在VMM上运行Starry-old跑helloworld程序

`测试环境`

`Unbuntu22.04`

`qemu三个架构(riscv64/aarch64/x86_64)版本均为9.2.50 (qemu源码)`

`    VMM: git clone https://github.com/arceos-hypervisor/arceos-umhv.git`

`Starry-old: git clone https://github.com/Starry-OS/Starry-Old.git`

`在vmm中的MakeFile中加入一些测试脚本，方便后期创建disk.img`

脚本

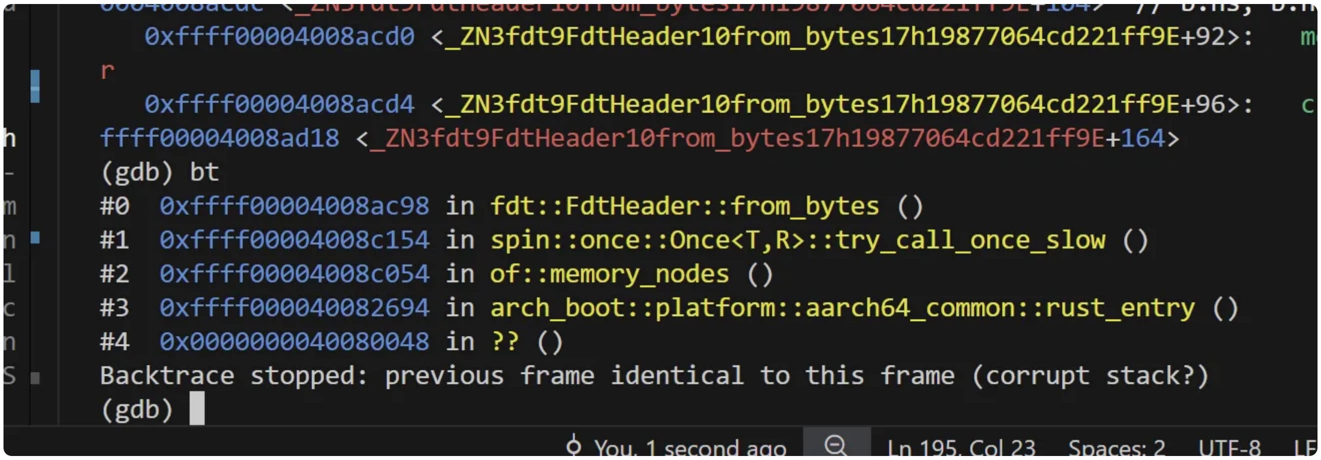
```
COPYFILE ?=
test:
rm disk.img
make disk_img
sudo mount disk.img tmp/
sudo cp $(COPYFILE) tmp
sudo umount tmp
//使用方法
make test COPYFILE=$(YOUR_FILE)
```

在裸机riscv64上跑starry_old发现的问题：qemu版本不宜过高，过高的话会出现问题，仍然是qemu和sbi不兼容的问题。

在aarch64架构下qemu环境中VMM运行unikernel版本的Starry-old跑helloworld程序

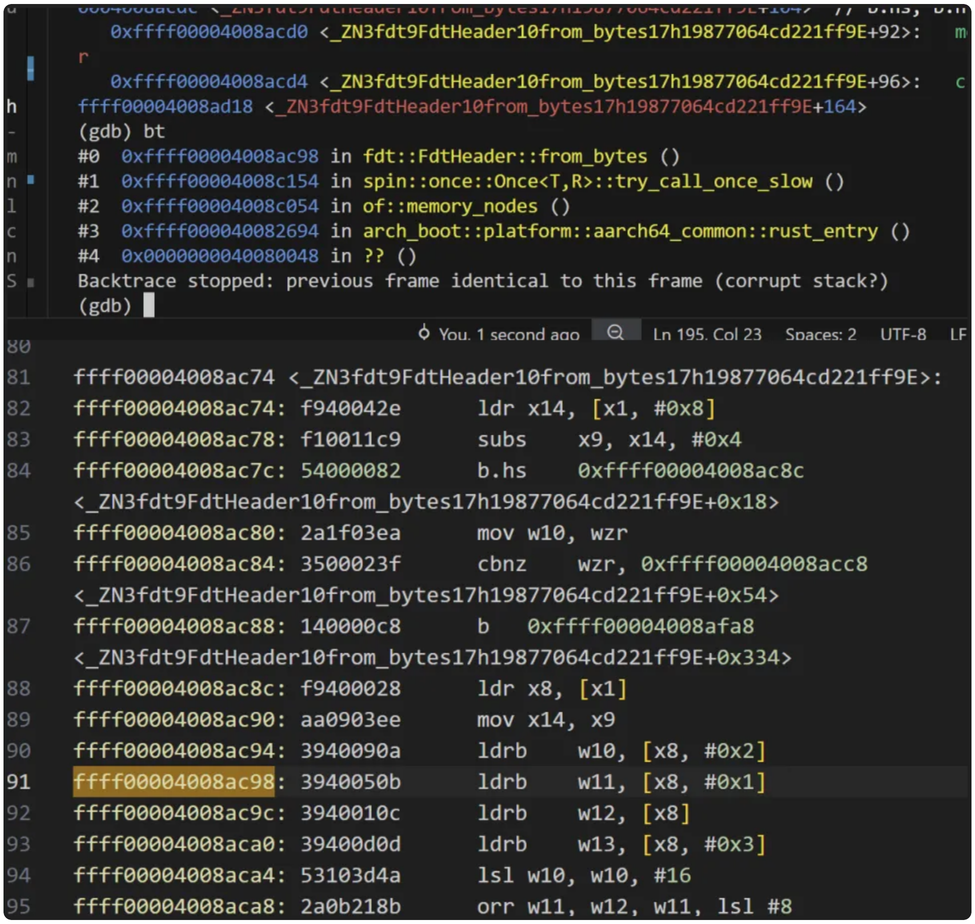
过程的话参照在vmm上跑arceos的过程，两者大致流程类似，但是值得注意的是，目前直接跑starry的话，经过gdb调试，发现存在一定问题。

starry 想去读设备树的内存地址，我们给了一个为0的地址给 starry ， 所以 starry 从 0 + 2 的地址去读设备树了，但是这块内存我们没有分配，导致会出现访存问题。实际上，dtb这部分是没有用的，starry其实在启动时也没有这个需求，经过尝试，其实只要分配一块有效的内存进去，比如将dtb的内存位置设在0x4000_0000处，就可以跑起来了。



```
   0xffff00004008acd0 <_ZN3fdt9FdtHeader10from_bytes17h19877064cd221ff9E+92>:
r
   0xffff00004008acd4 <_ZN3fdt9FdtHeader10from_bytes17h19877064cd221ff9E+96>:
ffff00004008ad18 <_ZN3fdt9FdtHeader10from_bytes17h19877064cd221ff9E+164>
(gdb) bt
#0  0xffff00004008ac98 in fdt::FdtHeader::from_bytes ()
#1  0xffff00004008c154 in spin::once::Once<T,R>::try_call_once_slow ()
#2  0xffff00004008c054 in of::memory_nodes ()
#3  0xffff000040082694 in arch_boot::platform::aarch64_common::rust_entry ()
#4  0x0000000040080048 in ?? ()
Backtrace stopped: previous frame identical to this frame (corrupt stack?)
(gdb) 
```

You, 1 second ago   Ln 195, Col 23   Spaces: 2   UTF-8   LF



```
   0xffff00004008acd0 <_ZN3fdt9FdtHeader10from_bytes17h19877064cd221ff9E+92>:
r
   0xffff00004008acd4 <_ZN3fdt9FdtHeader10from_bytes17h19877064cd221ff9E+96>:
ffff00004008ad18 <_ZN3fdt9FdtHeader10from_bytes17h19877064cd221ff9E+164>
(gdb) bt
#0  0xffff00004008ac98 in fdt::FdtHeader::from_bytes ()
#1  0xffff00004008c154 in spin::once::Once<T,R>::try_call_once_slow ()
#2  0xffff00004008c054 in of::memory_nodes ()
#3  0xffff000040082694 in arch_boot::platform::aarch64_common::rust_entry ()
#4  0x0000000040080048 in ?? ()
Backtrace stopped: previous frame identical to this frame (corrupt stack?)
(gdb) 
```

You, 1 second ago   Ln 195, Col 23   Spaces: 2   UTF-8   LF

```
ffff00004008ac74 <_ZN3fdt9FdtHeader10from_bytes17h19877064cd221ff9E>:
ffff00004008ac74: f940042e      ldr x14, [x1, #0x8]
ffff00004008ac78: f10011c9      subs    x9, x14, #0x4
ffff00004008ac7c: 54000082      b.hs    0xffff00004008ac8c
<_ZN3fdt9FdtHeader10from_bytes17h19877064cd221ff9E+0x18>
ffff00004008ac80: 2a1f03ea      mov w10, wzr
ffff00004008ac84: 3500023f      cbnz    wzr, 0xffff00004008acc8
<_ZN3fdt9FdtHeader10from_bytes17h19877064cd221ff9E+0x54>
ffff00004008ac88: 140000c8      b   0xffff00004008afa8
<_ZN3fdt9FdtHeader10from_bytes17h19877064cd221ff9E+0x334>
ffff00004008ac8c: f9400028      ldr x8, [x1]
ffff00004008ac90: aa0903ee      mov x14, x9
ffff00004008ac94: 3940090a      ldrb    w10, [x8, #0x2]
ffff00004008ac98: 3940050b      ldrb    w11, [x8, #0x1]
ffff00004008ac9c: 3940010c      ldrb    w12, [x8]
ffff00004008aca0: 39400d0d      ldrb    w13, [x8, #0x3]
ffff00004008aca4: 53103d4a      lsl w10, w10, #16
ffff00004008aca8: 2a0b218b      orr w11, w12, w11, lsl #8
```

具体来说，由于arceos和starry的相似性，其实可以直接采用arceos的配置文件进行修改，就是要在config文件里面加入这两行就可以了

修改代码 Plain Text

```
dtb_load_addr = 0x4000_0000
dtb_path = "helloworld_aarch64-qemu-virt.bin"
```

加载镜像

先编译starry_old，然后将编译后的arceos的bin文件放入$(YOUR_FILE)中

加载镜像 Plain Text

```
make test COPYFILE=$(YOUR_FILE)
```

运行VMM

运行VMM Plain Text

```
cd arceos-vmm
make defconfig ARCH=aarch64
make ACCEL=n ARCH=aarch64 LOG=info VM_CONFIGS=configs/vms/arceos-aarch64.toml APP_FEATURES=fs run
```

运行结果

运行结果 Plain Text

```
Running on qemu...
qemu-system-aarch64 -m 128M -smp 1 -cpu cortex-a72 -machine virt,virtualization=on,gic-version=2 -kernel /home/zjz/arceos/arceos-umhv/arceos-vmm/arceos-vmm_aarch64-qemu-virt-hv.bin -device virtio-blk-pci,drive=disk0 -drive id=disk0,if=none,format=raw,file=disk.img -nographic -machine virtualization=on,gic-version=2

       d8888                            .d88888b.   .d8888b.
      d88888                           d88P" "Y88b d88P  Y88b
     d88P888                           888     888 Y88b.
    d88P 888 888d888  .d8888b  .d88b.  888     888  "Y888b.
   d88P  888 888P"   d88P"    d8P  Y8b 888     888     "Y88b.
  d88P   888 888     888      88888888 888     888       "888
 d8888888888 888     Y88b.    Y8b.     Y88b. .d88P Y88b  d88P
d88P     888 888      "Y8888P  "Y8888   "Y88888P"   "Y8888P"

arch = aarch64
platform = aarch64-qemu-virt-hv
target = aarch64-unknown-none-softfloat
build_mode = release
log_level = info
smp = 1

[  0.007298 0 axruntime:130] Logging is enabled.
[  0.009221 0 axruntime:131] Primary CPU 0 started, dtb = 0x44000000.
[  0.010061 0 axruntime:133] Found physcial memory regions:
[  0.012218 0 axruntime:135]   [PA:0x40080000, PA:0x400f0000) .text (READ | EXECUTE | RESERVED)
[  0.016457 0 axruntime:135]   [PA:0x400f0000, PA:0x40106000) .rodata (READ | RESERVED)
[  0.018589 0 axruntime:135]   [PA:0x40106000, PA:0x4010c000) .data .tdata .tbss .percpu (READ | WRITE | RESERVED)
[  0.019096 0 axruntime:135]   [PA:0x4010c000, PA:0x4014c000) boot stack (READ | WRITE | RESERVED)
[  0.019612 0 axruntime:135]   [PA:0x4014c000, PA:0x40152000) .bss (READ | WRITE | RESERVED)
[  0.020778 0 axruntime:135]   [PA:0x40152000, PA:0x48000000) free memory (READ | WRITE | FREE)
[  0.022103 0 axruntime:135]   [PA:0x9000000, PA:0x9001000) mmio (READ | WRITE | DEVICE | RESERVED)
[  0.022664 0 axruntime:135]   [PA:0x9100000, PA:0x9101000) mmio (READ | WRITE | DEVICE | RESERVED)
[  0.023192 0 axruntime:135]   [PA:0x8000000, PA:0x8020000) mmio (READ | WRITE | DEVICE | RESERVED)

[  0.023651 0 axruntime:135]   [PA:0xa000000, PA:0xa004000) mmio (READ | WRITE | DEVICE | RESERVED)
[  0.024122 0 axruntime:135]   [PA:0x10000000, PA:0x3eff0000) mmio (READ | WRITE | DEVICE | RESERVED)
[  0.024709 0 axruntime:135]   [PA:0x4010000000, PA:0x4020000000) mmio (READ | WRITE | DEVICE | RESERVED)
[  0.025590 0 axruntime:208] Initialize global memory allocator...
[  0.026552 0 axruntime:209]   use TLSF allocator.
[  0.029691 0 axmm:60] Initialize virtual memory management...
[  0.058847 0 axruntime:150] Initialize platform devices...
[  0.060084 0 axhal::platform::aarch64_common::gic:67] Initialize GICv2...
[  0.062292 0 axtask::api:73] Initialize scheduling...
[  0.064754 0 axtask::api:79]   use FIFO scheduler.
[  0.065357 0 axdriver:152] Initialize device drivers...
[  0.065911 0 axdriver:153]   device model: static
[  0.078949 0 virtio_drivers::device::blk:59] config: 0x1000e000
[  0.080297 0 virtio_drivers::device::blk:64] found a block device of size 65536KB
[  0.083325 0 axdriver::bus::pci:104] registered a new Block device at 00:02.0: "virtio-blk"
[  0.158229 0 axfs:41] Initialize filesystems...
[  0.158972 0 axfs:44]   use block device 0: "virtio-blk"
[  0.227339 0 fatfs::dir:139] Is a directory
[  0.319920 0 fatfs::dir:139] Is a directory
[  0.414972 0 fatfs::dir:139] Is a directory
[  0.556155 0 fatfs::dir:139] Is a directory
[  0.618329 0 axruntime:176] Initialize interrupt handlers...
[  0.619937 0 axruntime:186] Primary CPU 0 init OK.
[  0.620702 0:2 arceos_vmm:17] Starting virtualization...
[  0.621296 0:2 arceos_vmm:19] Hardware support: true
[  0.623769 0:4 arceos_vmm::hal:113] Hardware virtualization support enabled on core 0
[  0.651653 0:2 arceos_vmm::vmm::config:33] Creating VM [1] "arceos"
[  0.653576 0:2 axvm::vm:113] Setting up memory region: [0x40000000~0x41000000] READ | WRITE | EXECUTE | USER
[  0.662654 0:2 axvm::vm:156] Setting up passthrough device memory region: [0x8000000~0x8050000] -> [0x8000000~0x8050000]
[  0.664860 0:2 axvm::vm:156] Setting up passthrough device memory region: [0x9000000~0x9001000] -> [0x9000000~0x9001000]
[  0.666999 0:2 axvm::vm:156] Setting up passthrough device memory region: [0x9010000~0x9011000] -> [0x9010000~0x9011000]
[  0.668506 0:2 axvm::vm:156] Setting up passthrough device memory region: [0x9030000~0x9031000] -> [0x9030000~0x9031000]
[  0.669380 0:2 axvm::vm:156] Setting up passthrough device memory region: [0xa000000~0xa004000] -> [0xa000000~0xa004000]
[  0.672602 0:2 axvm::vm:191] VM created: id=1
[  0.674043 0:2 axvm::vm:206] VM setup: id=1
[  0.676408 0:2 arceos_vmm::vmm::config:40] VM[1] created success, loading images...
[  0.678548 0:2 arceos_vmm::vmm::images::fs:102] Loading VM images from filesystem
[  0.854029 0:2 arceos_vmm::vmm:27] Setting up vcpus...
[  0.855307 0:2 arceos_vmm::vmm::vcpus:176] Initializing VM[1]'s 1 vcpus
[  0.856104 0:2 arceos_vmm::vmm::vcpus:207] Spawning task for VM[1] Vcpu[0]
[  0.857219 0:2 arceos_vmm::vmm::vcpus:219] Vcpu task Task(5, "VM[1]-VCpu[0]") created cpumask: [0, ]
[  0.858414 0:2 arceos_vmm::vmm:34] VMM starting, booting VMs...
[  0.859242 0:2 axvm::vm:273] Booting VM[1]
[  0.860088 0:2 arceos_vmm::vmm:40] VM[1] boot success
[  0.863003 0:5 arceos_vmm::vmm::vcpus:240] VM[1] Vcpu[0] waiting for running
[  0.865493 0:5 arceos_vmm::vmm::vcpus:243] VM[1] Vcpu[0] running...

       d8888                            .d88888b.   .d8888b.
      d88888                           d88P" "Y88b d88P  Y88b
     d88P888                           888     888 Y88b.
    d88P 888 888d888  .d8888b  .d88b.  888     888  "Y888b.
   d88P  888 888P"   d88P"    d8P  Y8b 888     888     "Y88b.
  d88P   888 888     888      88888888 888     888       "888
 d8888888888 888     Y88b.    Y8b.     Y88b. .d88P Y88b  d88P
d88P     888 888      "Y8888P  "Y8888   "Y88888P"   "Y8888P"

arch = aarch64
platform = aarch64-qemu-virt
target = aarch64-unknown-none-softfloat
smp = 1
build_mode = release
log_level = debug

[  0.882677 0 axruntime:120] Logging is enabled.
[  0.886773 0 axruntime:121] Primary CPU 0 started, dtb = 0x40000000.
[  0.889375 0 axruntime:122] Platform name aarch64-qemu-virt.
[  0.890640 0 axruntime:124] Found physcial memory regions:
[  0.893011 0 axruntime:126]   [PA:0x40080000, PA:0x4008d000) .text (READ | EXECUTE | RESERVED)
[  0.894442 0 axruntime:126]   [PA:0x4008d000, PA:0x40090000) .rodata (READ | RESERVED)
[  0.896672 0 axruntime:126]   [PA:0x40090000, PA:0x40094000) .data .tdata .tbss .percpu (READ | WRITE | RESERVED)
[  0.899534 0 axruntime:126]   [PA:0x40094000, PA:0x400d4000) boot stack (READ | WRITE | RESERVED)
[  0.900965 0 axruntime:126]   [PA:0x400d4000, PA:0x400d5000) .bss (READ | WRITE | RESERVED)
[  0.902732 0 axruntime:126]   [PA:0x40000000, PA:0x40100000) fdt reserved (READ | RESERVED)
[  0.904765 0 axruntime:126]   [PA:0x400d5000, PA:0x0) free memory (READ | WRITE | FREE)
[  0.907149 0 axruntime:126]   [PA:0x9000000, PA:0x9001000) mmio (READ | WRITE | DEVICE | RESERVED)
[  0.909351 0 axruntime:126]   [PA:0x9030000, PA:0x9031000) mmio (READ | WRITE | DEVICE | RESERVED)
[  0.910601 0 axruntime:126]   [PA:0x9010000, PA:0x9011000) mmio (READ | WRITE | DEVICE | RESERVED)
[  0.911546 0 axruntime:126]   [PA:0x8000000, PA:0x8020000) mmio (READ | WRITE | DEVICE | RESERVED)
[  0.915904 0 axruntime:126]   [PA:0xa000000, PA:0xa004000) mmio (READ | WRITE | DEVICE | RESERVED)
[  0.916772 0 axruntime:126]   [PA:0x10000000, PA:0x3eff0000) mmio (READ | WRITE | DEVICE | RESERVED)
[  0.917885 0 axruntime:126]   [PA:0x4010000000, PA:0x4020000000) mmio (READ | WRITE | DEVICE | RESERVED)
[  0.919461 0 axruntime:143] Initialize platform devices...
[  0.920002 0 axruntime:182] Primary CPU 0 init OK.
Hello, world!
[  0.922695 0 axruntime:192] main task exited: exit_code=0
[  0.924893 0 axhal::platform::aarch64_common::psci:96] Shutting down...
[  0.926247 0:5 arceos_vmm::vmm::vcpus:288] VM[1] run VCpu[0] SystemDown
[  0.926976 0:5 axhal::platform::aarch64_common::psci:98] Shutting down...
```