RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 1
Issue 3

October
2007

Performance: Resident Data Blocks (RDBs)

The RACF database is divided into 4K blocks. Most are Data blocks which contain profiles and their segments. Some are Index blocks which contain the location of profiles. Others contain information about free space in the database and are named Block Availability Mask (BAM) blocks. RACF reads and writes data by block and not by individual profile or index entry.

To process a profile, RACF must perform I/O to retrieve the Index blocks until it finds the location of the desired profile and then retrieve the Data block containing the profile. The Index blocks are organized into a hierarchy such that upper level Index blocks contain pointers to lower level Index blocks. The lowest level Index blocks contain pointers to profiles. A typical database has 3 or 4 index levels, meaning 3 or 4 I/Os are required just to find each profile. If database I/O is slow, RACF can become a bottleneck to the entire system.

To reduce I/O, RACF can cache copies of the most recently used blocks in memory buffers known as Resident Data Blocks (RDBs). These cached blocks can be referenced immediately without requiring additional I/O. Data, Index, and BAM blocks are all eligible for caching. The most frequently referenced blocks tend to be Index blocks, and they fill many of the RDBs.

The number of RDBs is specified in the RACF Database Name Table ICHRDSNT. This table is primarily used to identify the names of the RACF databases and to specify options related to statistics and Sysplex. Here is a sample of the source code for an ICHRDSNT:

```
AL1(1)              Number of databases
CL44'RACF.PRIMARY'  Primary DB name
CL44'RACF.BACKUP'   Backup DB name
AL1(100)            # of RDBs
XL1'80'             Statistics/Sysplex
```

ICHRDSNT must be assembled to create a load module. It is loaded into memory during IPL and can only be changed with another IPL. In a Sysplex environment, the ICHRDSNT loaded by the first system to IPL is used for all the others. To change the ICHRDSNT in a Sysplex environment, all the systems must first be shut down before any are restarted.

As indicated in the table below, there are minimum and default specifications for the number of RDBs, and they differ for Sysplexed and non-Sysplexed environments.

Number of RDBs	Environment	
	Non-Sysplex	Sysplex
Minimum	0	50
Default	10	50

In a Sysplex, RACF also creates RDBs for the backup database equaling 20% of the number of RDBs set for the primary. This alone can have a significant performance benefit especially during the morning logon tidal wave. For the first logon of the day, RACF updates a user profile's last logon date in *both* the primary and the backup database. In a non-Sysplex system, each time a profile is updated in the backup database, RACF must retrieve all the index blocks as well as the profile data block; whereas, in a Sysplex system, the index blocks may be in RDBs.

The maximum number of RDBs that can be specified is 255. Since RDBs are the single most important RACF performance feature, *always* set the number of RDBs to the maximum.

Auditors: Review Outbound NJE Transmission Controls

z/OS systems can be linked to other z/OS systems and to VM and AS/400 systems using Network Job Entry (NJE). NJE networks are managed by the Job Entry Subsystem (JES) and are used to route batch jobs and output (SYSOUT) between systems. Each system on an NJE network is referred to as a node, and each node has a unique identifier known as its nodename.

If your installation has multiple z/OS systems, it is almost certain they will be connected via NJE. It is not uncommon to find z/OS systems linked to systems belonging to external organizations such as business partners and application service providers.

Imagine what could happen if someone on your system inadvertently sends data with personally identifiable information to another firm's system!

RACF can control who can send jobs and output out of your system to another node. This control is implemented by profiles in the WRITER class.

Before releasing outbound data to another node, JES calls RACF to ask whether the user has permission to the associated NJE node resource. The format of the resource name is:

```
jesname.NJE.nodename
```

When the WRITER class is active, RACF will find and check the profile that most closely matches the name of the resource and advise JES to allow the transmissions only when the user has at least READ authority.

To see if NJE transmission control has been properly implemented, do the following:

- Ask the JES system programmer to provide you with the names of the JES subsystems (e.g., JES2) and all the NJE nodes (e.g., SYST2) defined to JES on each of your systems as well as information about each node including the system name and the owner of the node. You can obtain some of this information on your own by reviewing the JES startup parameters. Due to staff changes and the passage of time, do not be surprised if the system programmer cannot provide complete information about the identity of each node.

- Confirm the WRITER class is active by executing the RACF command below and checking the 'ACTIVE CLASSES =' section of the output.

  ```
  SETROPTS LIST
  ```

- Using the JES subsystem and node names in combination, find the WRITER class profile protecting each outbound NJE resource and examine the profile to see who is allowed to send outbound transmissions. Here is the format of the command to accomplish this as well as a sample.

  ```
  RLIST WRITER jesname.NJE.nodename ALL

  RLIST WRITER JES2.NJE.SYST2 ALL
  ```

The WRITER class is a Default Return Code 8 class. When there is no profile covering a resource, RACF issues a Return Code 8 signifying access is to be disallowed.

It is generally acceptable to allow users to send transmissions to other systems belonging to their own firm. However, the ability to send transmissions to external nodes should be tightly controlled. Hopefully, you will find a 'catchall' profile such as JES%.NJE.* with no access permitted. This prevents transmissions to nodes not explicitly defined and requires the RACF staff to intervene to allow transmissions.

RSH News

For those of you who were unable to attend our presentations at **IBM's z/Expo conference** in September, you can obtain copies of the handouts from our website via the RACF Center webpage. The presentation topics were RACF Performance Tuning, Common Holes in RACF Defenses, and the FACILITY Class.

Be sure to catch our RACF presentations at the following **RACF User Group meetings**.

- NYRUG - RACF Performance Tuning, 10/9
- KOIRUG - z/OS Unix File Security, 10/30

Upcoming ***RACF Training*:**

- RACF - Audit for Results
  November 6-8, 2007 - Charlotte, NC

See our website for details and registration form.

RSH CONSULTING, INC.
RACF & ENDEVOR Specialists
www.rshconsulting.com ■ 617-969-9050
29 Caroline Park, Newton, Massachusetts 02468

SECURITY
SUPPORT
SOLUTIONS