8     }
9 }
```



举报

此module_call_init将依次调用注册的回调，如PIT的pit_register_types：

```
1 static const TypeInfo pit_info = {
2     .name      = "isa-pit",    //做为type_table的key
3     .parent    = "pit-common", //父类型，这个比较重要，如果本TypeInfo没有设置class_size，会根据parent获取parent TypeImpl的class_size
4     .instance_size = sizeof(PITCommonState), //分配实例的大小
5     .class_init = pit_class_init, //初始化函数
6 };
7
8 static void pit_register_types(void)
9 {
10     type_register_static(&pit_info);
11 }
```


pit_register_types又进一步调用type_register_static -> type_register -> type_register_internal，这个函数完成的功能其实只是向type_table中插入了一个HASH键值对，以TypeInfo的name为KEY，malloc了一个TypeInfo结构的超集TypeImpl为VALUE，在以name为KEY查找TypeInfo时，这个hash也可以做成一个tree。

点赞 收藏 分享 ...



tycoon1988

发布了707 篇原创文章 · 获赞 55 · 访问量 100万+



传统ERP已经过时，2019流行的ERP系统是这一款！

主流erp系统

文章不错哦，我要夸奖作者两句...

- qemu2 machine的注册和的选择

阅读量 149

在qemu里面，machine代表一台要虚拟的硬件机器，那么qemu是如何注册和选择机器的？我们今天就来分析一下... 博文 来自: [woai110120130的...](#)
- imx6ull-qemu 裸机教程1：GPIO,IOMUX,I2C

阅读量 389

无意间搜到了韦东山老师的6ul网站，上面有一个6ul的qemu仿真器，下载下来用了用，非常好用，有UI，比原装的... 博文 来自: [u011280717的博客](#)
- 在qemu中运行wince 5.0/6.0(1)

阅读量 764

把wince(windows ce)系统移植到qemu模拟器中,目前网上还没有详细的移植步骤,曾经看到过一个帖子,说通过qemu... 博文 来自: [云, 无处不在 雾, ...](#)
- QEMU 设备模拟

阅读量 4381

设备模拟目的我们好像不会干一件事而毫无目的，就算不停刷微信朋友圈也是为了打发你无聊的时间。其实最装B的... 博文 来自: [万能的终端和网络](#)
- 开发网站,电子商务系统设计,推广+网站制作

网站建设开发
- KVM虚拟机和QEMU（命令行选项）

阅读量 2万+

KVM安装RHEL/Fedora/CentOSyum install bridge-utils kvmbridge-utils是网卡桥接工具，示例1：Redhat系统KV... 博文 来自: [少帅的天空](#)
- qemu参数解析

阅读量 4516

代码版本： qemu1.5static QemuOptsList *vm_config_groups[32]; qemu_add_opts(&qemu_drive_opts); qemu_... 博文 来自: [ayu_ag的专栏](#)
- QEMU使用简介

阅读量 1万+

QEMU使用简介。 博文 来自: [jiangwei0512的博客](#)
- QEMU测试环境搭建

阅读量 102

本人的github仓库： <https://github.com/rikeyone/qemu.git>仓库中集成了整个QEMU环境，包含install、build、st... 博文 来自: [程序猿的日记](#)
- Qemu 简述

阅读量 213

Qemu 架构Qemu 是纯软件实现的虚拟化模拟器，几乎可以模拟任何硬件设备，我们最熟悉的的就是能够模拟一台能够... 博文 来自: [weixin_33921089...](#)

👍

🔖

💬

☆

📱

<

>

赏




🔊

102

举报

qemu虚拟开发板_tycoon的专栏-CSDN博客

PC 上 QEMU模拟arm_tycoon的专栏-CSDN博客



传统ERP已经过时，2019流行的ERP系统是这一款！

主流erp系统

用模拟器加载基于ARM平台的WinCE6.0 内核（NK.bin）

虽然公司在一年以前就开始做基于WinCE4.2系统的触摸屏，但是作为侧重应用层面开发的我，对WinCE内核相关知… 博文 来自： weixin_34

用Qemu模拟ARM - tycoon的专栏 - CSDN博客

QEMU 快速使用指南 (译) ***_tycoon的专栏-CSDN博客

2.1 Qemu用户态 Machine与cpu管理

本节主要分析PC机在Qemu中的构成结构(QEMU的对象模型)，特别是CPU的相关结构



TangGeeA

130篇文章

排名:千里之外

关注



FRAWSCCC

22篇文章

排名:千里之外

关注



coolper

162篇文章

排名:千里之外

关注



winceos

82篇文章

排名:千里之外

关注

KVM虚拟化原理与实践(连载)_运维_tycoon的专栏-CSDN博客

OpenStack QEMU_tycoon的专栏-CSDN博客

在qemu中运行wince 5.0/6.0(2)

Qemu 模拟的Mainstone platform,内存是64M，而WinCE 6默认编译的时候内存设置为128M,故需要把mainstoneiii… 博文 来自： 云，无处不在 雾，…

在qemu中增加pci设备并用linux驱动验证


声明本文主要针对x86架构进行说明。使用的qemu版本是：qemu-kvm-1.2.0-rc21)PCI结构简介每个PCI设备都有一… 博文 来自： XscKernel的专栏 …

qemu QOM(qemu object model)和设备模拟_ayu_ag的专栏-CSDN博客

虚拟机迁移技术漫谈_运维_tycoon的专栏-CSDN博客

qemu QOM(qemu object model)和设备模拟

本文所用qemu为1.5版本的，不是android emulator的。之前几篇文章介绍的都是android emulator中的设备模拟… 博文 来自： ayu_ag的专栏



开发网站,电子商务系统设计,推广+网站制作

网站建设开发

...04使用QEMU模拟ARM平台开发环境_运维_acrux1985的专栏-CSDN博客

QEMU中如何定义所有Device的基类和BUS的基类

本文介绍QEMU如何模拟设备、总线、主板的连接关系。 博文 来自： YuanruiZJU的博客

QEMU PCIe设备实现


PCIe 设备虚拟化QEMU中的实现 包括处理中断的硬件以及Linux如何响应和处理终端。技术分析分享


成功把Wince 6.0移植到qemu中运行


鼠标,键盘,磁盘是通过usb设备来模拟的,网卡是lan91c111的,使用的是smc公司提供的wince驱动. 管理员在2009年8… 博文 来自： 云，无处不在 雾，…


QEMU中的对象模型——QOM（介绍篇）


QEMU提供了一套面向对象编程的模型——QOM，即QEMU Object Module，几乎所有的设备如CPU、内存、总线等… 博文 来自： YuanruiZJU的博客




















17

来自： wanthehelping的博客

阅读数 1899

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

博文 来自： wanthehelping的博客

qemu中device和driver的区别 使用9 p文件系统 阅读数 121
qemu配置中经常会出现-driver/-device的选项，可以理解成-driver是后端设备，即一个实际的物理的磁盘；de博文 来自: weixin_30741653...



开发网站,电子商务系统设计,推广+网站制作

网站建设开发

一步步教你如何在Ubuntu虚拟机中安装QEMU并模拟模拟arm 开发环境（一）ulmage u-boot 阅读数 1万+
初次接触qemu是因为工作的需要，有时候下了班，可能需要在家里研究一些东西，因为博主用到arm环境，这时候博文 来自: IT---庸才的

qemu模拟显卡，使用spice源码解析
qemu是怎么模拟显卡的，qemu中加入spice支持，这部分源码怎么理解，绘图系统是怎么实现的

QEMU虚拟网卡设备的创建流程 阅读数 113
基于qemu-kvm-0.12.1.2-2.160.el6_1.8.src.rpm虚拟网卡类型为virtio-net-pcivirtio网卡设备对应的命令行参数为-d博文 来自: sdulibh的专

使用 qemu 来模拟 nvme 设备 阅读数 715
使用 qemu 模拟 nvme 设备，本篇可以参考。引用本文请注明出处: https://blog.csdn.net/Hello_NB1/article/deta博文 来自: Hello_NB1的博客

QEMU建模之设备创建总体流程 阅读数 111
(这里的设备创建以中断控制器即openpic为例)1.main函数之前执行type_init1> 在vl.c文件的主函数执行前会先执博文 来自: sinat_38205774的...

qemu 中是怎么模拟的新的设备 阅读数 49
kvm_cpu_exec 和 demo 中演示的一样转载于:https://www.cnblogs.com/honpey/p/8063875.html...博文 来自: weixin_30244681...

Qemu-KVM基本工作原理分析 阅读数 9795
1、理解KVM与Qemu的关系 我们都知道开源虚拟机KVM，并且知道它总是跟Qemu结合出现，那这两者之间有什么博文 来自: Mr.Buffoon

虚拟块设备的实现技术-nbd/iscsi/qemu等模式 阅读数 5428
nbd方式：一.NBD简介NBD(Network Block Device)让你可以将一个远程主机的磁盘空间,当作一个块设备来使用.就博文 来自: KEN的专栏

在WINCE6.0下用的是Device Emulator
现在的最终目的就是想在WINCE6.0下通过Device Emulator熟悉实现嵌入式操作系统 我已经大概了解了如何搭建一个环境...论坛

怎么用qemu生成一个用管道虚拟的串口, windows下的qemu 论坛
我在搭建 wdk 的调试环境，用windbg调试 虚拟机的xp 虚拟机用的qemu 0.13 我在《寒江独钓》中跟着做，windbg 我设...

终于能够在GDB+qemu进行跟踪和调试了 阅读数 5833
经过几天努力，终于能够在GDB+qemu进行跟踪和调试了，但是现在只能调试ntoskrnl,还不知到，freeldr怎么跟踪...博文 来自: sstower的专栏

qemu虚拟开发板 阅读数 1571
虚拟开发板From armuxJump to: navigation, search如果你想拥有一块开发板，而又不想花钱，那你就自己博文 来自: 孤独小剑的专栏

选择Linux还是WinCE 阅读数 2743
最近打算在开发中引入嵌入式操作系统，转向arm9平台。可控选择的定位在linux和wince两项中。对于选择确是痛博文 来自: 拥抱变化

【转】Wince Device Emulator使用介绍-Device Emulator 2.0 阅读数 9
【转】Wince Device Emulator使用介绍-Device Emulator 2.0 转自: http://tech.ddvip.com/2008-12/1230082051...博文 来自: weixin_30443747...

使用QEMU模拟搭建ARM开发平台（三）——添加SCSI和MTD以及NAND flash支持 阅读数 2429
使用versatile_defconfig编译的内核不能满足要求，现在，添加SCSI磁盘，MTD以及NAND flash的支持。交叉编译li博文 来自: tycoon的专栏

KVM虚拟机代码揭秘——QEMU的PCI总线与设备（上） 阅读数 1万+
最近研究了一下QEMU的虚拟PCI设备，打算虚拟一个PCI-PCI桥和一个PCI设备，设备挂在桥上，桥挂在pci主桥上。博文 来自: Shawn的专

kvm-qemu 设备IO虚拟化
虚拟设备的IO地址注册如我们所知，KVM虚拟机的设备模拟是在QEMU中实现的，而KVM实现的实质上只是IO的拦截...博文 来自: weixin_42...



举报

virtio的qemu总线与设备模型

阅读数 1万+

(很多内容是网上找的，+上我个人的一点理解，推荐大家去看 http://mnstory.net/2014/10/qemu-device-simulati... 博文 来自: majieyue的牛++

虚拟化中如何实现设备模拟？

在计算机虚拟化领域中，对设备进行模拟是虚拟化实现的基础。设备的模拟主要包括一下三个方面：设备状态的记录...

qemu-kvm 对mmio的模拟

转: http://blog.chinaunix.net/uid-28541347-id-5789579.htmlMMIO和PIO的区别I/O作为CPU和外设交流的一个渠... 博文 来自: weixin_42...

Java C语言 Python C++ C# Visual Basic .NET JavaScript PHP SQL Go语言 R语言 Assembly language Swift R语言
MATLAB PL/SQL Perl Visual Basic Objective-C Delphi/Object Pascal Unity3D



tycoon1988

TA的个人主页>

原创 707 粉丝 172 获赞 55 评论 39 访问 100万+

等级: 博客 周排名: 5万+
积分: 1万+ 总排名: 1675
勋章: 4

关注

私信

最新文章

linux中ip tunnel的实现及协议简介

qemu 启动虚拟机 sheepdog

使用 QEMU 进行嵌入式系统开发

QEMU 快速使用指南 (译)

qemu 在当前OS中运行其它的操作系统

分类专栏

linux 10篇
linux开发 107篇
C++ 7篇
云计算 99篇
淘测试 2篇

展开



举报

归档	
2015年6月	15篇
2015年5月	8篇
2015年4月	49篇
2015年2月	11篇
2015年1月	21篇
2014年12月	2篇
2014年11月	60篇
2014年10月	82篇
展开	

热门文章	
application/json 四种常见的 POST 提交数据方式	阅读数 114215
python中cursor操作数据库	阅读数 29322
shell中括号的特殊用法 linux if多条件判断	阅读数 23540
ZooKeeper用途	阅读数 20271
静态路由与默认路由（原理+区别+实例）	阅读数 18347

最新评论	
G++ -l 与 -L选项 编译...	luhuilong01：感谢
G++ -l 与 -L选项 编译...	luhuilong01：nice
Python id() 函数	littleboy：您好。您认为，对于列表，其id()值返回的是列表第一个子元素L[0]的存储地址。我ð ...
NF_HOOK	qq_39006318：白背景用白色字？？
skb_dst_set - ...	sibaoxiang：您好，我这边也是需要指定从哪个物理网口转发数据，但转发后的数据无法正常被 ...

👤 QQ客服	✉ kefu@csdn.net
🗣 客服论坛	☎ 400-660-0108
工作时间 8:30-22:00	
关于我们 招聘 广告服务 网站地图	
京ICP备19004658号 经营性网站备案信息	
🚓 公安备案号 11010502030143	
©1999-2020 北京创新乐知网络技术有限公司	
司 网络110报警服务	
北京互联网违法和不良信息举报中心	
中国互联网举报中心 家长监护	
版权与免责声明 版权申诉	

举报