Publication: z/OS: z/OS MVS System Commands

Reference Link:
https://www.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R5SA380666/$file/ieag100_v2r5.pdf

Section:
Communicating with the device manager address space

...
<insert after the following line>

Restriction: Use this command only at the direction of the system programmer.

<new text as Note:>
DEVMAN RACF Requirements

The DEVMAN started task needs to have a protected USERID assigned to it.

Steps to define a protected USERID to DEVMAN:

1. Define a protected user ID for the DEVMAN started task if one is not already established. A protected user ID cannot be used to enter the system by any method that uses a supplied password.

The attributes NOPASSWORD and NOPHRASE for the ADDUSER/ALTUSER-constitute the PROTECTED attribute.
For example:
ADDUSER userid NOPASSWORD NOPHRASE DFLTGRP(SYS1) OWNER(M16)

2. Define a profile for DEVMAN in the RACF STARTED class. Assign the user ID from Step 1 to the DEVMAN procedure in the STARTED class.
For example:
RDEFINE STARTED DEVMAN.* STDATA(USER(userid) GROUP(SYS1)) OWNER(M16SPEC)

See z/OS Security Server RACF Security Administrator's Guide. “Defining protected user IDs” for additional information.

DEVMAN parameters require communication with ICKDSF. Currently, only the REFVTOC parameter has this requirement.

During startup of the DEVMAN address space, the ICKDSF program is loaded by DEVMAN. If you are using RACF or another security product to control the use of the ICKDSF program, then the USERID

associated with the DEVMAN address space must have READ access to use ICKDSF program. Otherwise, a security violation will occur when the DEVMAN address space is started.

Steps to take if ICKDSF is Program Controlled when using RACF:

1. Permit the user ID for the DEVMAN started task to call ICKDSF by allowing read access to ICKDSF in the PROGRAM class.
   For example:
   PERMIT ICKDSF CLASS(PROGRAM) ID(userid) ACCESS(READ)

2. Refresh the storage RACF profiles by using the command:
   SETR WHEN(PROGRAM) REFRESH.

3. Refresh the STARTED profiles, if necessary, using the command:
   SETR RACLIST(STARTED) REFRESH.

If you are using RACF or another security product to control specific ICKDSF commands, then profiles must be created for either the specific commands or for a generic profile.
For example: STGADMIN.ICK.REFORMAT or STGADMIN.ICK.**. Then the USERID associated with the DEVMAN address space must have read access to the security product profile(s) that protect the ICKDSF command(s). Otherwise, a security violation will occur when DEVMAN attempts to invoke the ICKDSF command. The specific ICKDSF commands that are used by DEVMAN are REFORMAT and INIT.

Steps to take if ICKDSF Functions (REFORMAT or INIT) ~~is Controlled~~ are protected when using RACF:

1. If the DEVMAN REFVTOC function is enabled and you have a security profile controlling this ICKDSF REFORMAT function, permit the userid associated with the DEVMAN address space read access to this profile. For example if a generic security profile is used:
   PERMIT STGADMIN.ICK.** CLASS(FACILITY) ID(userid)ACCESS(READ)
For example if a discrete security profile is used:
   PERMIT STGADMIN.ICK.REFORMAT CLASS(FACILITY) ID(userid)ACCESS(READ)

2. If you are using the z/OS Management Facility (z/OSMF) interface for Storage Management and have a security profile controlling the ICKDSF INIT function, permit the userid associated with the DEVMAN address space read access to this profile.
   For example if a generic security profile is used:
   PERMIT STGADMIN.ICK.** CLASS(FACILITY) ID(userid)ACCESS(READ)
   For example if a discrete security profile is used:
   PERMIT STGADMIN.ICK.INIT CLASS(FACILITY) ID(userid)ACCESS(READ)

Reference information:
For information about using program control to restrict access to programs such as ICKDSF, see z/OS Security Server RACF Security Administrator's Guide.

For information about using RACF commands to set up the security definitions,

see z/OS Security Server RACF Command
<existing>