

# CCP907T SDF 虚拟化使用说明

## V1.0

文件修改履历表:

版本号	文件修改描述	修订者	日期
V1.0	创建	李玲勇	2021-06-16

# 目 录

1. 简介 .....	3
2. CCP907T 虚拟化开发环境搭建 .....	3
2.1 判断平台是否支持虚拟化技术 .....	3
2.2 AMD R9 平台 BIOS 虚拟化配置 .....	3
2.3 INTEL XEON 平台虚拟化配置 .....	3
2.4 虚拟机安装 .....	4
3. CCP907T SDF 虚拟化程序运行 .....	5
3.1 安装 PF 驱动 .....	5
3.2 虚拟机 PCIE 设备配置 .....	6
3.3 安装 VF 驱动和内核模块 .....	7
3.4 运行测试程序 .....	7

## 1. 简介

本文主要介绍了在 AMD R9 平台和 INTEL XEON 平台上 CCP907T 密码卡 SDF 虚拟化环境的搭建和使用。所使用的软件有：

CCP907T PF 驱动；

CCP907T VF 驱动；

CCP907T SDF 内核库；

CCP907T SDF 应用层库；

CCP907T SDF 测试程序；

## 2. CCP907T 虚拟化开发环境搭建

### 2.1 判断平台是否支持虚拟化技术

- 1.使用 `egrep '(vmx|svm)' /proc/cpuinfo` 命令查看，如果没有输出说明 CPU 不支持虚拟化，需在 BIOS 中配置，或者需咨询 CPU 本身是否支持虚拟化技术。其中 `vmx` 表示 Intel-VT 技术，`svm` 表示 AMD-V 技术。
- 2.主板和 CPU 需支持 Intel 的 VT-d 或者 AMD 的 IOMMU 以及 PCI-SIG 的 IOV。通常情况下默认是关闭的，需在 BIOS 中重新配置或者修改 linux 系统启动参数。IOV 通过在硬件设备中增加一个 PCIE 设备，用于呈现一个 PF 或多个 VF，从而可以将每个 VF 单独分配给不同的虚拟机使用。

### 2.2 AMD R9 平台 BIOS 虚拟化配置

Advanced CPU Settings → SVM Mode Enabled (CPU 虚拟化)；

Chipset → IOMMU Enabled (PCIE 虚拟化)；

AMD CBS → ACS Enable Enable (不同 PCIE 总线使用不同 IOMMU 地址组)；

AMD CBS → PCIe ARI Support Enable (选择性开启，使用更多的 PCIE 总线号)；

AMD CBS → Enable AER Cap Auto (不要使用高级错误功能)；

### 2.3 INTEL XEON 平台虚拟化配置

启动虚拟机时提示 PCI Pass-through 的 ERROR 信息，可通过以下方式修改：

1. `cat /proc/cmdline | grep intel_iommu` 判断内核启动是否支持 `intel_iommu` 技术;
2. 若无上述启动参数, 把 `intel_iommu=on iommu=pt` 添加到 `grub` 配置文件的 `GRUB_CMDLINE_LINUX` 一行的最后。

`vi /etc/default/grub`

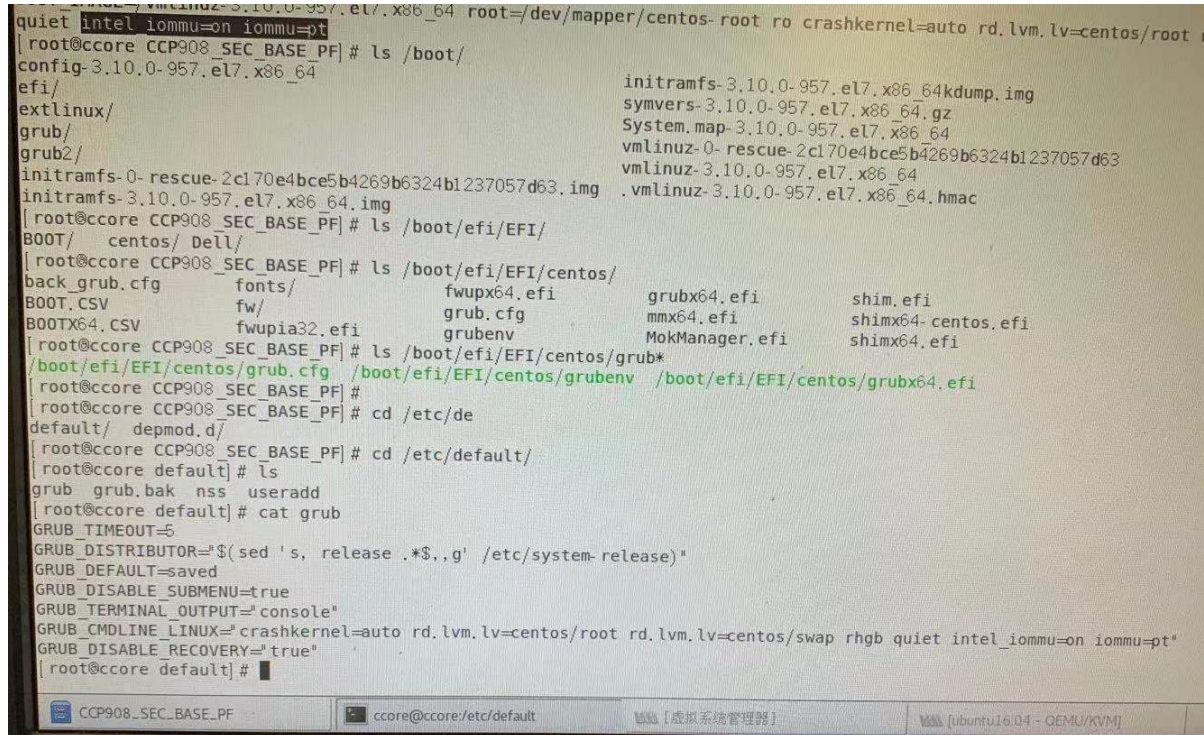


图 2.1 grub 配置信息

3. 刷新 `grub.cfg` 文件并重新启动主机生效。通过 `grub2-mkconfig -o /boot/grub2/grub.cfg` 重新生成 `grub.cfg` 文件。系统若是通过 `efi` 启动, 需将 `/boot/efi/EFI/centos/grub.cfg` 更新成上述生成的 `grub.cfg` 文件

## 2.4 虚拟机安装

1. `centos` 系统通常默认安装虚拟机管理程序, 测试机安装的是 `Ubuntu1804` 系统, 需手动安装 `qemu-kvm`:
  - a) `atp-get install qemu-kvm`
2. 安装 `libvirt` 虚拟化管理模块
  - a) `atp-get install libvirt`
3. 安装 `virt-manage`:
  - a) `apt-get install virt-manger`
4. 虚拟机安装系统:
  - a) 将虚拟机 ISO 文件拷贝入电脑, 打开 `virtual machine manager` 软件, 选择 `create a new virtual`

machine 在虚拟机中安装 linux 系统。

## 3.CCP907T SDF 虚拟化程序运行

### 3.1 安装 PF 驱动

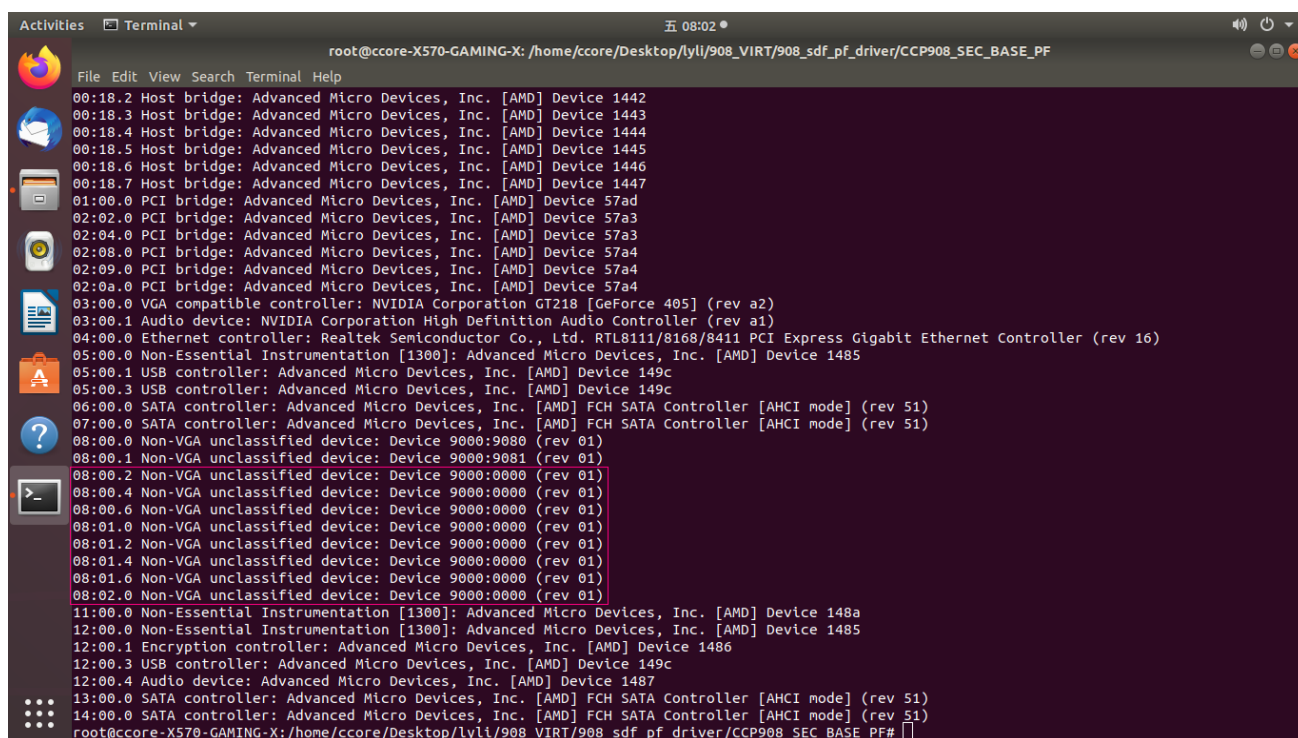
将 908\_sdf\_pf\_driver 考入主系统，进入 CCP907\_SEC\_BASE\_PF 目录，运行如下命令安装 PF 驱动：

```
make clean
```

```
make
```

```
insmod PCIE_CCP907_PF.ko
```

安装成功后，输入 `lspci` 命令，可以看到如下多出的 8 个 PCIE 设备（ID 号为 9000:0000）：



```
Activities Terminal 五 08:02
root@ccore-X570-GAMING-X: /home/ccore/Desktop/lyli/908_sdf_pf_driver/CCP908_SEC_BASE_PF
File Edit View Search Terminal Help
00:18.2 Host bridge: Advanced Micro Devices, Inc. [AMD] Device 1442
00:18.3 Host bridge: Advanced Micro Devices, Inc. [AMD] Device 1443
00:18.4 Host bridge: Advanced Micro Devices, Inc. [AMD] Device 1444
00:18.5 Host bridge: Advanced Micro Devices, Inc. [AMD] Device 1445
00:18.6 Host bridge: Advanced Micro Devices, Inc. [AMD] Device 1446
00:18.7 Host bridge: Advanced Micro Devices, Inc. [AMD] Device 1447
01:00.0 PCI bridge: Advanced Micro Devices, Inc. [AMD] Device 57ad
02:02.0 PCI bridge: Advanced Micro Devices, Inc. [AMD] Device 57a3
02:04.0 PCI bridge: Advanced Micro Devices, Inc. [AMD] Device 57a3
02:08.0 PCI bridge: Advanced Micro Devices, Inc. [AMD] Device 57a4
02:09.0 PCI bridge: Advanced Micro Devices, Inc. [AMD] Device 57a4
02:0a.0 PCI bridge: Advanced Micro Devices, Inc. [AMD] Device 57a4
03:00.0 VGA compatible controller: NVIDIA Corporation GT218 [GeForce 405] (rev a2)
03:00.1 Audio device: NVIDIA Corporation High Definition Audio Controller (rev a1)
04:00.0 Ethernet controller: Realtek Semiconductor Co., Ltd. RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller (rev 16)
05:00.0 Non-Essential Instrumentation [1300]: Advanced Micro Devices, Inc. [AMD] Device 1485
05:00.1 USB controller: Advanced Micro Devices, Inc. [AMD] Device 149c
05:00.3 USB controller: Advanced Micro Devices, Inc. [AMD] Device 149c
06:00.0 SATA controller: Advanced Micro Devices, Inc. [AMD] FCH SATA Controller [AHCI mode] (rev 51)
07:00.0 SATA controller: Advanced Micro Devices, Inc. [AMD] FCH SATA Controller [AHCI mode] (rev 51)
08:00.0 Non-VGA unclassified device: Device 9000:9080 (rev 01)
08:00.1 Non-VGA unclassified device: Device 9000:9081 (rev 01)
08:00.2 Non-VGA unclassified device: Device 9000:0000 (rev 01)
08:00.4 Non-VGA unclassified device: Device 9000:0000 (rev 01)
08:00.6 Non-VGA unclassified device: Device 9000:0000 (rev 01)
08:01.0 Non-VGA unclassified device: Device 9000:0000 (rev 01)
08:01.2 Non-VGA unclassified device: Device 9000:0000 (rev 01)
08:01.4 Non-VGA unclassified device: Device 9000:0000 (rev 01)
08:01.6 Non-VGA unclassified device: Device 9000:0000 (rev 01)
08:02.0 Non-VGA unclassified device: Device 9000:0000 (rev 01)
11:00.0 Non-Essential Instrumentation [1300]: Advanced Micro Devices, Inc. [AMD] Device 148a
12:00.0 Non-Essential Instrumentation [1300]: Advanced Micro Devices, Inc. [AMD] Device 1485
12:00.1 Encryption controller: Advanced Micro Devices, Inc. [AMD] Device 1486
12:00.3 USB controller: Advanced Micro Devices, Inc. [AMD] Device 149c
12:00.4 Audio device: Advanced Micro Devices, Inc. [AMD] Device 1487
13:00.0 SATA controller: Advanced Micro Devices, Inc. [AMD] FCH SATA Controller [AHCI mode] (rev 51)
14:00.0 SATA controller: Advanced Micro Devices, Inc. [AMD] FCH SATA Controller [AHCI mode] (rev 51)
root@ccore-X570-GAMING-X: /home/ccore/Desktop/lyli/908_sdf_pf_driver/CCP908_SEC_BASE_PF
```

图 3.1 虚拟出的 PCIE 设备

## 3.2 虚拟机 PCIE 设备配置

打开虚拟机，右击选择 Add Hardware 添加虚拟化出的 PCIE 设备：

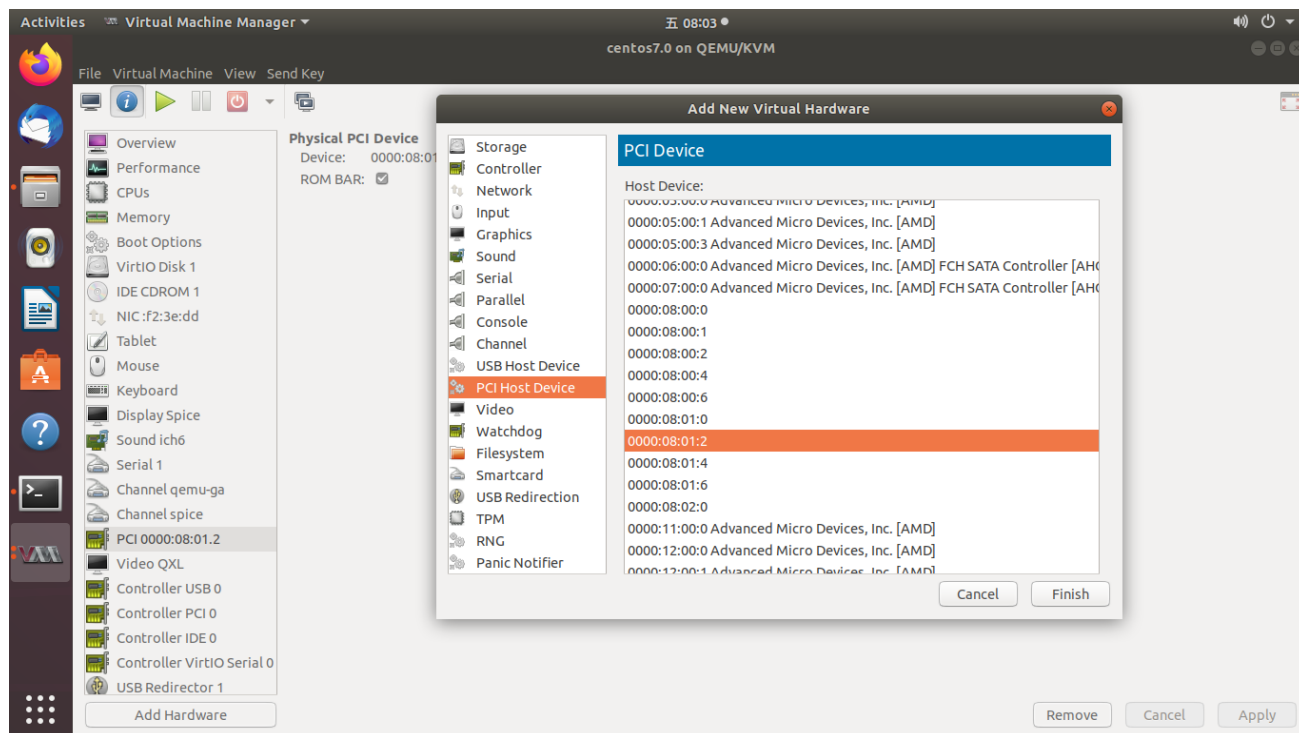


图 3.2 虚拟机添加虚拟出的 PCIE 设备

启动虚拟机，输入 `lspci` 命令可以看到添加的设备（设备 ID 为 9000:0000）：

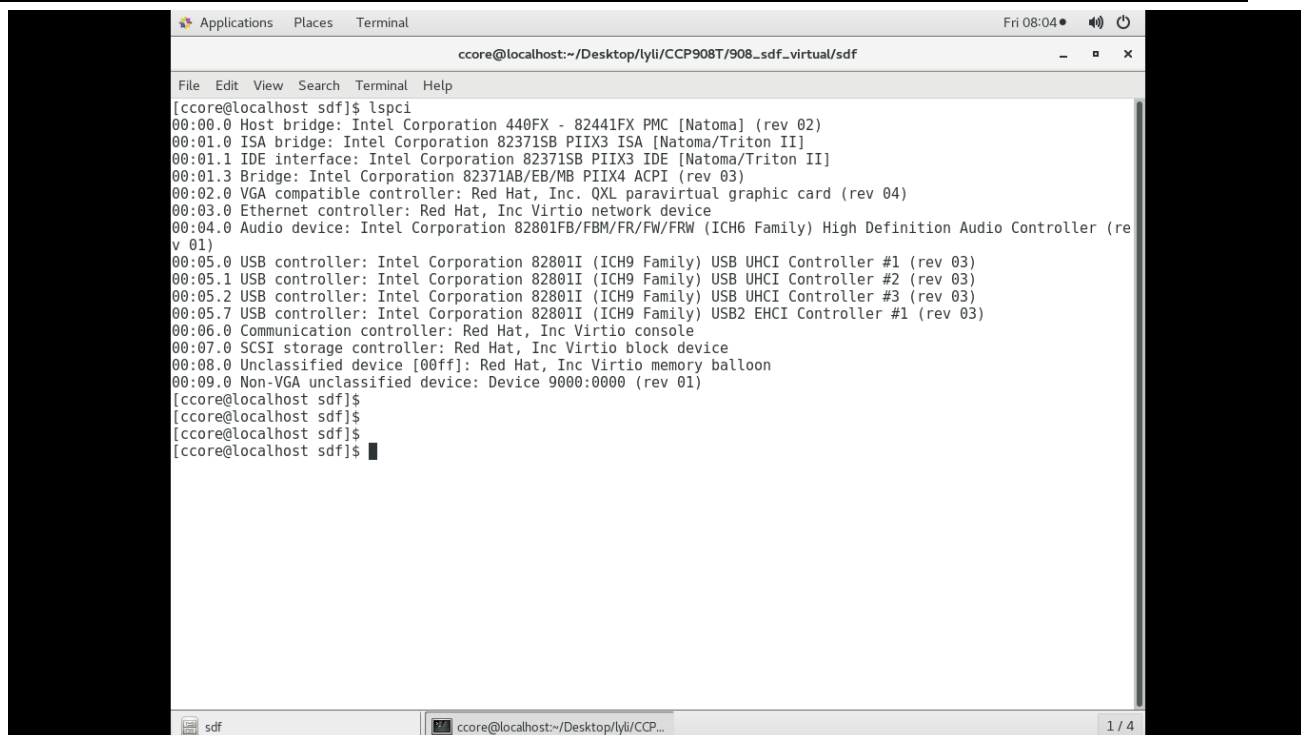


图 3.3 虚拟机中识别的 PCIE 设备

### 3.3 安装 VF 驱动和内核模块

将 908\_sdf\_virtual 文件夹考入虚拟机系统中，进入 sdf 目录，运行

```
source script/build_sdf.sh
```

```
source script/insmod_sdf.sh
```

编译并安装 PCIE\_CCP907\_VF.ko 和 ntl\_crypto.ko 两个内核 ko 文件。

### 3.4 运行测试程序

将 LIB 目录下 libsdf\_crypto.so 库文件拷贝至 sdf\_test 目录下，编辑 main.c 文件，打开不同的宏定义保存后，输入如下命令：

```
make clean
```

```
make
```

```
source run_command.sh
```

```
./sdfest
```

进行不同测试项的测试。