Selinux策略文件配置方法

V1.0

星联天通科技有限公司

修改记录

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 版本号 | | 拟制人/修改人 | 拟制日期/  修改日期 | 更改理由 | 主要更改内容  （写要点即可） |
| <V1.0> |  | |  | <初稿> |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |

目 录

[1 背景 5](#_Toc514838587)

[2 遇到的问题 5](#_Toc514838588)

[3 解决思路 5](#_Toc514838589)

[4 实践情况 6](#_Toc514838590)

[5 效果评价 6](#_Toc514838591)

[6 推广建议 6](#_Toc514838592)

[6.1 应用时机 6](#_Toc514838593)

[6.2 适用对象 6](#_Toc514838594)

[6.3 应用场景 6](#_Toc514838595)

[6.4 过程改进建议 6](#_Toc514838596)

[7 参考资料 6](#_Toc514838597)

【摘要】

【关键词】

# 背景

*T901项目需基于android8.1进行开发，需要移植T900（android5.1） RIL相关代码。*

*涉及代码有rild进程、ril相关库、串口复用进程muxd。*

# 遇到的问题

*在移植的过程中，发现rild进程以及muxd进程无法启动。*

*原因是，android8.1默认开启selinux，需要配置对应的selinux策略文件才能启动进程。*

# 解决思路

*下面以串口复用进程muxd说明，*

*修改步骤：*

*1）device/qcom/sepolicy/common/file\_contexts目录下*

*添加/(vendor|system/vendor)/bin/hw/muxd-cetc54 u:object\_r:muxd-cetc54\_exec:s0*

*2）device/qcom/sepolicy/common目录添加进程的te文件 --- muxd-cetc54.te*

*type muxd-cetc54, domain;*

*type muxd-cetc54\_exec, exec\_type, vendor\_file\_type, file\_type;*

*init\_daemon\_domain(muxd-cetc54)*

*net\_domain(muxd-cetc54)*

*allow muxd-cetc54 vendor\_shell\_exec:file execute\_no\_trans;*

*allow muxd-cetc54 vendor\_toolbox\_exec:file execute\_no\_trans;*

*allow muxd-cetc54 vendor\_radio\_data\_file:dir { add\_name remove\_name search write };*

*allow muxd-cetc54 vendor\_radio\_data\_file:lnk\_file { create getattr read unlink};*

*allow muxd-cetc54 tty\_device:chr\_file rw\_file\_perms;*

*allow muxd-cetc54 console\_device:chr\_file rw\_file\_perms;*

*allow muxd-cetc54 device:chr\_file { open ioctl read write };*

*te策略文件上面4行是基本类型定义、域定义。网上参考资料很多。*

*注意vendor\_file\_type必须要配置，否则会出现莫名其妙的编译错误。*

*比较麻烦的是te文件中后面allow规则配置，如果自己手动添加，非常麻烦。这里有一个非常方便的linux工具audit2allow。*

*当我们添加的muxd-cetc54进程启动时，如果没有对应的权限执行，就会自动退出，并且在kernel日志有allert提示：*

*[ 160.091653] type=1400 audit(50779.129:53): avc: denied { remove\_name } for pid=3916 comm="rm" name="rcpts" dev="mmcblk0p34" ino=23445 scontext=u:r:muxd-cetc54:s0 tcontext=u:object\_r:vendor\_radio\_data\_file:s0 tclass=dir permissive=0*

*我们把上面的警告提示保存在avc.txt文件中，然后使用工具audit2allow*

*audit2allow –i avc.txt 就会输出需要添加的allow规则，*

*allow muxd-cetc54 vendor\_radio\_data\_file:dir remove\_name ;*

*然后把上面输出的规则，添加到muxd-cetc54.te文件中，如此循环，最后就可以把执行muxd进程所有需要的相关权限都添加进去了。*

# 实践情况

*添加selinux策略文件后，muxd进程就可以运行起来了。*

# 效果评价

# 推广建议

## 应用时机

## 适用对象

## 应用场景

*在Android oreo系统添加自定义进程。*

## 过程改进建议

# 参考资料