Qemu System mode quick Ref

前言/概述

虽然固件模拟运行时有Firmadyne，Firmware-Analysis-Toolkit等自动化工具，但是使用qemu-system模式快速运行MIPS、ARM架构虚拟机对固件的文件系统进行分析调试在一些情况下仍是必要的，所以在查阅资料与测试后将命令记录下来方便执行时查询。

主要记录了qemu模拟运行与端口转发的配置。

快速运行

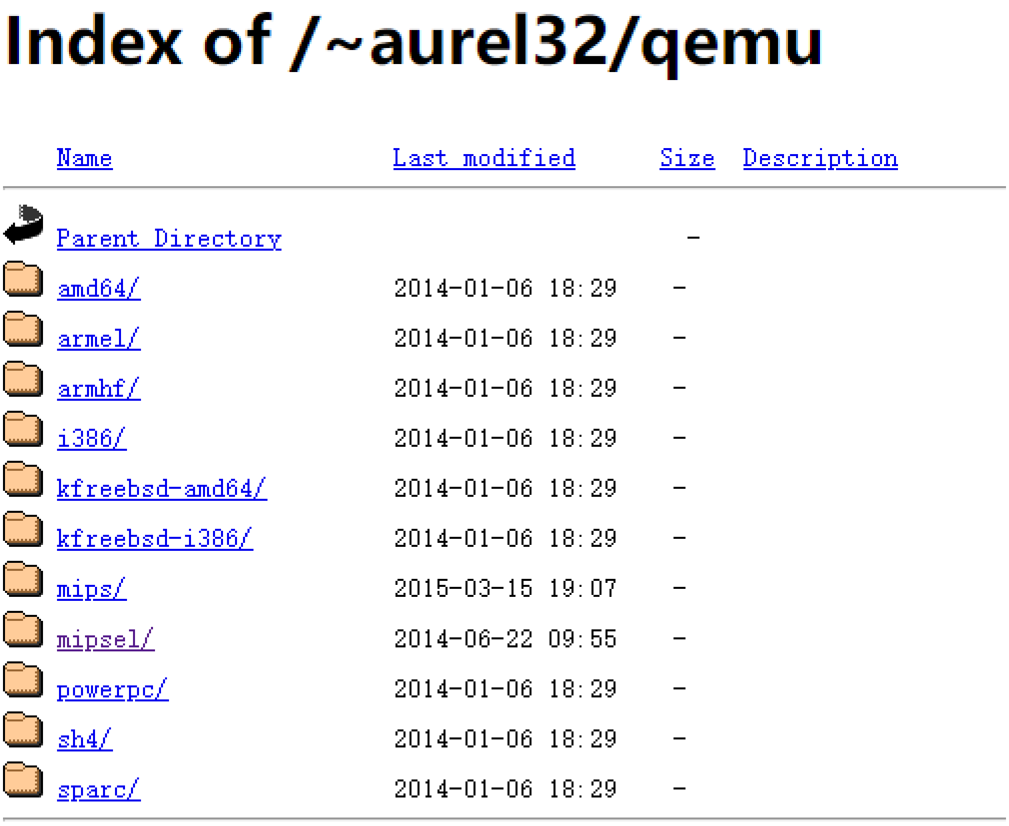
准备

1. Linux操作系统，安装Qemu

```
#Ubuntu 系统
sudo apt install qemu
```

2. 下载对应架构的镜像

   https://people.debian.org/~aurel32/qemu/

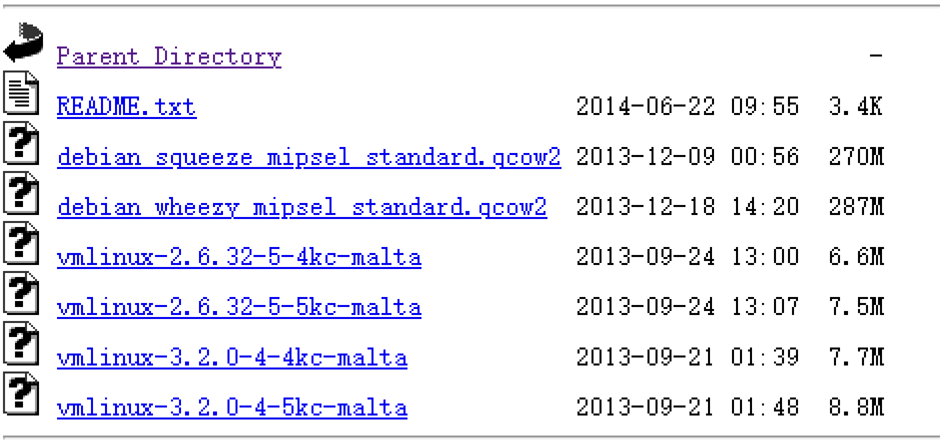


Index of /~aurel32/qemu

Name	Last modified	Size	Description
Parent Directory		-	
amd64/	2014-01-06 18:29	-	
armel/	2014-01-06 18:29	-	
armhf/	2014-01-06 18:29	-	
i386/	2014-01-06 18:29	-	
kfreebsd-amd64/	2014-01-06 18:29	-	
kfreebsd-i386/	2014-01-06 18:29	-	
mips/	2015-03-15 19:07	-	
mipsel/	2014-06-22 09:55	-	
powerpc/	2014-01-06 18:29	-	
sh4/	2014-01-06 18:29	-	
sparc/	2014-01-06 18:29	-	

运行

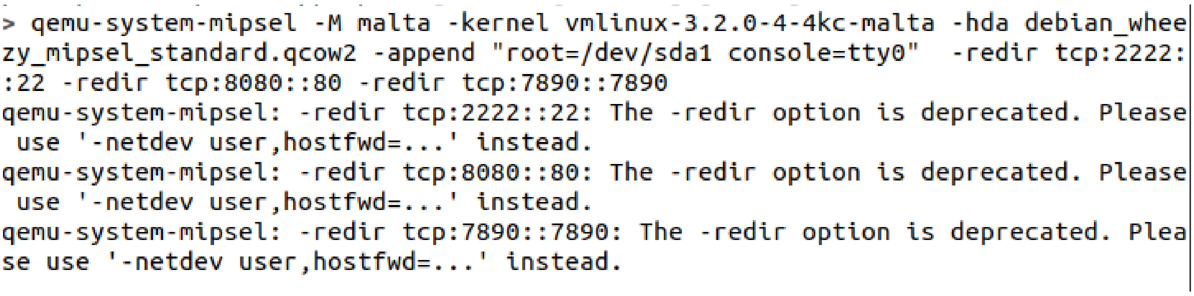
接下来以运行mipsel架构 32位debian_wheezy机器为例。



Parent Directory		-
README.txt	2014-06-22 09:55	3.4K
debian_squeeze_mipsel_standard.qcow2	2013-12-09 00:56	270M
debian_wheezy_mipsel_standard.qcow2	2013-12-18 14:20	287M
vmlinux-2.6.32-5-4kc-malta	2013-09-24 13:00	6.6M
vmlinux-2.6.32-5-5kc-malta	2013-09-24 13:07	7.5M
vmlinux-3.2.0-4-4kc-malta	2013-09-21 01:39	7.7M
vmlinux-3.2.0-4-5kc-malta	2013-09-21 01:48	8.8M

在终端中执行

```
qemu-system-mipsel -M malta -kernel vmlinux-3.2.0-4-4kc-malta -hda debian_wheezy_mipsel_standard.qcow2 -append "root=/dev/sda1 console=tty0"  -redir tcp:2222::22 -redir tcp:8080::80 -redir tcp:7890::7890
```



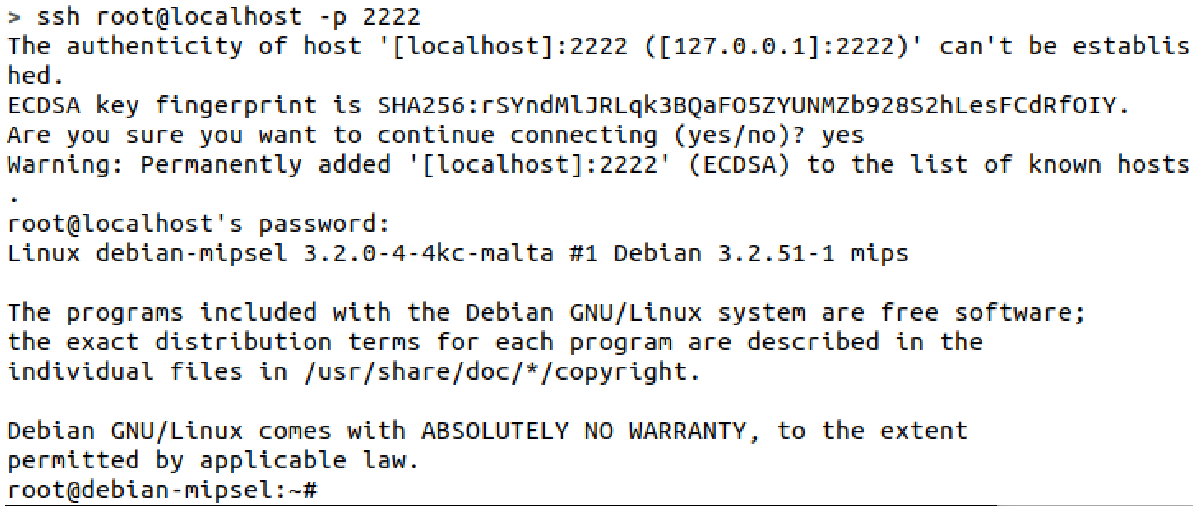
```
> qemu-system-mipsel -M malta -kernel vmlinux-3.2.0-4-4kc-malta -hda debian_whee
zy_mipsel_standard.qcow2 -append "root=/dev/sda1 console=tty0"  -redir tcp:2222:
:22 -redir tcp:8080::80 -redir tcp:7890::7890
qemu-system-mipsel: -redir tcp:2222::22: The -redir option is deprecated. Please
 use '-netdev user,hostfwd=...' instead.
qemu-system-mipsel: -redir tcp:8080::80: The -redir option is deprecated. Please
 use '-netdev user,hostfwd=...' instead.
qemu-system-mipsel: -redir tcp:7890::7890: The -redir option is deprecated. Plea
se use '-netdev user,hostfwd=...' instead.
```

虽然提示redir参数（端口转发）已经废弃，但是在QEMU emulator version 2.11.1(Debian 1:2.11+dfsg-1ubuntu7.32)中仍然正常工作。

或者使用以下命令端口转发

```
qemu-system-mipsel -M malta -kernel vmlinux-3.2.0-4-4kc-malta -hda debian_wheezy_mipsel_standard.qcow2 -append "root=/dev/sda1 console=tty0"  -netdev user,id=ethernet.0,hostfwd=tcp::2222-:22,hostfwd=tcp::8080-:80 -device rtl8139,netdev=ethernet.0
```

ssh登录虚拟机，成功运行。



```
> ssh root@localhost -p 2222
The authenticity of host '[localhost]:2222 ([127.0.0.1]:2222)' can't be establis
hed.
ECDSA key fingerprint is SHA256:rSYndMlJRLqk3BQaFO5ZYUNMZb928S2hLesFCdRfOIY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:2222' (ECDSA) to the list of known hosts
.
root@localhost's password:
Linux debian-mipsel 3.2.0-4-4kc-malta #1 Debian 3.2.51-1 mips

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@debian-mipsel:~#
```

接下来使用scp命令传输固件文件系统与对应架构下的gdb-server远程调试。

快速运行命令列表

1. mipsel 32bit debian wheezy

```
qemu-system-mipsel -M malta -kernel vmlinux-3.2.0-4-4kc-malta -hda debian_wheezy_mipsel_standard.qcow2 -append "root=/dev/sda1 console=tty0"  -netdev user,id=ethernet.0,hostfwd=tcp::2222-:22,hostfwd=tcp::8080-:80,hostfwd=tcp::8443-:443 -device rtl8139,netdev=ethernet.0
```

2. mipsel 64bit debian wheezy

```
qemu-system-mips64el -M malta -kernel vmlinux-3.2.0-4-5kc-malta -hda debian_wheezy_mipsel_standard.qcow2 -append "root=/dev/sda1 console=tty0" -netdev user,id=ethernet.0,hostfwd=tcp::2222-:22,hostfwd=tcp::8080-:80,hostfwd=tcp::8443-:443 -device rtl8139,netdev=ethernet.0
```

3. mips 32bit debian wheezy

```
qemu-system-mips -M malta -kernel vmlinux-3.2.0-4-4kc-malta -hda debian_wheezy_mips_standard.qcow2 -append "root=/dev/sda1 console=tty0" -netdev user,id=ethernet.0,hostfwd=tcp::2222-:22,hostfwd=tcp::8080-:80,hostfwd=tcp::8443-:443 -device rtl8139,netdev=ethernet.0
```

4. mips 64bit debian wheezy

```
qemu-system-mips64 -M malta -kernel vmlinux-3.2.0-4-5kc-malta -hda debian_wheezy_mips_standard.qcow2 -append "root=/dev/sda1 console=tty0" -netdev user,id=ethernet.0,hostfwd=tcp::2222-:22,hostfwd=tcp::8080-:80,hostfwd=tcp::8443-:443 -device rtl8139,netdev=ethernet.0
```

5. armel debian wheezy

```
qemu-system-arm -M versatilepb -kernel vmlinuz-3.2.0-4-versatile -initrd
initrd.img-3.2.0-4-versatile -hda debian_wheezy_armel_standard.qcow2 -append
"root=/dev/sda1" -netdev
user,id=ethernet.0,hostfwd=tcp::2222-:22,hostfwd=tcp::8080-:80,hostfwd=tcp::
8443-:443 -device rtl8139,netdev=ethernet.0
```

详细解释

- -M 参数

  -M -machine 选择模拟机器类型

- -append 参数

  `-append` 中可以传递许多 kernel parameter， 需要用单引号或双引号将 他们包起来

- -kernel -initrd

  手动指定 kernel 和 initrd

- -hda

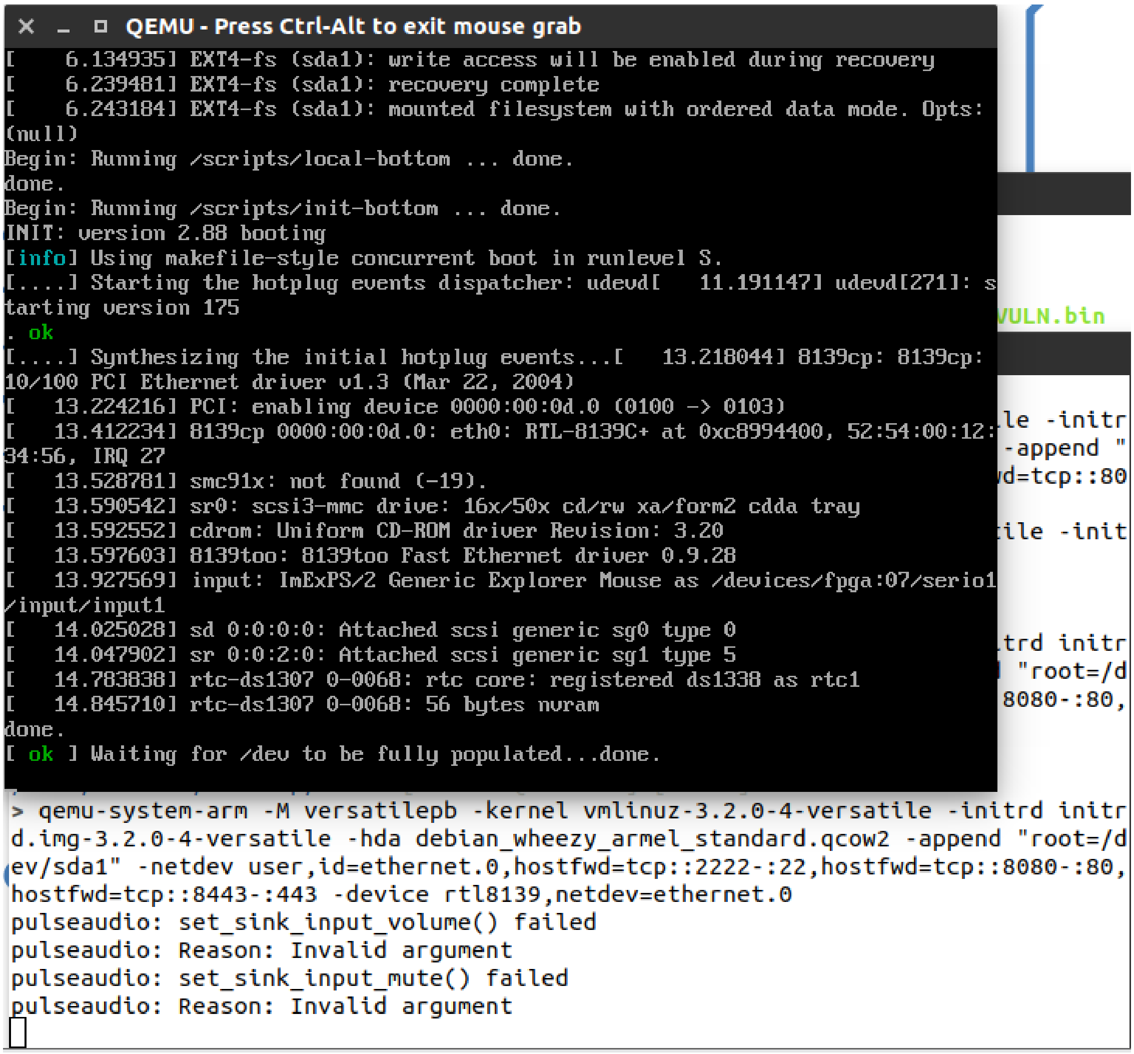
  指定硬盘镜像

- -device -netdev

  设置网络设备，并配置端口转发

- -nographic

  不显示图形界面



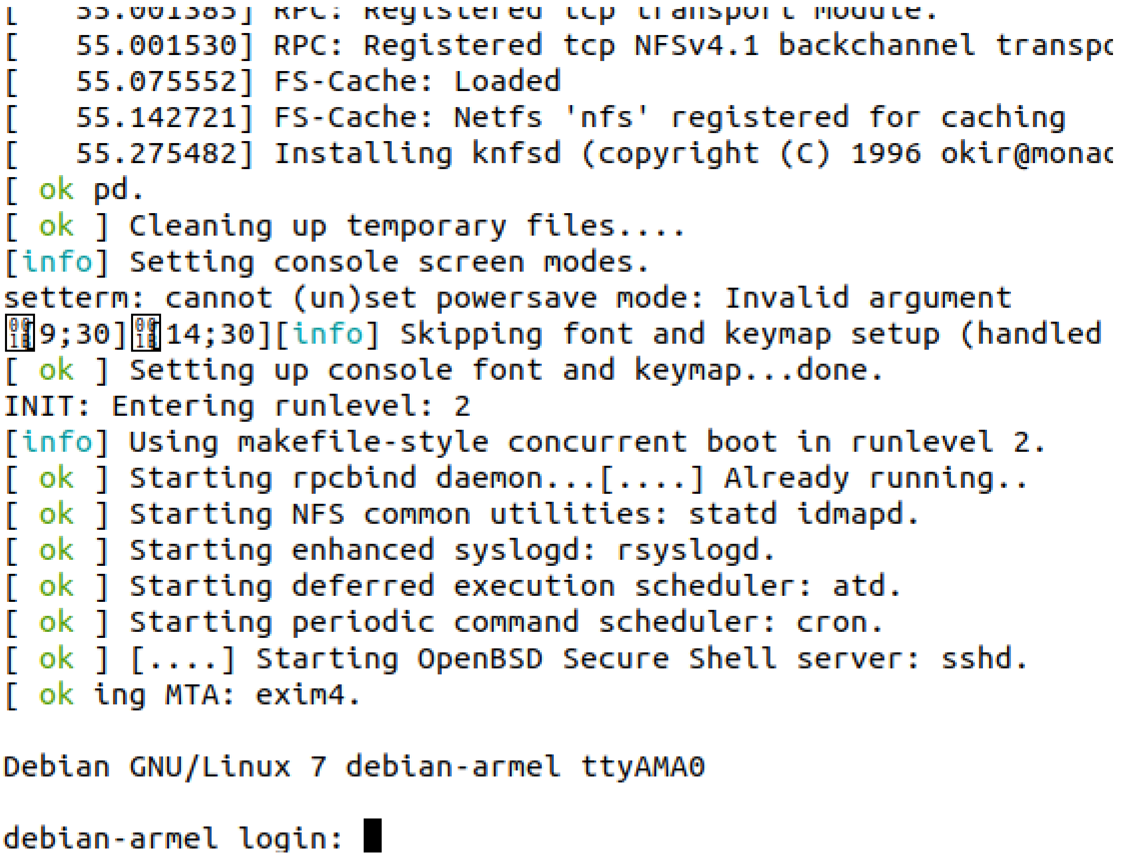
```
[    6.134935] EXT4-fs (sda1): write access will be enabled during recovery
[    6.239481] EXT4-fs (sda1): recovery complete
[    6.243184] EXT4-fs (sda1): mounted filesystem with ordered data mode. Opts:
(null)
Begin: Running /scripts/local-bottom ... done.
done.
Begin: Running /scripts/init-bottom ... done.
INIT: version 2.88 booting
[info] Using makefile-style concurrent boot in runlevel S.
[....] Starting the hotplug events dispatcher: udevd[   11.191147] udevd[271]: s
tarting version 175
. ok
[....] Synthesizing the initial hotplug events...[   13.218044] 8139cp: 8139cp:
10/100 PCI Ethernet driver v1.3 (Mar 22, 2004)
[   13.224216] PCI: enabling device 0000:00:0d.0 (0100 -> 0103)
[   13.412234] 8139cp 0000:00:0d.0: eth0: RTL-8139C+ at 0xc8994400, 52:54:00:12:
34:56, IRQ 27
[   13.528781] smc91x: not found (-19).
[   13.590542] sr0: scsi3-mmc drive: 16x/50x cd/rw xa/form2 cdda tray
[   13.592552] cdrom: Uniform CD-ROM driver Revision: 3.20
[   13.597603] 8139too: 8139too Fast Ethernet driver 0.9.28
[   13.927569] input: ImExPS/2 Generic Explorer Mouse as /devices/fpga:07/serio1
/input/input1
[   14.025028] sd 0:0:0:0: Attached scsi generic sg0 type 0
[   14.047902] sr 0:0:2:0: Attached scsi generic sg1 type 5
[   14.783838] rtc-ds1307 0-0068: rtc core: registered ds1338 as rtc1
[   14.845710] rtc-ds1307 0-0068: 56 bytes nvram
done.
[ ok ] Waiting for /dev to be fully populated...done.
```

```
VULN.bin
le -initr
 -append "
d=tcp::80
ile -init
trd initr
 "root=/d
8080-:80,
```

```
> qemu-system-arm -M versatilepb -kernel vmlinuz-3.2.0-4-versatile -initrd initr
d.img-3.2.0-4-versatile -hda debian_wheezy_armel_standard.qcow2 -append "root=/d
ev/sda1" -netdev user,id=ethernet.0,hostfwd=tcp::2222-:22,hostfwd=tcp::8080-:80,
hostfwd=tcp::8443-:443 -device rtl8139,netdev=ethernet.0
pulseaudio: set_sink_input_volume() failed
pulseaudio: Reason: Invalid argument
pulseaudio: set_sink_input_mute() failed
pulseaudio: Reason: Invalid argument
```

根据README.txt 在append参数"console=tty0"替换为"console=ttyS0"或者在结尾添加"console=ttyAMA0"。

```
qemu-system-mipsel -M malta -kernel vmlinux-3.2.0-4-4kc-malta -hda debian_wheezy_mipsel_standard.qcow2 -append "root=/dev/sda1 console=tty0"  -netdev user,id=ethernet.0,hostfwd=tcp::2222-:22,hostfwd=tcp::8080-:80,hostfwd=tcp::8443-:443 -device rtl8139,netdev=ethernet.0
#====================
qemu-system-mipsel -M malta -kernel vmlinux-3.2.0-4-4kc-malta -hda debian_wheezy_mipsel_standard.qcow2 -append "root=/dev/sda1 console=ttyS0" -netdev user,id=ethernet.0,hostfwd=tcp::2222-:22,hostfwd=tcp::8080-:80,hostfwd=tcp::8443-:443 -device rtl8139,netdev=ethernet.0
#################################
qemu-system-arm -M versatilepb -kernel vmlinuz-3.2.0-4-versatile -initrd initrd.img-3.2.0-4-versatile -hda debian_wheezy_armel_standard.qcow2 -append "root=/dev/sda1" -netdev user,id=ethernet.0,hostfwd=tcp::2222-:22,hostfwd=tcp::8080-:80,hostfwd=tcp::8443-:443 -device rtl8139,netdev=ethernet.0
#====================
qemu-system-arm -M versatilepb -kernel vmlinuz-3.2.0-4-versatile -initrd initrd.img-3.2.0-4-versatile -hda debian_wheezy_armel_standard.qcow2 -append "root=/dev/sda1 console=ttyAMA0 -netdev user,id=ethernet.0,hostfwd=tcp::2222-:22,hostfwd=tcp::8080-:80,hostfwd=tcp::8443-:443 -device rtl8139,netdev=ethernet.0
```



```
[   55.001385] RPC: Registered tcp transport module.
[   55.001530] RPC: Registered tcp NFSv4.1 backchannel transpo
[   55.075552] FS-Cache: Loaded
[   55.142721] FS-Cache: Netfs 'nfs' registered for caching
[   55.275482] Installing knfsd (copyright (C) 1996 okir@monac
[ ok pd.
[ ok ] Cleaning up temporary files....
[info] Setting console screen modes.
setterm: cannot (un)set powersave mode: Invalid argument
□9;30]□14;30][info] Skipping font and keymap setup (handled
[ ok ] Setting up console font and keymap...done.
INIT: Entering runlevel: 2
[info] Using makefile-style concurrent boot in runlevel 2.
[ ok ] Starting rpcbind daemon...[....] Already running..
[ ok ] Starting NFS common utilities: statd idmapd.
[ ok ] Starting enhanced syslogd: rsyslogd.
[ ok ] Starting deferred execution scheduler: atd.
[ ok ] Starting periodic command scheduler: cron.
[ ok ] [....] Starting OpenBSD Secure Shell server: sshd.
[ ok ing MTA: exim4.

Debian GNU/Linux 7 debian-armel ttyAMA0

debian-armel login: █
```

Q&A

1. ssh登录失败

   ~/.ssh/known_hosts 文件中删除之前记录的机器信息

参考资料

1. qemu man page
2. Arch Linux Wiki Qemu文档
3. Debian on an emulated MIPS(EL) machine
4. 通过QEMU 和 IDA Pro远程调试设备固件 – cssembly
5. EmbedOS