1. userdebug和user版本
2. 关闭selinux
   system/core

```
diff --git a/init/selinux.cpp b/init/selinux.cpp
index 5a0255acd..787917274 100644
--- a/init/selinux.cpp
+++ b/init/selinux.cpp
@@ -104,6 +104,8 @@ EnforcingStatus StatusFromCmdline() {
 }

 bool IsEnforcing() {
+    return false;
+
     if (ALLOW_PERMISSIVE_SELINUX) {
         return StatusFromCmdline() == SELINUX_ENFORCING;
     }
```

3. 修改su.cpp，注释用户组权限检测
   system/extras/su/su.cpp

```
diff --git a/su/su.cpp b/su/su.cpp
index 1a1ab6bf..af3d2a68 100644
--- a/su/su.cpp
+++ b/su/su.cpp
@@ -80,8 +80,8 @@ void extract_uidgids(const char* uidgids, uid_t* uid, gid_t*
gid, gid_t* gids, i
 }

 int main(int argc, char** argv) {
-    uid_t current_uid = getuid();
-    if (current_uid != AID_ROOT && current_uid != AID_SHELL) error(1, 0, "not
allowed");
+    //uid_t current_uid = getuid();
+    //if (current_uid != AID_ROOT && current_uid != AID_SHELL) error(1, 0, "not
allowed");

     // Handle -h and --help.
     ++argv;
```

4. 给 su 文件默认授予 root 权限
   system/core/libcutils/fs_config.cpp

```
diff --git a/libcutils/fs_config.cpp b/libcutils/fs_config.cpp
index 5805a4d19..92e93e76f 100644
--- a/libcutils/fs_config.cpp
+++ b/libcutils/fs_config.cpp
@@ -86,7 +86,7 @@ static const struct fs_path_config android_dirs[] = {
     { 00751, AID_ROOT,         AID_SHELL,        0, "system/bin" },
     { 00755, AID_ROOT,         AID_ROOT,         0, "system/etc/ppp" },
     { 00755, AID_ROOT,         AID_SHELL,        0, "system/vendor" },
-    { 00750, AID_ROOT,         AID_SHELL,        0, "system/xbin" },
+    { 00755, AID_ROOT,         AID_SHELL,        0, "system/xbin" },
     { 00751, AID_ROOT,         AID_SHELL,        0, "system/apex/*/bin" },
     { 00751, AID_ROOT,         AID_SHELL,        0, "system_ext/bin" },
     { 00751, AID_ROOT,         AID_SHELL,        0, "system_ext/apex/*/bin" },
@@ -190,7 +190,7 @@ static const struct fs_path_config android_files[] = {
     // the following two files are INTENTIONALLY set-uid, but they
     // are NOT included on user builds.
     { 06755, AID_ROOT,      AID_ROOT,      0, "system/xbin/procmem" },
-    { 04750, AID_ROOT,      AID_SHELL,     0, "system/xbin/su" },
+    { 06755, AID_ROOT,      AID_SHELL,     0, "system/xbin/su" },
```

frameworks/base/core/jni/com_android_internal_os_Zygote.cpp

```
diff --git a/core/jni/com_android_internal_os_Zygote.cpp
b/core/jni/com_android_internal_os_Zygote.cpp
index 9eede83e21e5..694eec2a40ac 100644
--- a/core/jni/com_android_internal_os_Zygote.cpp
+++ b/core/jni/com_android_internal_os_Zygote.cpp
@@ -656,6 +656,7 @@ static void EnableKeepCapabilities(fail_fn_t fail_fn) {
 }

 static void DropCapabilitiesBoundingSet(fail_fn_t fail_fn) {
+/*
   for (int i = 0; prctl(PR_CAPBSET_READ, i, 0, 0, 0) >= 0; i++) {;
     if (prctl(PR_CAPBSET_DROP, i, 0, 0, 0) == -1) {
       if (errno == EINVAL) {
@@ -666,6 +667,7 @@ static void DropCapabilitiesBoundingSet(fail_fn_t fail_fn) {
       }
     }
   }
+  */
 }
```

kernel/security/commoncap.c

```
diff --git a/security/commoncap.c b/security/commoncap.c
index f86557a8e43f6..19124dd6239a1 100644
--- a/security/commoncap.c
+++ b/security/commoncap.c
@@ -1147,12 +1147,12 @@ int cap_task_setnice(struct task_struct *p, int nice)
 static int cap_prctl_drop(unsigned long cap)
 {
        struct cred *new;
-
+/*
        if (!ns_capable(current_user_ns(), CAP_SETPCAP))
                return -EPERM;
        if (!cap_valid(cap))
                return -EINVAL;
-
+*/
        new = prepare_creds();
        if (!new)
                return -ENOMEM;
```

5. user版本需要把su编进系统

```
build/core
```

```
diff --git a/target/product/base_system.mk b/target/product/base_system.mk
index 4569bceff9..5c8eaaa87c 100644
--- a/target/product/base_system.mk
+++ b/target/product/base_system.mk
@@ -273,6 +273,7 @@ PRODUCT_PACKAGES += \
     wificond \
     wifi.rc \
     wm \
+    su \

 # VINTF data for system image
 PRODUCT_PACKAGES += \
@@ -378,7 +379,6 @@ PRODUCT_PACKAGES_DEBUG := \
     ss \
     start_with_lockagent \
     strace \
-    su \
     sanitizer-status \
     tracepath \
     tracepath6 \
```