## VM功能测试用例

### 验证不同VM内，同个uuid的TA同时加载

**[测试步骤]**

1. 创建VM1，VM2

2. VM1中编写CA1/TA, VM2中编写CA2/TA

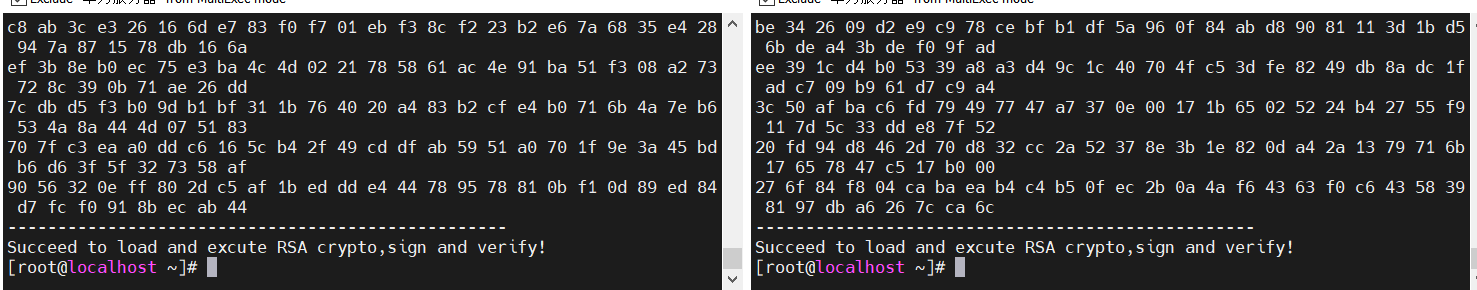
3. 在VM1,VM2中同时运行CA1/TA,CA2/TA，预期结果1

**[预期结果]**

1. VM1和VM2中的TA均加载成功

**[测试结论及现象]**

符合预期



### 验证VM部署下的安全存储存储于该VM下的目录

**[测试步骤]**

1. 创建VM,启动VM中的CA/TA

2. 通过CA调用接口secstorage\_create\_file去调用TA侧，传入正确的参数

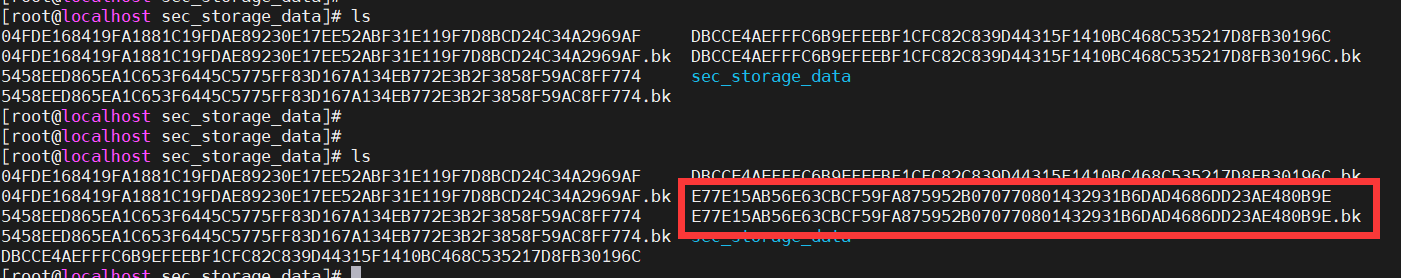
3. 查看输出结果，查看/var/itrustee/sec\_storage\_data日志信息

**[预期结果]**

1.CA运行成功，在VM /var/itrustee/sec\_storage\_data目录下，生成目标文件。

**[测试结论及现象]**

符合预期



### 验证VM部署下的TA日志存储于该VM下的目录

**[测试步骤]**

1. 创建VM,启动VM中的CA/TA

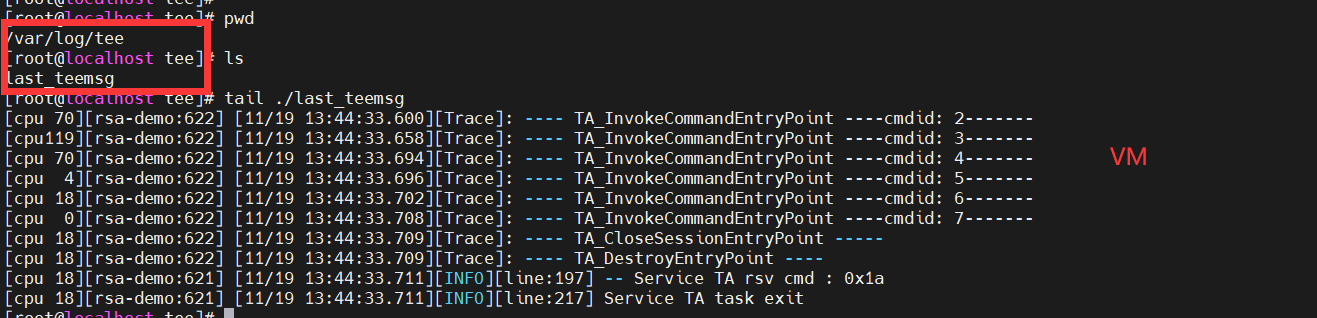
2. 查看输出结果，VM内和host侧启动tlogcat -f日志信息，预期结果1

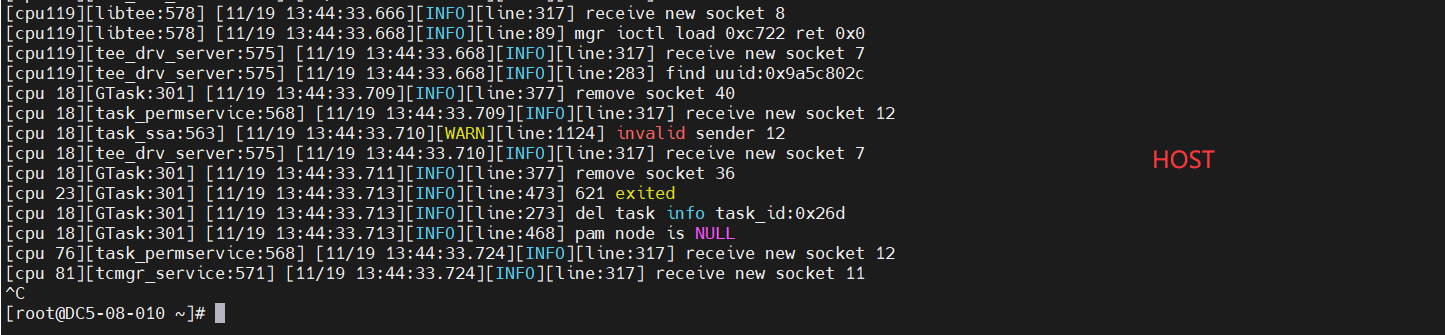
**[预期结果]**

1. CA/TA运行成功，日志存在于VM内目录/var/log/tee，host上不存在该TA日志

**[测试结论及现象]**

符合预期





### 验证host侧与VM内可同时运行CA/TA应用

**[测试步骤]**

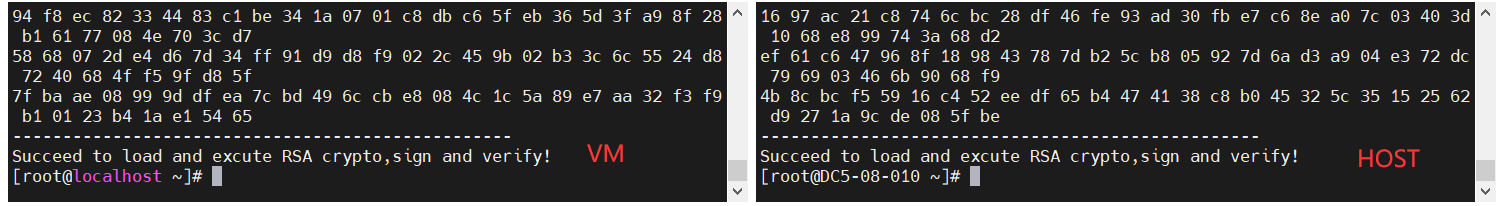
1. 同时启动VM和host侧中的CA/TA应用，预期结果1

**[预期结果]**

1.VM和host侧中的CA/TA应用均运行成功

**[测试结论及现象]**

符合预期



### Switchless功能测试

**[测试步骤]**

1. REE侧创建share memory 256M，预期结果1

2. 使传参方式为Switchless模式编写CA/TA, 预期结果2

3. CA发起线程数为：4，TA发起多线程：8

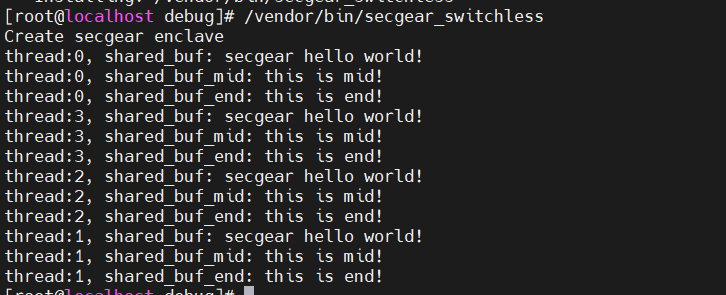
**[预期结果]**

1.内存创建成功；

2. 测试CA/TA成功运行

**[测试结论及现象]**

符合预期



### 验证VM内TA远程证明场景测试

**[测试步骤]**

1. REE侧虚机被拉起，虚机内radaemon启动，radaemon向raserver进行注册socket通道，raserver与radaemon建立连接；

2. raclient向raserver发起TA证明，携带TA uuid/nonce、虚机名、虚机type等；

3. raserver根据虚机名和虚机type，通过虚机管理命令行获取vmid和虚机名信息，向QTA注册：<vmid,vm-name>;

4. radaemon通过虚机名，找到连接的radaemon,发送: type+虚机名+TA uuid;

5. radaemon ->QTA-report: 用户证明参数+tzdriver获取的vmid;

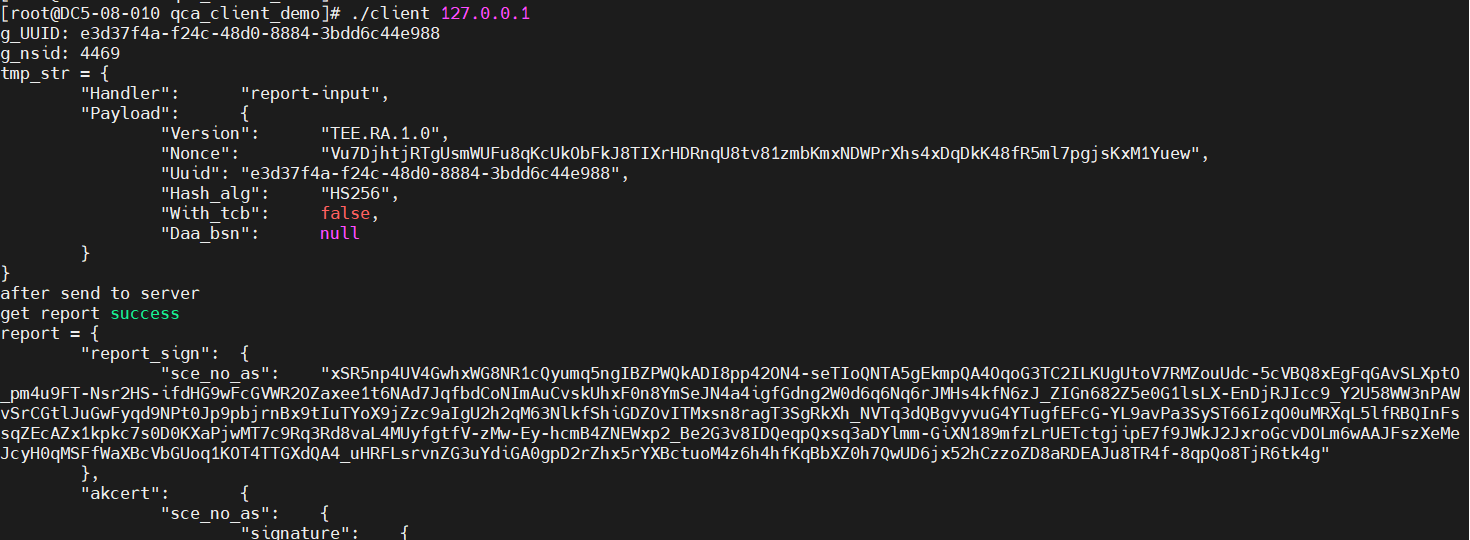
6. 报告返回：tcmgr -> QTA-report -> radaemon -> raserver，预期结果1

**[预期结果]**

预期结果1：用户可以从报告中验证 QTA-report的hash、虚机名与TA uuid

**[测试结论及现象]**

符合预期



## VM性能测试用例

### 基于itrust\_sdk,使用RSA-4096签名验签性能测试

**[测试步骤]**

1. 基于itrust\_sdk, 编写TA/CA测试程序调用RSA-4096加解密函数

2. 分别在host侧和VM内运行TA/CA测试程序，记录接口函数调用时间t1,t2，预期结果1

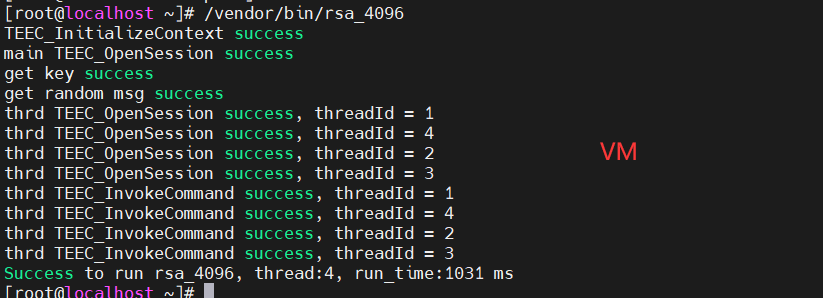
3. CA发起线程数为：4，TA发起多线程：8

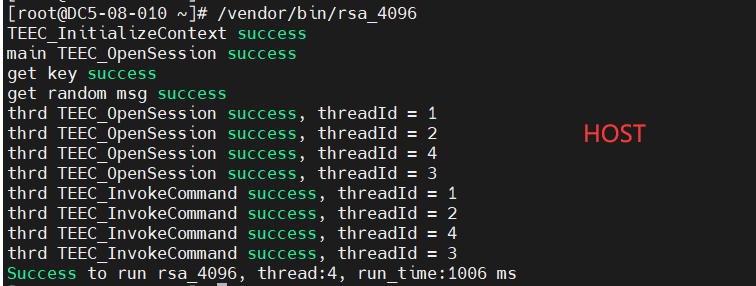
**[预期结果]**

1.VM内性能指标低于10%

**[测试结论及现象]**

符合预期





### 基于switchless,使用RSA-4096签名验签性能测试

**[测试步骤]**

1. 基于switchless, 编写TA/CA测试程序调用RSA-4096加解密函数

2. 分别在host侧和VM内运行TA/CA测试程序，记录接口函数调用时间t1,t2，预期结果1

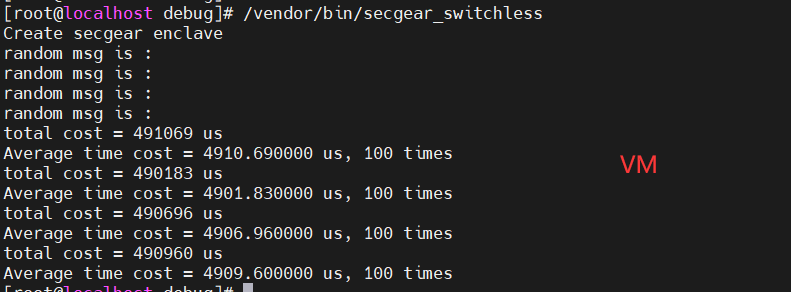
3. CA发起线程数为：4，TA发起多线程：8

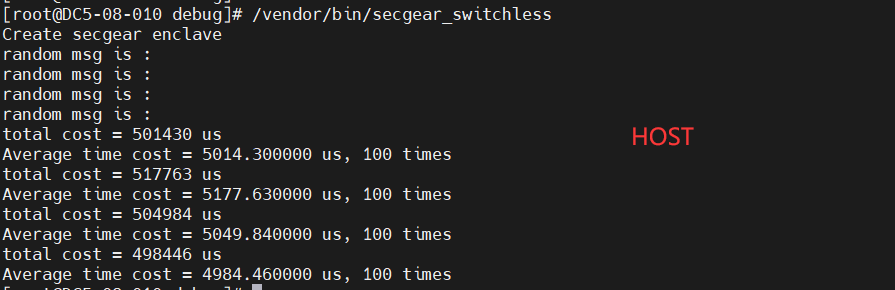
**[预期结果]**

1.VM内性能指标低于10%

**[测试结论及现象]**

符合预期





## SEC驱动用例

### huk密钥派生，salt不同长度测试

**[测试步骤]**

1、CA发起salt长度分别为1、32、255、1023，密钥长度64的huk密钥派生请求。（TA内申请内存即可）

2、CA发起salt长度64，密钥长度16、32、255、4096、4097的huk密钥派生

3、两次发送相同salt，返回的密钥一致

**[预期结果]**

1、获取最大长度，

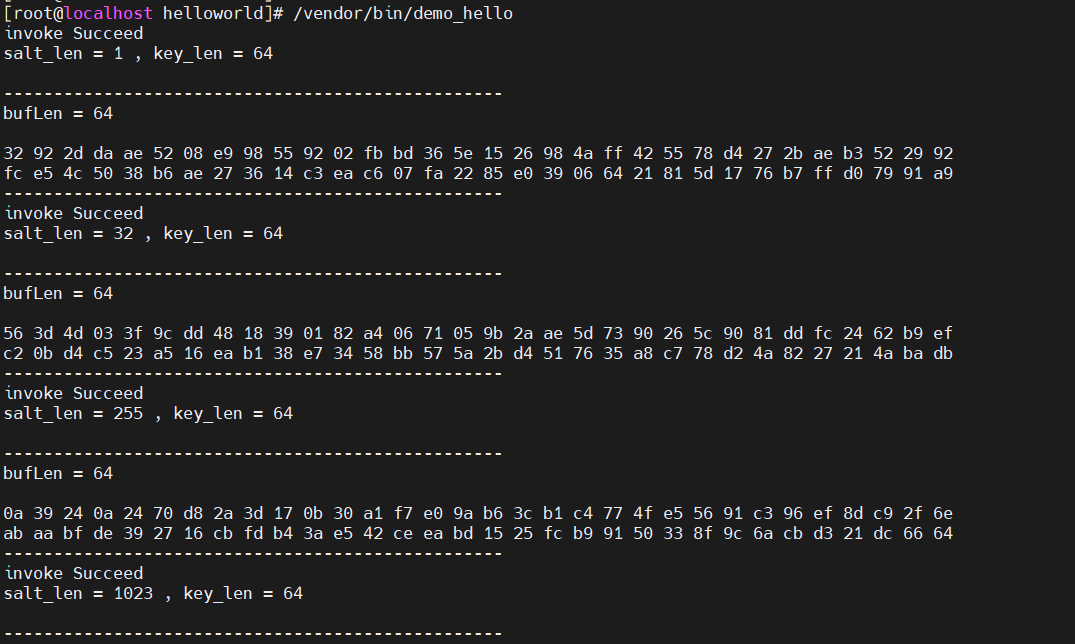
2、在支持的最大长度内，所列长度调用都成功返回，

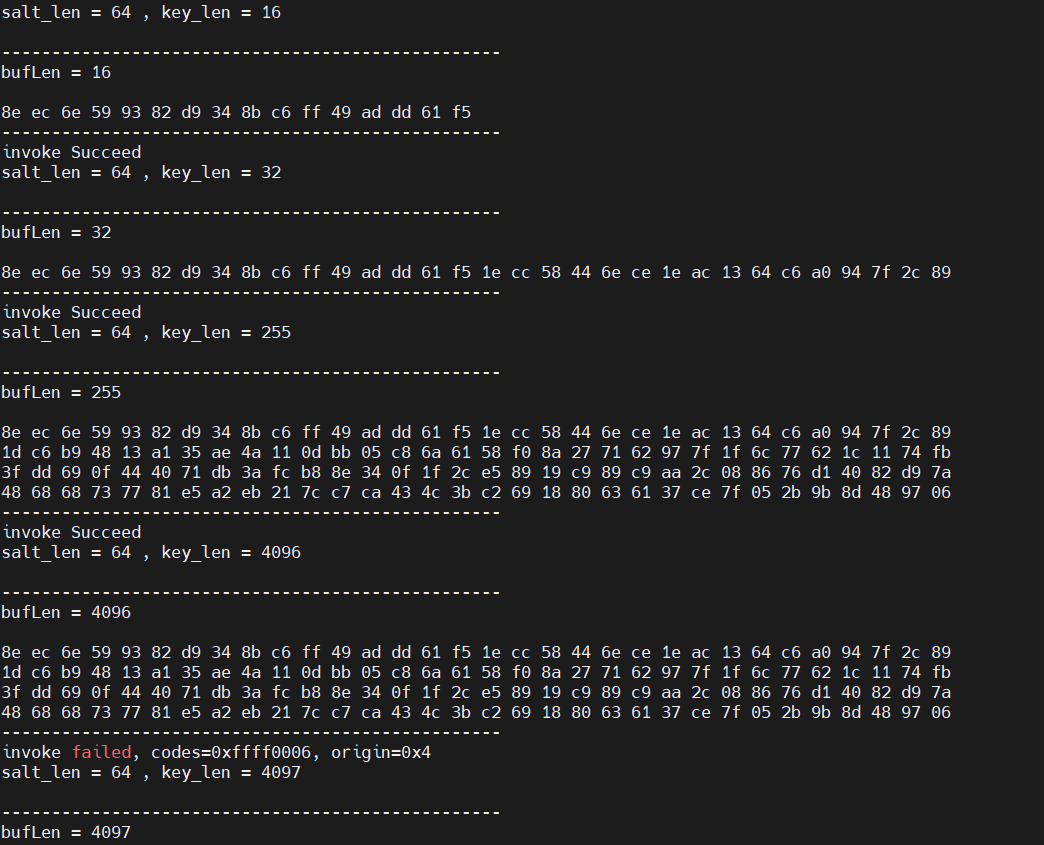
3、相同salt密钥一致

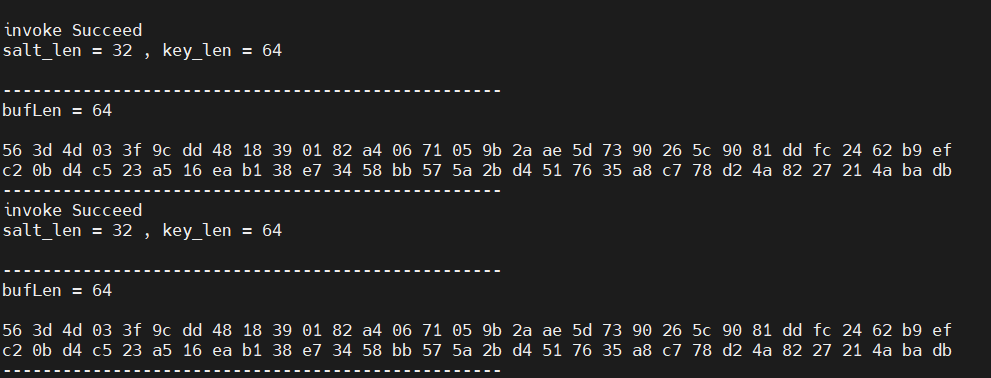
**[测试结论及现象]**

符合预期；

密钥长度4097失败，其余成功；







### huk密钥派生，TA内多线程调用

**[测试步骤]**

1、TA内开启多个线程，每个线程发起100次盐32和密钥512长度的GP接口调用，

2、线程测试范围：128

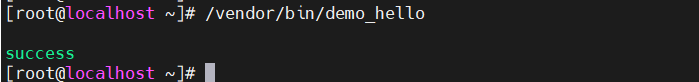
**[预期结果]**

1、所有接口调用正常

2、结果一致

**[测试结论及现象]**

符合预期



## 零拷贝

### CA创建Share Memory测试(内存页4K)

**[测试步骤]**

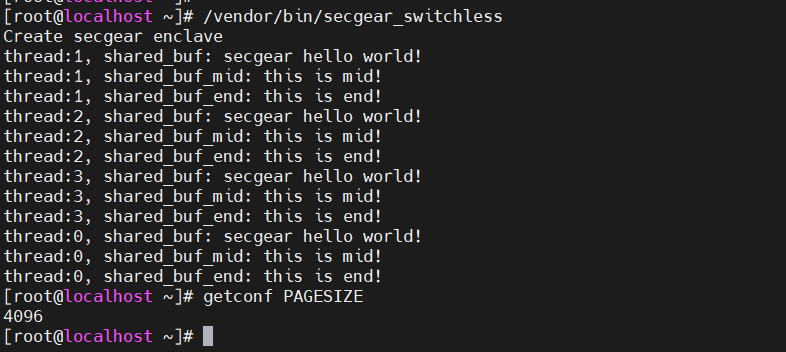
1. REE侧创建share memory 256M，预期结果1；

**[预期结果]**

结果1：内存创建成功

**[测试结论及现象]**

符合预期



### CA创建Share Memory测试(内存页64K)

**[测试步骤]**

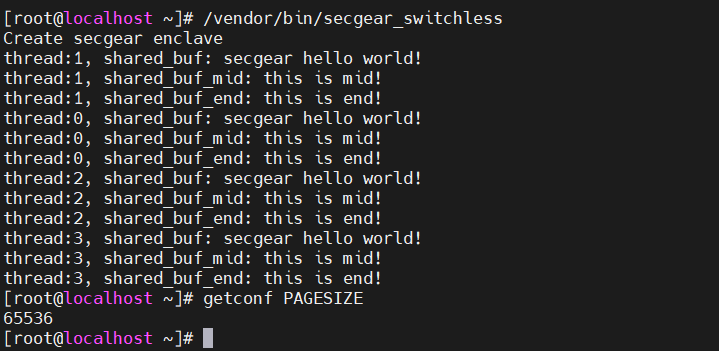
1. REE侧创建share memory 256M，预期结果1；

**[预期结果]**

结果1：内存创建成功

**[测试结论及现象]**

符合预期



### 零拷贝功能测试(内存页4K)

**[测试步骤]**

1. REE侧创建share memory 256M，预期结果1；

2. 使传参方式为零拷贝模式编写CA/TA, 预期结果2

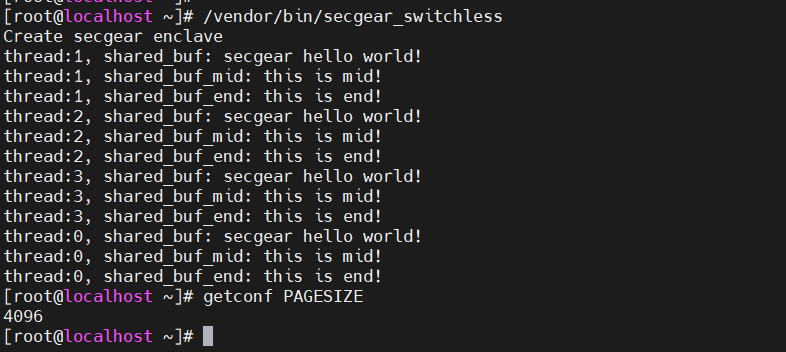
**[预期结果]**

结果1：内存创建成功

结果2：测试CA/TA成功运行

**[测试结论及现象]**

符合预期



### 零拷贝功能测试(内存页64K)

**[测试步骤]**

1. REE侧创建share memory 256M，预期结果1；

2. 使传参方式为零拷贝模式编写CA/TA, 预期结果2

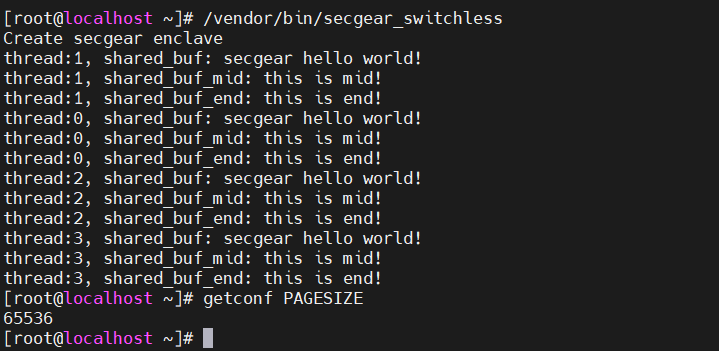
**[预期结果]**

结果1：内存创建成功

结果2：测试CA/TA成功运行

**[测试结论及现象]**

符合预期



## 安全存储demo

### 验证CMD\_SECSTORAGE\_XXXXX\_FILE接口功能是否正常

**[测试步骤]**

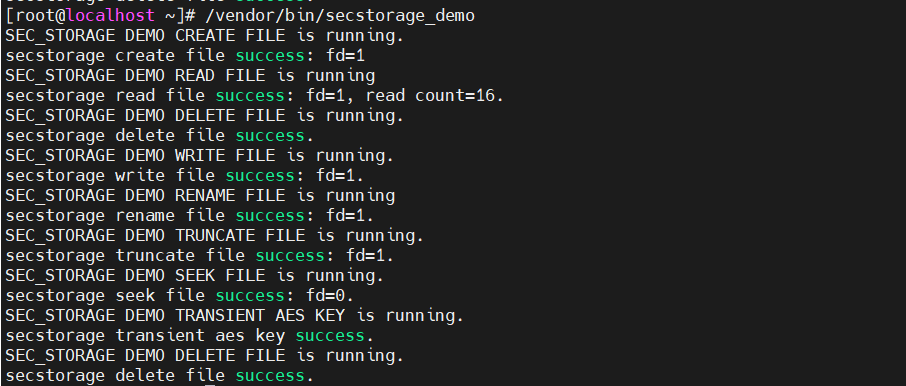
1.通过CA调用接口secstorage\_create\_file去调用TA侧，传入正确的参数 2.查看输出结果，查看tlog日志信息。3.再次调用CA接口，传入错误的参数。4.查看输出结果，查看tlog日志信息

**[预期结果]**

1.CA运行成功，tlog日志无错误信息。在/data/目录下，生成目标文件 2.CA运行失败，并打印相应的错误信息。在/data/目录下，没有生成目标文件

**[测试结论及现象]**

符合预期



## 十个VM同时运行CATA

**[测试步骤]**

1. 创建VM1到VM10

2. VM中编写CA/TA

3. 在VM1到VM10中同时运行CATA，预期结果1

**[预期结果]**

1. VM1到VM10中的TA均加载成功

**[测试结论及现象]**

符合预期

