- Close Window
- Print This Page
- Expand All | Collapse All

SELinux:How to add a new domain for a new executable file and its policy

Solution Number 00030298

Please Note:

If Qualcomm documentation is referenced in this solution, your access to it is based on your company's

Language Key Words

Detail Information

Solution Title SELinux:How to add a new domain for a new executable file and its policy

Solution Details

Question: How to add a new domain for a new executable file and its policy
Answer:
Android baseline sepolicy file is stored at external/sepolicy/
Qualcomm related sepolicy file is stored in devices/qcom/sepolicy/common/
the two folder file will be merged together.
for example:
A new executable file, like /system/bin/perfd
1. need to add a new file devices/qcom/sepolicy/common/perfd.te
add it to list of BOARD_SEPOLICY_UNION
devices/qcom/sepolicy/Androd.mk
2. in perfd.te, define new domain name(perfd) and new exec file type(perfd_exec)

```
type perfd, domain;
type perfd_exec, exec_type, file_type;
```

if it is a service started by init, call macro init_daemon_domain, then allow transition from init to perfd domain.

```
init_daemon_domain(perfd)
```

3. add exec type in devices/qcom/sepolicy/common/file_contexts

```
/system/bin/perfd                      u:object_r:perfd_exec:s0
```

4.add other file type or device type that perfd may need to access in devices/qcom/sepolicy/common/file_contexts

```
/dev/socket/perfd(/.*)?                u:object_r:mpctl_socket:s0
/data/system/perfd(/.*)?               u:object_r:mpctl_data_file:s0
```

5. Then add all kinds of policy in later of perfd.te
like

```
allow perfd mpctl_socket:dir rw_dir_perms;
allow perfd mpctl_data_file:file { create_file_perms unlink };
```

could check kernel log about avc: denied { xxxx} and add more policy

6. after modify, need to rebuild boot.img and system.img and download

7.
check by ls -Z for all your added file/device/socket, whether secure context is as you expected.
check by ps -Z to see whether your new process is working in expected download

8. If what added is a new service, please also refer to solution 00030216 SElinux:How to add policy for a new service?
you could also add exec domain in init.xxxx.rc in a service property seclabel
like

```
 seclabel u:r:perfd:s0
```

for quickly recreate a system.img, use -S to specify file_contexts file with mkae_ext4fs command.
e.g.:

```
make_ext4fs -s -S out/target/product/msm8974/root/file_contexts -l 1073741824 -a system
out/target/product/msm8974/obj/PACKAGING/systemimage_intermediates/system.img
out/target/product/msm8974/system
```

Applicable Products AMSS 8936, AMSS 8939, AMSS 8974, AMSS 8974AB, AMSS8916, AMSS8926, AMSS8992, AMSS8994, AMSS8996