RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 12
Issue 3
July
2018

DSMON - NOPASS_ALLOWBATCH

When a program is assigned attribute NOPASS in the z/OS Program Properties Table (PPT), the DSMON PPT report displays YES under column BYPASS PASSWORD PROTECTION. However, the DSMON PPT report incorrectly displays NO if a program is assigned NOPASS_ALLOWBATCH. RSH discovered this discrepancy and alerted IBM.

For more on NOPASS_ALLOWBATCH, see article "PPT NOPASS Change" in the January 2017 issue of this newsletter.

Z/OS 2.3 - 8-Character TSO IDs

z/OS 2.3 allows the use of 8-character USERIDs in TSO; however, this feature must be activated by adding option USERIDMAX(8) to the LOGON parameter in the IKJTSOxx PARMLIB member. USERIDMAX(7) is the default.

Here are a few items worth noting related to use of 8-character IDs for TSO.

- The SUBMIT command will assign job names that match the USERID. Check your JESJOBS profiles to see if they are affected.
- To save messages sent to these IDs via the SEND command, enable user logs.
- Users of these IDs cannot invoke Information Center Facility (ICF) functions.
- These IDs can only be used for TSO on z/OS 2.3 systems with USERIDMAX(8). If the RACF database is shared with pre-2.3 z/OS systems or 2.3 systems with the default setting, the IDs cannot be used for TSO on those systems.

Hacking Z - Clear-text Passwords

Obtaining IDs and passwords is a hacker's first objective. Failure to configure z/OS to encrypt protocols like TN3270, telnet, smtp, ftp, and http exposes clear-text passwords to capture by network packet inspection tools like Wireshark.

Pathname in Unix SMF Records

Many Unix-related SMF 80 records have a field for the pathname. This field contains only the pathname entered by the user, which is not necessarily the full path name. If a user currently in directory /a/b enters 'cd c' to change directory to 'c' (a subdirectory under /a/b), the SMF record only shows 'c' for pathname, not '/a/b/c'.

Command Violation Anomaly

If a user tries to add or change a segment field without sufficient access to a FIELD class profile, the command fails and RACF does not make the requested change. But the SMF record generated for the command indicates it was successful.

CDT vs. ICHRRCDE Class Deletion

RACF will not allow deletion of a CDT class profile when profiles are still defined in the corresponding class. No such safety mechanism exists when removing the ICHRRCDE table entry for a class. At IPL, any profiles still defined to the class will become orphaned. You will need to redefine the class and activate GENCMD to remove them.

IBM Classes Defined by CDT Profiles Now In ICHRRCDX

IBM previously required creation of CDT class profiles to add classes HBRADMIN, HBRCONN, HBRCMD, and WBEM to RACF. In z/OS 2.3, definitions for these classes are now included in RACF's static class descriptor table ICHRRCDX. If you applied APAR OA53185, WBEM was added earlier. Before you upgrade any systems, change the CDTINFO POSIT values in the CDT profiles for these classes to match those specified in the new ICHRRCDX entries and then reactivate the

classes. Refer to the z/OS 2.3 migration guide and OA53185 for guidance. Once all systems sharing a RACF database are z/OS 2.3, the CDT profiles will be ignored, and you can delete them.

New CICS 5.4 Resources

The following CICS supplied transactions have been added to CICS Transaction Server 5.4 and, if underlined, earlier by APAR. The ones prefixed "CO" are CICSPlex related.

Category 1: CHCK CJSP CMPE COHT COIE COIR COI0 CONA COND CONH CONL CONM COWC
Category 2: CEPR

CICS command resource MQINI has been replaced by MQMON, which has different action functions and levels of access authorization.

Review your existing profiles to ensure these resources are properly protected.

PRIVILEGED + TRUSTED

If a Started Task is assigned both PRIVILEGED and TRUSTED authority, PRIVILEGED is used. This precludes any RACF logging of its activity. We recommend you remove PRIVILEGED.

Auditors: Ensure "Authorized" Program Libraries are Protected

An "Authorized" program can execute privileged instructions and Supervisor Calls (SVCs). A malicious authorized program can circumvent RACF, read and manipulate data, disrupt the operation of the system, and leave no audit trail.

Many programs brought into memory by z/OS at system startup run authorized. Other programs can run authorized if they reside in a dataset designated as an Authorized Program Facility (APF) library. Most APF libraries are assigned this status at startup by configuration options specified in z/OS Parameter Libraries (PARMLIBs). Operator commands and assembly programs using the CSVAPF macro can be used to make libraries APF-authorized at any time thereafter.

Anyone hacking a z/OS system will try to obtain update access to an APF library in order to add a malicious program to the library and execute it. A single improperly protected APF library is enough to leave your system completely exposed.

Ensure all z/OS system libraries, APF-authorized libraries, and mechanisms for making libraries APF-authorized are very tightly controlled and monitored. Use RACF's DSMON utility to identify these libraries for each z/OS system.

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

Shadow and ICHRIX02

Rocket Shadow (formerly Neon Shadow) specifies parameter SYSTEM=YES in its RACROUTE REQUEST=VERIFY calls to validate user logons. This parameter causes the VERIFY post-processing exit ICHRIX02 to be bypassed.

RSH News

RSH offers Penetration and Vulnerability Testing services specifically designed for z/OS. This offering has been expanded by Robyn Gilchrist, the newest member of the RSH team. Robyn is a highly-experienced Systems Programmer with exceptionally strong z/OS Unix and networking skills. Call today for an assessment.

To find out how others have implemented RACF options and controls, check out the results of our monthly surveys posted on the RSH website.

Register for our upcoming training today to take advance of the early registration discount.