[FAQ06317]如何永久性开启adb 的root权限

[Description]
如何永久性开启adb 的root权限

[Keyword]
user debug root adb adbd

[Solution]
* adb 的root 权限是在system/core/adb/adb.c 中控制。主要根据ro.secure 以及 ro.debuggable 等system property 来控制。
默认即档ro.secure 为0 时，即开启root 权限，为1时再根据ro.debuggable 等选项来确认是否可以用开启root 权限。为此如果要永久性开启adb 的root 权限，有两种修改的方式:
1. 修改system property ro.secure， 让ro.secure=0。
2. 修改adb.c 中开启root 权限的判断逻辑。
* 在L 版本上adb 会受到SELinux 的影响, 所以需要调整SELinux policy 设置.
下面详细说明这两种修改方式:
第一种方法. 修改system property ro.secure， 让ro.secure=0。
(1)修改alps/build/core/main.mk
ifneq (,$(user_variant))
Target is secure in user builds.
ADDITIONAL_DEFAULT_PROPERTIES += ro.secure=1
将ADDITIONAL_DEFAULT_PROPERTIES += ro.secure=1 改成 ADDITIONAL_DEFAULT_PROPERTIES += ro.secure=0 即可。
(2)在android JB 版本(4.1) 以后，google 从编译上直接去除了adbd 的user 版本root 权限， 为此您要修改system/core/adb/Android.mk 中的编译选项ALLOW_ADBD_ROOT, 如果没有打开这个选项，那么adb.c 中将不会根据ro.secure 去选择root 还是shell 权限，直接返回shell 权限。因此您必须需要Android.mk 中的第126行：
ifneq (,$(filter userdebug eng,$(TARGET_BUILD_VARIANT)))
===> ifneq (,$(filter userdebug user eng,$(TARGET_BUILD_VARIANT)))
(3)在android L (5.0) 以后, google 默认开启SELinux enforce mode, 需要在user build 上将su label 默认build 进SEPolicy.
放开SELinux 的限制. 更新alps/external/sepolicy/Android.mk 116 行, 将su label 默认编译进入sepolicy.
sepolicy_policy.conf := $(intermediates)/policy.conf
$(sepolicy_policy.conf): PRIVATE_MLS_SENS := $(MLS_SENS)
$(sepolicy_policy.conf): PRIVATE_MLS_CATS := $(MLS_CATS)
$(sepolicy_policy.conf) : $(call build_policy, $(sepolicy_build_files))
@mkdir -p $(dir $@)
$(hide) m4 -D mls_num_sens=$(PRIVATE_MLS_SENS) -D mls_num_cats=$(PRIVATE_MLS_CATS) \
-D target_build_variant=$(TARGET_BUILD_VARIANT) \
-D force_permissive_to_unconfined=$(FORCE_PERMISSIVE_TO_UNCONFINED) \
-s $^ > $@
$(hide) sed '/dontaudit/d' $@ > $@.dontaudit

将-D target_build_variant=$(TARGET_BUILD_VARIANT) 改成 -D target_build_variant=eng

即第一种方法在android L(5.0) 以后你需要改(1),(2),(3).

第二种方法. 修改adb.c 中开启root 权限的判断逻辑。这里针对4.1 以后版本 和4.1以前版本有所区别。
(1).如果是JB 4.1 以后版本，直接修改函数should_drop_privileges() 函数, 清空这个函数，直接返回 0 即可。返回0 即开启root 权限。
(2).如果是JB 4.1 以前版本，直接修改函数adb_main 函数，在
```
/* don't listen on a port (default 5037) if running in secure mode */
/* don't run as root if we are running in secure mode */
if (secure) {
struct __user_cap_header_struct header;
struct __user_cap_data_struct cap;
if (prctl(PR_SET_KEEPCAPS, 1, 0, 0, 0) != 0) {
exit(1);
}
```

在这段代码前加一行:
```
secure = 0; //mtk71029 add for root forever.
/* don't listen on a port (default 5037) if running in secure mode */
/* don't run as root if we are running in secure mode */
if (secure) {
struct __user_cap_header_struct header;
struct __user_cap_data_struct cap;
if (prctl(PR_SET_KEEPCAPS, 1, 0, 0, 0) != 0) {
exit(1);
}
```

(3)在android L (5.0) 以后, google 默认开启SELinux enforce mode, 需要在user build 上将su label 默认build 进SEPolicy.
放开SELinux 的限制. 更新alps/external/sepolicy/Android.mk 116 行, 将su label 默认编译进入sepolicy.
```
sepolicy_policy.conf := $(intermediates)/policy.conf
$(sepolicy_policy.conf): PRIVATE_MLS_SENS := $(MLS_SENS)
$(sepolicy_policy.conf): PRIVATE_MLS_CATS := $(MLS_CATS)
$(sepolicy_policy.conf) : $(call build_policy, $(sepolicy_build_files))
@mkdir -p $(dir $@)
$(hide) m4 -D mls_num_sens=$(PRIVATE_MLS_SENS) -D mls_num_cats=$(PRIVATE_MLS_CATS) \
-D target_build_variant=$(TARGET_BUILD_VARIANT) \
-D force_permissive_to_unconfined=$(FORCE_PERMISSIVE_TO_UNCONFINED) \
-s $^ > $@
$(hide) sed '/dontaudit/d' $@ > $@.dontaudit
```

将-D target_build_variant=$(TARGET_BUILD_VARIANT) 改成 -D target_build_variant=eng

即第二种方法在android L(5.0) 以后你需要改(1),(3).

[测试与确认]

当修改完成后，只需要重新build bootimage ，然后download 即可，然后到setting 中开启debug 选项，adb 连接后，会显示 #, 即root 成功。

[相关FAQ]
JB 版本后user build + eng bootimage 无法开机
如何打开user debug选项
JB 4.2 user 版本的开发选项不见了，如何打开adb debug