RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 13
Issue 3

July
2019

Password Phrase Console Logon

APAR OA54790 introduced new functionality to allow operators to log onto MCS consoles with password phrases. After applying the APAR, you enable this new feature by defining discrete profile MVS.CONSOLE.PASSWORDPHRASE.CHECK in the OPERCMDS class and then recycle your consoles with a VARY command or an IPL.

Note the following phrase syntax rules:

- Phrases must be enclosed within single quotation marks, but the quotation marks are not part of the phrase.
- The maximum phase length is 45 characters (excluding the enclosing quotes).
- If a single quotation mark is intended to be part of the phrase, do not double up the embedded quotation mark (e.g. **'**John's c@r is ye11ow**'**).

See the APAR for further details.

Owner Authority & RACLIST

A non-SPECIAL user who owns a General Resource profile can list, change, and permit access to the profile. However, if the profile's class is RACLISTed, an owning user is prevented from administering a newly created profile until a RACLIST REFRESH of the class is performed.

Auditors: IBMUSER

IBMUSER is RACF's default ID. It is automatically defined when a new RACF database is created. Its only intended use is to create a few IDs with SPECIAL authority (i.e., Administrator IDs), after which it is to be deactivated (REVOKED). RSH recommends further limiting its capabilities by removing its SPECIAL and OPERATIONS authority, making it RESTRICTED and PROTECTED, and assigning it a null Unix UID.

IBMUSER should not be deleted. The DELUSER command ignores attempts to delete it. If an installation managed to delete it, RACF would automatically recreate the ID when the system is restarted. The resurrected IBMUSER would have all of its original powerful authorities, it would not be REVOKED, and it would have its original, well-known default password.

Attend our course "RACF - Audit and Compliance Roadmap" for more details on auditing RACF.

OPERATIONS - Dataset Creation

Except as noted below, a user with OPERATIONS can create a dataset even when permitted less than ALTER access to the profile that protects the dataset. Once the dataset is created, however, the user's access is capped at the permitted level of access. Hence, an OPERATIONS user could create a dataset but not be able to access it.

If the dataset's High Level Qualifier (HLQ) is a group, an OPERATIONS user can be blocked from creating a dataset with that HLQ by connecting the user to the HLQ group with USE authority. Profile permissions alone would then determine if the user could create a dataset.

If an OPERATIONS user creates a dataset when permitted less than ALTER access, the SMF DEFINE event record will indicate OPERATIONS authority was used. However, if the user creates a dataset when not permitted any access, the DEFINE will not indicate OPERATIONS use.

TSO CANCEL and Exit IKJEFF53

To allow ALTER access to JESJOBS resources CANCEL.*localnode.userid.jobname* to control whether TSO users can cancel other user's jobs using the TSO CANCEL command, you must first remove or replace TSO's pre-installed default IKJEFF53 exit. The default exit ignores JESJOBS and lets a user cancel any job whose name begins with their own ID regardless of who owns the job. (The exit also ignores JESSPOOL with the TSO STATUS and OUTPUT commands.)

To determine if the IKJEFF53 exit is active, execute the TSO command: **ISRDDN**. Next, at ISRDDN's command line, enter: **LOAD IKJEFF53**

If the exit does not exist, message “Load failed” will appear in the upper right corner of the panel.

If the exit exists, a message indicating the module was found to be already loaded will be displayed along with details about the module. If the size in hex is 238 (z/OS 2.2) or 2A0 (z/OS 2.3) and the exit was loaded from SYS1.LINKLIB, it is most likely the default exit.

Pressing "Enter" will show a hex and character display of IKJEFF53. Note the following text on the right at the end of the module.

```
* .......-JOBREJEC *
* TED - JOBNAME MU *
* ST BE YOUR USERI *
* D PLUS AT LEAST  *
* ONE CHARACTERREJ *
* ECTED - JOBNAME  *
* MUST BE YOUR USE *
* RID OR MUST STAR *
* T WITH YOUR USER *
* ID.....èZAPZAPZA *
* PZAPZAPZAPZAP... *
```

Messages generated by the exit and descriptions in IBM documentation state that a user can only cancel a job whose name begins with their ID plus one character. Our tests determined the jobname can have any number of characters after the ID.

You can optionally use the IBM-supplied exit code provided in SYS1.SAMPLIB(IKJEFF5X) as a replacement for the default exit. If the IKJEFF53 load module size is hex 390 and it has the same text as shown above, it is probably the IBM replacement. This exit lets JESJOBS control access if the class is active; otherwise, it governs access like the default. Likewise for JESSPOOL.

Do not remove the default exit if JESJOBS and JESSPOOL have not be been activated.

JESJOBS Resource Name Increase

APAR OA57721 increases the MAXLENX length of JESJOBS resource names from 39 to 246.

Loading IRRDPI00 at Startup

The RACF Command Parsing Table, IRRDPI00, must be resident in memory in order for RACF to process commands with profile segment keywords. It is typically loaded into memory during system startup either by a Started Task, commonly named IRRDPTAB, or by the RACF Subsystem Address Space.

JES must be active in order to start a Started Task, but it need not be active for RACF subsystem initialization. Therefore, we recommend configuring the RACF Subsystem to load IRRDPI00 to enable recovery from a RACF issue that prevents JES from initializing.

Attend our course "RACF - Level II Administration for details on loading IRRDPI00.

JES NJE Security Health Checks

New in z/OS 2.3 are health checks which review JES parameters to determine if JES NJE nodes considered trusted by RACF are configured in a secure manner. The check names are JES_NJE_SECURITY for the primary subsystem and JES_NJE_SECURITY_*ssname* for secondary subsystems. The owner of the checks is IBMJES. PTFs for APAR OA49171 add these checks to z/OS 2.1 and 2.2 systems.

To perform these checks, the Health Checker Started Task will require READ access to FACILITY resource IRR.RADMIN.RLIST and the ROAUDIT attribute (or AUDITOR with z/OS 2.1).

RSH News

This is the **50th** issue of RSH RACF Tips. Kindly let us know if they have been of help to you.

With our RACF Mentor services, your staff can call our highly experienced RACF professionals whenever they need occasional guidance, advice, or one-on-one training. Call today for details.