OP-TEE 3.17.0 QEMU V8的环境搭建（Ubuntu20.04)

安装Ubuntu

先安装一下Virtualbox+Ubuntu20.04,可以参考[How TO]-图解virtualbox下安装ubuntu20.04虚拟机

安装Ubuntu基础工具

```
sudo apt-get install samba smbclient git make expect vim net-tools python3-pip
python2.7 binfmt-support qemu qemu-user-static openssl
```

注意安装python2.7后，需要创建一个软链接。

```
cd /usr/bin/
sudo ln -sf python2.7 python
```

安装http服务

```
sudo apt-get install apache2
sudo /etc/init.d/apache2 restart
```

安装repo

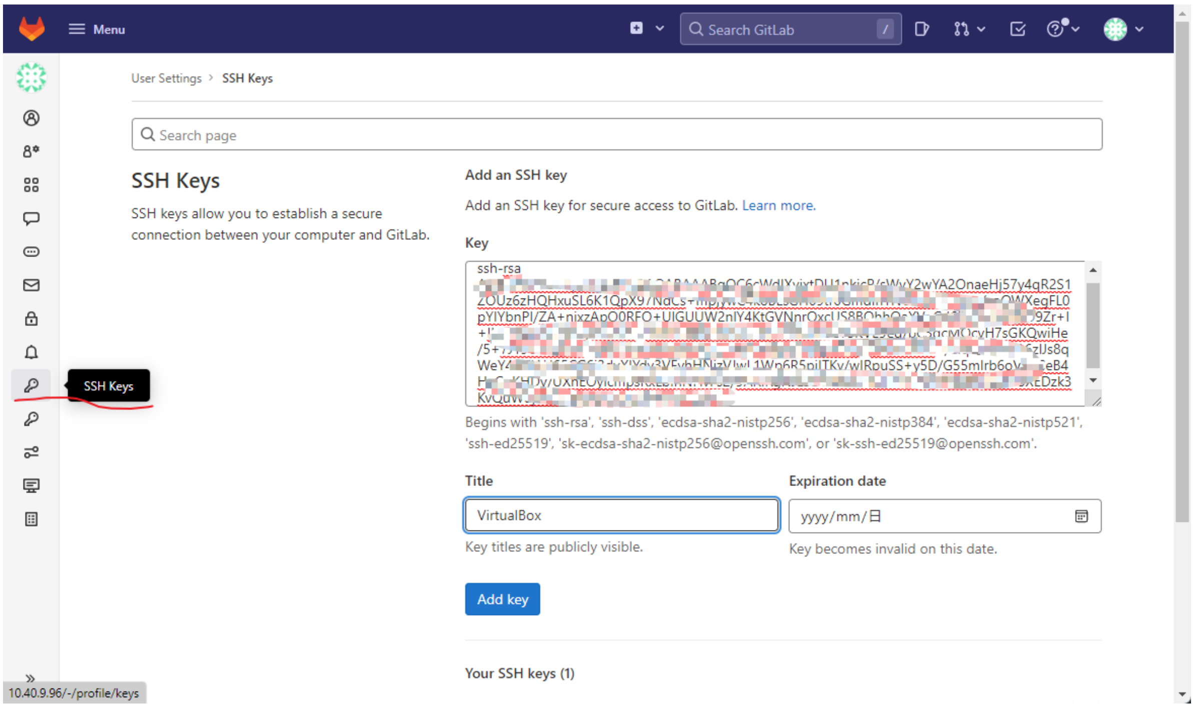
```
git clone http://10.40.9.96/clourneysemi/git-repo.git
cd git-repo/
cp repo /bin/
sudo chmod a+x /bin/repo
```

配置github SSH Key

```
ssh-keygen -t rsa -C "weitao.zhu@aliyun.com"

cat ~/.ssh/id_rsa.pub
```

选择gitlab账号的 -> User Settings -> SSH key。将id_rsa.pub中内容拷贝到Key中，点击 Add key。



User Settings › SSH Keys

Search page

SSH Keys

SSH keys allow you to establish a secure connection between your computer and GitLab.

Add an SSH key

Add an SSH key for secure access to GitLab. Learn more.

Key

ssh-rsa
[redacted]

Begins with 'ssh-rsa', 'ssh-dss', 'ecdsa-sha2-nistp256', 'ecdsa-sha2-nistp384', 'ecdsa-sha2-nistp521', 'ssh-ed25519', 'sk-ecdsa-sha2-nistp256@openssh.com', or 'sk-ssh-ed25519@openssh.com'.

Title: VirtualBox

Key titles are publicly visible.

Expiration date: yyyy/mm/日

Key becomes invalid on this date.

Add key

Your SSH keys (1)

配置git

```
git config --global user.email "wez057@clourneysemi.com"
git config --global user.name "weston"
```

输入命令

```
git config --global credential.helper store
```

这一步会在用户目录下的.gitconfig文件最后添加：

push代码
这一步会在用户目录下生成文件.git-credential记录用户名密码的信息
格式：

```
https:{username}:{password}@github.com
```

安装OP-TEE

1. 安装编译OP-TEE的工具

```
$ sudo apt-get install android-tools-adb android-tools-fastboot autoconf \
        automake bc bison build-essential ccache cscope curl device-tree-
compiler \
        expect flex ftp-upload gdisk iasl libattr1-dev libcap-dev \
        libfdt-dev libftdi-dev libglib2.0-dev libgmp-dev libhidapi-dev \
        libmpc-dev libncurses5-dev libpixman-1-dev libssl-dev libtool make \
        mtools netcat ninja-build  python3-crypto  \
        python3-pycryptodome python3-pyelftools  python3-serial \
        rsync unzip uuid-dev xdg-utils xterm xz-utils zlib1g-dev
```

2. 更新对应QEMU V8的optee代码

```
$ repo init --no-clone-bundle -u http://10.40.9.96/clourneysemi/op-tee/manifest.git -m qemu_v8.xml --repo-url=http://10.40.9.96/clourneysemi/git-repo.git -b 3.17.0-clourney

Downloading Repo source from http://10.40.9.96/clourneysemi/git-repo.git
remote: Enumerating objects: 7372, done.
remote: Counting objects: 100% (7372/7372), done.
remote: Compressing objects: 100% (3331/3331), done.
remote: Total 7372 (delta 3971), reused 7372 (delta 3971), pack-reused 0
Receiving objects: 100% (7372/7372), 6.65 MiB | 25.49 MiB/s, done.
Resolving deltas: 100% (3971/3971), done.
repo: Updating release signing keys to keyset ver 2.3
Downloading manifest from http://10.40.9.96/clourneysemi/op-tee/manifest.git
remote: Enumerating objects: 1392, done.
remote: Counting objects: 100% (1392/1392), done.
remote: Compressing objects: 100% (357/357), done.
remote: Total 1392 (delta 1037), reused 1389 (delta 1034), pack-reused 0
Receiving objects: 100% (1392/1392), 286.50 KiB | 17.91 MiB/s, done.
Resolving deltas: 100% (1037/1037), done.

Your identity is: Weston <wez057@clourneysemi.com>
If you want to change this, please re-run 'repo init' with --config-name

Testing colorized output (for 'repo diff', 'repo status'):
  black    red      green    yellow   blue     magenta  cyan     white
  bold     dim      ul       reverse
Enable color display in this user account (y/N)? y

repo has been initialized in /home/weston/workspace/optee-atf-armv8/
If this is not the directory in which you want to initialize repo, please run:
   rm -r /home/weston/workspace/optee-atf-armv8//.repo
and try again.
```

3. 用repo拖取代码

```
$ repo sync --no-clone-bundle -j8
Fetching: 100% (14/14), done in 1m51.471s
Garbage collecting: 100% (14/14), done in 0.118s
Updating files: 100% (75032/75032), done.
Updating files: 100% (11690/11690), done.
Updating files: 100% (17747/17747), done.
Checking out: 100% (14/14), done in 38.045s
repo sync has finished successfully.
```

4. 编译

在build目录下开始编译

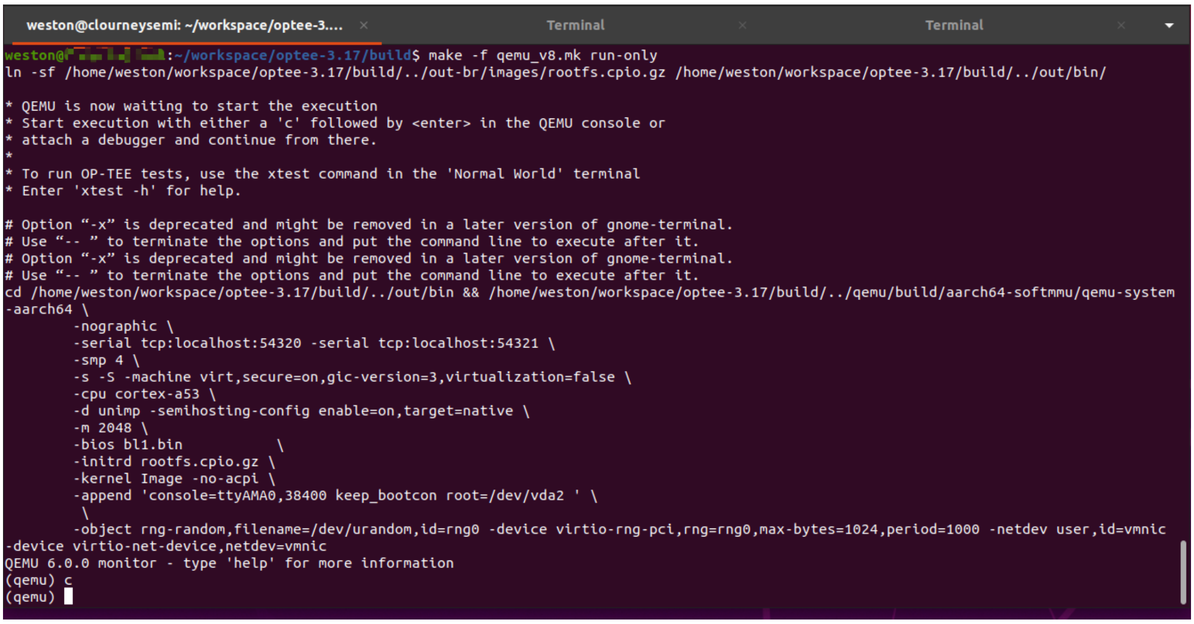
```
make -f qemu_v8.mk all -j8
```

5. 运行

在build目录下运行

```
make -f qemu_v8.mk run-only
```

敲完命令运行后，记得继续按c然后按回车健。

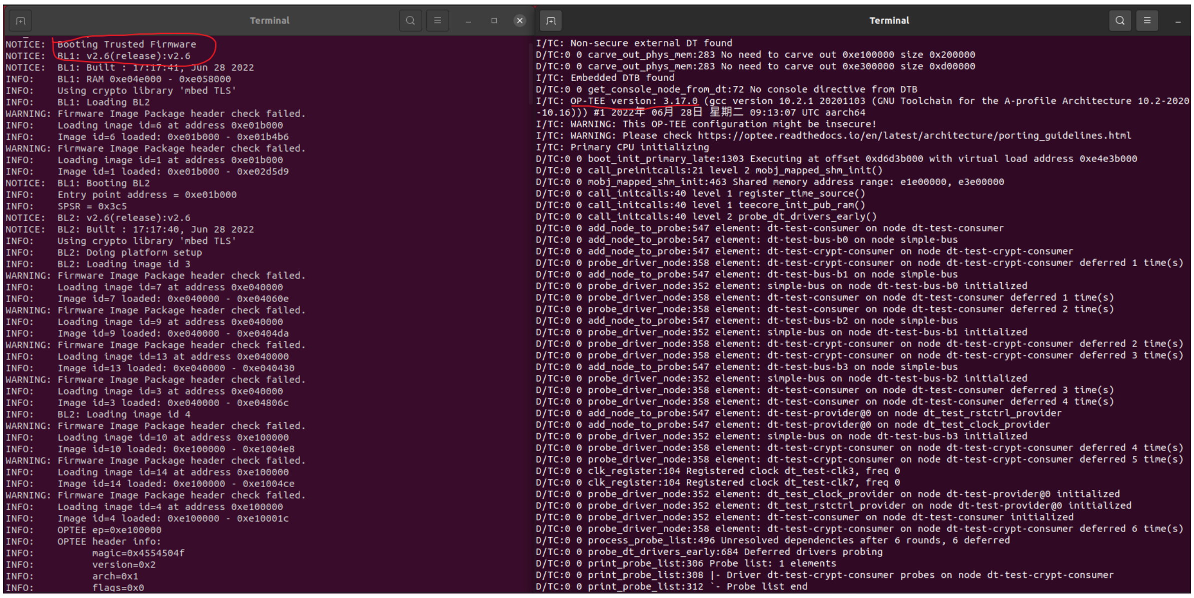


```
weston@[redacted]:~/workspace/optee-3.17/build$ make -f qemu_v8.mk run-only
ln -sf /home/weston/workspace/optee-3.17/build/../out-br/images/rootfs.cpio.gz /home/weston/workspace/optee-3.17/build/../out/bin/

* QEMU is now waiting to start the execution
* Start execution with either a 'c' followed by <enter> in the QEMU console or
* attach a debugger and continue from there.
*
* To run OP-TEE tests, use the xtest command in the 'Normal World' terminal
* Enter 'xtest -h' for help.

# Option “-x” is deprecated and might be removed in a later version of gnome-terminal.
# Use “-- ” to terminate the options and put the command line to execute after it.
# Option “-x” is deprecated and might be removed in a later version of gnome-terminal.
# Use “-- ” to terminate the options and put the command line to execute after it.
cd /home/weston/workspace/optee-3.17/build/../out/bin && /home/weston/workspace/optee-3.17/build/../qemu/build/aarch64-softmmu/qemu-system
-aarch64 \
        -nographic \
        -serial tcp:localhost:54320 -serial tcp:localhost:54321 \
        -smp 4 \
        -s -S -machine virt,secure=on,gic-version=3,virtualization=false \
        -cpu cortex-a53 \
        -d unimp -semihosting-config enable=on,target=native \
        -m 2048 \
        -bios bl1.bin           \
        -initrd rootfs.cpio.gz \
        -kernel Image -no-acpi \
        -append 'console=ttyAMA0,38400 keep_bootcon root=/dev/vda2 ' \
         \
        -object rng-random,filename=/dev/urandom,id=rng0 -device virtio-rng-pci,rng=rng0,max-bytes=1024,period=1000 -netdev user,id=vmnic
-device virtio-net-device,netdev=vmnic
QEMU 6.0.0 monitor - type 'help' for more information
(qemu) c
(qemu) 
```

接下来会弹出两个窗口，一个是CA（Linux）窗口，一个是TA（OP-TEE）窗口。



```
NOTICE:  Booting Trusted Firmware
NOTICE:  BL1: v2.6(release):v2.6
NOTICE:  BL1: Built : 17:17:41, Jun 28 2022
INFO:    BL1: RAM 0xe04e000 - 0xe058000
INFO:    Using crypto library 'mbed TLS'
INFO:    BL1: Loading BL2
WARNING: Firmware Image Package header check failed.
INFO:    Loading image id=6 at address 0xe01b000
INFO:    Image id=6 loaded: 0xe01b000 - 0xe01b4b6
WARNING: Firmware Image Package header check failed.
INFO:    Loading image id=1 at address 0xe01b000
INFO:    Image id=1 loaded: 0xe01b000 - 0xe02d5d9
NOTICE:  BL1: Booting BL2
INFO:    Entry point address = 0xe01b000
INFO:    SPSR = 0x3c5
NOTICE:  BL2: v2.6(release):v2.6
NOTICE:  BL2: Built : 17:17:40, Jun 28 2022
INFO:    Using crypto library 'mbed TLS'
INFO:    BL2: Doing platform setup
INFO:    BL2: Loading image id 3
WARNING: Firmware Image Package header check failed.
INFO:    Loading image id=7 at address 0xe040000
INFO:    Image id=7 loaded: 0xe040000 - 0xe04060e
WARNING: Firmware Image Package header check failed.
INFO:    Loading image id=9 at address 0xe040000
INFO:    Image id=9 loaded: 0xe040000 - 0xe0404da
WARNING: Firmware Image Package header check failed.
INFO:    Loading image id=13 at address 0xe040000
INFO:    Image id=13 loaded: 0xe040000 - 0xe040430
WARNING: Firmware Image Package header check failed.
INFO:    Loading image id=3 at address 0xe040000
INFO:    Image id=3 loaded: 0xe040000 - 0xe04806c
INFO:    BL2: Loading image id 4
WARNING: Firmware Image Package header check failed.
INFO:    Loading image id=10 at address 0xe100000
INFO:    Image id=10 loaded: 0xe100000 - 0xe1004e8
WARNING: Firmware Image Package header check failed.
INFO:    Loading image id=14 at address 0xe100000
INFO:    Image id=14 loaded: 0xe100000 - 0xe1004ce
WARNING: Firmware Image Package header check failed.
INFO:    Loading image id=4 at address 0xe100000
INFO:    Image id=4 loaded: 0xe100000 - 0xe10001c
INFO:    OPTEE ep=0xe100000
INFO:    OPTEE header info:
INFO:          magic=0x4554504f
INFO:          version=0x2
INFO:          arch=0x1
INFO:          flags=0x0
```

```
I/TC: Non-secure external DT found
D/TC:0 0 carve_out_phys_mem:283 No need to carve out 0xe100000 size 0x200000
D/TC:0 0 carve_out_phys_mem:283 No need to carve out 0xe300000 size 0xd00000
I/TC: Embedded DTB found
D/TC:0 0 get_console_node_from_dt:72 No console directive from DTB
I/TC: OP-TEE version: 3.17.0 (gcc version 10.2.1 20201103 (GNU Toolchain for the A-profile Architecture 10.2-2020
-10.16))) #1 2022年 06月 28日 星期二 09:13:07 UTC aarch64
I/TC: WARNING: This OP-TEE configuration might be insecure!
I/TC: WARNING: Please check https://optee.readthedocs.io/en/latest/architecture/porting_guidelines.html
I/TC: Primary CPU initializing
D/TC:0 0 boot_init_primary_late:1303 Executing at offset 0xd6d3b000 with virtual load address 0xe4e3b000
D/TC:0 0 call_preinitcalls:21 level 2 mobj_mapped_shm_init()
D/TC:0 0 mobj_mapped_shm_init:463 Shared memory address range: e1e00000, e3e00000
D/TC:0 0 call_initcalls:40 level 1 register_time_source()
D/TC:0 0 call_initcalls:40 level 1 teecore_init_pub_ram()
D/TC:0 0 call_initcalls:40 level 2 probe_dt_drivers_early()
D/TC:0 0 add_node_to_probe:547 element: dt-test-consumer on node dt-test-consumer
D/TC:0 0 add_node_to_probe:547 element: dt-test-bus-b0 on node simple-bus
D/TC:0 0 add_node_to_probe:547 element: dt-test-crypt-consumer on node dt-test-crypt-consumer
D/TC:0 0 probe_driver_node:358 element: dt-test-crypt-consumer on node dt-test-crypt-consumer deferred 1 time(s)
D/TC:0 0 add_node_to_probe:547 element: dt-test-bus-b1 on node simple-bus
D/TC:0 0 probe_driver_node:352 element: simple-bus on node dt-test-bus-b0 initialized
D/TC:0 0 probe_driver_node:358 element: dt-test-consumer on node dt-test-consumer deferred 1 time(s)
D/TC:0 0 probe_driver_node:358 element: dt-test-consumer on node dt-test-consumer deferred 2 time(s)
D/TC:0 0 add_node_to_probe:547 element: dt-test-bus-b2 on node simple-bus
D/TC:0 0 probe_driver_node:352 element: simple-bus on node dt-test-bus-b1 initialized
D/TC:0 0 probe_driver_node:358 element: dt-test-crypt-consumer on node dt-test-crypt-consumer deferred 2 time(s)
D/TC:0 0 probe_driver_node:358 element: dt-test-crypt-consumer on node dt-test-crypt-consumer deferred 3 time(s)
D/TC:0 0 add_node_to_probe:547 element: dt-test-bus-b3 on node simple-bus
D/TC:0 0 probe_driver_node:352 element: simple-bus on node dt-test-bus-b2 initialized
D/TC:0 0 probe_driver_node:358 element: dt-test-consumer on node dt-test-consumer deferred 3 time(s)
D/TC:0 0 probe_driver_node:358 element: dt-test-consumer on node dt-test-consumer deferred 4 time(s)
D/TC:0 0 add_node_to_probe:547 element: dt-test-provider@0 on node dt_test_rstctrl_provider
D/TC:0 0 add_node_to_probe:547 element: dt-test-provider@0 on node dt_test_clock_provider
D/TC:0 0 probe_driver_node:352 element: simple-bus on node dt-test-bus-b3 initialized
D/TC:0 0 probe_driver_node:358 element: dt-test-crypt-consumer on node dt-test-crypt-consumer deferred 4 time(s)
D/TC:0 0 probe_driver_node:358 element: dt-test-crypt-consumer on node dt-test-crypt-consumer deferred 5 time(s)
D/TC:0 0 clk_register:104 Registered clock dt_test-clk3, freq 0
D/TC:0 0 clk_register:104 Registered clock dt_test-clk7, freq 0
D/TC:0 0 probe_driver_node:352 element: dt_test_clock_provider on node dt-test-provider@0 initialized
D/TC:0 0 probe_driver_node:352 element: dt_test_rstctrl_provider on node dt-test-provider@0 initialized
D/TC:0 0 probe_driver_node:352 element: dt-test-consumer on node dt-test-consumer initialized
D/TC:0 0 probe_driver_node:358 element: dt-test-crypt-consumer on node dt-test-crypt-consumer deferred 6 time(s)
D/TC:0 0 process_probe_list:496 Unresolved dependencies after 6 rounds, 6 deferred
D/TC:0 0 probe_dt_drivers_early:684 Deferred drivers probing
D/TC:0 0 print_probe_list:306 Probe list: 1 elements
D/TC:0 0 print_probe_list:308 |- Driver dt-test-crypt-consumer probes on node dt-test-crypt-consumer
D/TC:0 0 print_probe_list:312 `- Probe list end
```