Understanding Your FACILITY Class Profiles

The diverse collection of security definitions in RACF's FACILITY class are no longer a mystery. The information presented in this article will make your job easier when reviewing your security system.

BY MARK S. HAHN

Those of us who work with OS/390 or MVS systems are well aware of the potpourri of resource definitions in the FACILITY class. Since these are System Authorization Facility (SAF) calls, they are used by all the security packages presently being marketed. This article will provide you with a basic understanding of the profiles stored in the FACILITY class in RACF. Other security packages have their own version of how this is done.

First, there is no comprehensive reference defining *all* FACILITY class profiles. The FACILITY class is unique in that multiple products, both written by IBM and non-IBM vendors, place their profiles within it. It's advantageous to vendors to document their security setup as "Add a profile (or series of profiles) to the (known-to-exist) FACILITY class." This eliminates the coding of an installation-defined Class Descriptor Table (CDT) entry, an IPL, and any possible confusion that might result. By using the existing FACILITY class, the security profiles are bound by the rules established for FACILITY class definitions: no resource name exceeding 39 characters, profiles required to be storage-resident, etc.

Next, even in an ALWAYS CALL environment, FACILITY resources are only protected if there is a profile; if there is no profile, there is no protection. While this appears to be a contradiction, it is actually consistent with RACF's definition. Remember that RACF is passive security; when called, it makes a recommendation but cannot enforce it — the caller must act accordingly. It seems that in most FACILITY class calls, the decision logic is no profile means no protection.

If the urge to secure the FACILITY class is strong, exercise caution, as it could unintentionally create a Denial of Service situation. Since the protection hasn't been present previously, either put the profile into warning mode (alert the user that while they are not authorized, they are temporarily able to access the resource) or request that all accesses be journalled to

Figure 1: Searching Your RACF Database — A Summary Search

```
SEARCH CLASS(FACILITY) NOMASK
ICHBLP
ICHNL
IGG.CATLOCK
```

SMF or the audit file. This provides information prior to lockdown without inadvertent Denial of Service.

If it is your intent to lock down the service, you *must* define a global profile for that service with UACC(NONE). Do *not* build a universal resource definition for the facility class, such as a * or ** profile in RACF, as there are services looking for a match (which the universal definition does) instead of "no profile found" before taking action. This is further detailed below in the JES specifics.

When you are ready to begin reviewing your FACILITY class profiles, you can search the security package's database. In RACF, use the SEARCH or RLIST commands. By using the BATCH TMP, output can be captured for later use. Use either the TSO command "SEARCH CLASS(FACILITY) NOMASK" to list the names of all profiles as shown in Figure 1, or "RLIST FACILITY * ALL" to list the specifics of each FACILITY class profile, as shown in Figure 2.

It is important to note that the SEARCH command produces a RACF search-sequence list of the names of all FACILITY class profiles. This is valuable if resources are not protected as expected.

USING THE FACILITY CLASS

Historically, FACILITY has been responsible for controlling access to the VECTOR processing services on your processor. Does anyone still use **IEAVECTOR** profiles?

In the past, several profiles have been devoted to tape management. In these days of silos and tape cartridges, it hardly seems worth mentioning the **IEC.TAPERING** resource. This profile controls a user's ability to use a tape for input without requiring the operator to take out the "write enable ring," if present. In its time, this was a great boon to computer operators who were not keen on having OS demount the tape and require the ring's removal before remounting the tape. This profile does not apply for 3480 and 3490 tape devices.

At present, **ICHBLP** and **ICHNL** still control the use of DFP (Data Facility Products) services: Bypass Label Processing (BLP) and No Label (NL) processing respectively. READ access to the profiles allows the user to use BLP- or NL-defined tapes for input, while UPDATE access grants them output access. RACF checks these profiles only if the TAPEVOL class is active.

First, there is no comprehensive reference defining *all* FACILITY class profiles. The FACILITY class is unique in that multiple products, both written by IBM and non-IBM vendors, place their profiles within it.

Storage Management Subsystem (SMS) is one more DFP user of FACILITY class profiles. Profiles named **STGADMIN.**** control who is allowed to invoke protected functions. *The SMS Manual for Catalog Functions* lists dozens of such resources. For example, STGADMIN.IGG.DIRCAT (directed catalog) controls the IDCAMS ALTER functions for directing where an SMS-managed dataset is cataloged as well as EXPORT, EXPORT DISCONNECT, IMPORT and IMPORT DISCONNECT operations. Other IDCAMS-based profiles include STGADMIN.IDC.DCOLLECT, which controls access to DCOLLECT services, STGADMIN.IDC.DIAGNOSE.type, which controls access to various DIAGNOSE functions, and many more.

Job Entry Services

When jobs enter a system image from either Remote Job Entry (RJE) or Network Job Entry (NJE), the Job Entry Subsystem (JES) can be told to require and validate the RACF password instead of the JESPARMS password. JESPARMS stores passwords in clear text; RACF encrypts stored passwords. The following FACILITY class profiles invoke RACF checking for RJE and NJE connections:

- **RJE.workstation:** Requires JES to validate the password for the workstation using RACF.
- **NJE.nodename:** Requires JES to validate the password for the network node using RACF.

Instead of being a true allow/disallow access profile, these function more as a switch. If the workstation or node name is matched (as *.* would be), the password is verified via RACF. Otherwise, the JESPARMS password is used. For example, "CSVAPF.**" is a comprehensive (service level i.e., dynamic APF) but not a global profile in RACF to lock down dynamic APF (see below) without triggering RJE/NJE processing. Otherwise, only those services for which profiles exist are restricted; those not covered by profiles are not restricted. However, an RJE.** or NJE.** profile would activate RACF password enforcement on all nodes and workstations, if desired.

Dump Services

When a program ABENDs within a controlled environment (either Program Access to Data Set [PADS] or EXEC-only access to a dataset), OS/390 protects the data that may reside in storage by refusing to allow a system dump (via SYSUDUMP, SYSABEND, or other dump DD card). The only exception is when the userid assigned to the job (STC, TSO or batch) has READ access to the **IEAABD.DMPAUTH** profile.

RACF Services

While the Storage Management Subsystem (SMS) makes problems with uncataloged datasets a thing of the past, there are some

Figure 2: Searching Your RACF Database — A Detailed Search

```
RLIST FACILITY * ALL
CLASS          NAME
FACILITY       ICHBLP

LEVEL    OWNER      UNIVERSAL ACCESS   YOUR ACCESS   WARNING
 00      SYSGRP           NONE             NONE         NO

. . .
```

Figure 3: Profiles

Profile Prototype	Service
BPX.**	OpenEdition services
CSVAPF.*.**	Dynamic APF list (ESA 4.3)
CSVDYNEX.*.**	Dynamic Exits control (ESA 5.1)
CSVDYNL.*.**	Dynamic LinkList (OS/390 R2.4)
CSVLLA.dsname	LinkLibrary Lookaside updates
ICHBLP	Bypass (tape) Label Processing
ICHNL	Non-Label (tape) Processing
ICHUNCAT.data.set.name	Access to uncataloged data sets
ICHUSERCAT	JOBCAT and STEPCAT authorization
IEAVECTOR	VECTOR services
IEC.TAPERING	Read tape with write ring intact
IGG.**	Catalog Management
IRRDPI00	RACF Dynamic Parse Initialization
IRR*.**	RACF Services
MVSADMIN.*.**	Cross System Communication
NJE.nodename or RJE.workstation	Job Entry Subsystem remote access password validation
STGADMIN.*.**	Storage Management Subsystem (SMS)

FACILITY class profiles controlling those RACF options that originally managed uncataloged datasets.

- **ICHUNCAT.data.set.name:** Makes it possible for READ-level users to access uncataloged datasets on volumes controlled by DFP. Activated by SETROPTS CATDSNS.

- **ICHUSERCAT:** Enables users with READ access to the profile to use JOBCAT and STEPCAT JCL statements when SETROPTS CATDSNS is in effect. Otherwise, their use is denied.

Use of RACF segments requires an initialization of the Dynamic Parse tables by means of a started task run at Initial Program Load (IPL). Normally, the started task IRRDPITAB runs at IPL to perform this initialization when it has READ access to the IRRDPI00 profile.

RACF enhanced its own decentralized user support with two new profiles:

- **IRR.PASSWORD.RESET:** New in Release 2.4, enables authorized users to reset passwords without requiring them to have GROUP or SYSTEM SPECIAL. READ access authorizes the user to RESUME and change the password to an expired value; UPDATE access allows use of the NOEXPIRED parameter. Granting the help desk personnel READ access to IRR.PASSWORD.RESET will enable them to reset a user's password (subject to appropriate procedures) without assigning them GROUP SPECIAL, which has been the traditional method in most cases.

- **IRR.LISTUSER:** READ level access makes it possible for authorized users to list other user's profiles using LISTUSER command; base segment fields controlled by Field Level Access Control (FLAC).

Distributed Computing Environment

Distributed Computing Environment (DCE) and digital certificates are becoming critical services in the enterprise environment and SAF calls are available to control their use as well. Each has its own definitions in the security database:

- **IRR.RDCERUID** controls the use of the SAF R_dceruid callable service, which maps the DCE UUID to the RACF user ID.

- **IRR.DIGTCERT.function** profiles control the use of functions within the Digital Certificate service (the RACDCERT command, introduced in OS/390 release 2.4). READ access allows the user to issue functions on his own behalf, and UPDATE access allows him to issue it on behalf of other users. This can be valuable in a decentralized environment.

Dynamic OS/390 Services

As 24x7 coverage becomes more important, an increasing number of OS/390 services have moved into a dynamic arena. Instead of continuing to build the list at IPL and locking it until the next IPL, these dynamic services make it possible to change the system environment and modify: Link Library list, APF list, exits list and the Link List (also known as the LNKLST).

Previously, these tables were built at IPL and were unchangeable until the next IPL. However, vendors and users provided ways to make changes, usually without SAF calls, to authorize and/or track the changes. Now, each of these dynamic tables reference PROGxx parmlib member(s) for their changes (or the SETPROG command enters the changes directly within the command without referencing parmlib).

First came the LinkList Lookaside (later named Link Library lookAside) or LLA. This service improves system performance by storing the directories of specific datasets in storage (a.k.a. BLDL in years gone by). This list uses **CSVLLA.data.set.name** profiles to provide a means to control who is able to manipulate the list of program libraries on the LLA list as defined in parmlib member(s) CSVLLAxx.

Next, MVS/ESA 4.3 introduced dynamic Authorized Program Facility (APF) lists. Since by definition, APF-authorized modules within APF-authorized libraries are considered to be part of the operating system, controlling changes to the APF list is critical. The new PROGxx member supersedes IEAAPFxx and makes it possible to change the APF library list without requiring an IPL. The CSVAPF.data.set.name profiles authorize users to add, remove or change specific library entries in the APF list. If a program calls dynamic APF services, it must have APF-authorization.

Dynamic exits became available in MVS 5.1. Prior to this, if multiple products or services made use of the same system exit (e.g., SMF exit IEFACTRT), it was necessary to manually connect the exits. This service made it possible to chain multiple modules into a single exit point without cumbersome link-editing or building an exit driver at each installation. Exits can now be added, removed, activated, etc., using PROGxx members of parmlib or the SETPROG command. The RACF resource checked for such calls is **CSVDYNEX.exitname.function/modname.** UPDATE access is required to make any changes to the exit environment.

The newest service, dynamic linklist,

uses FACILITY class profiles named **CSV-DYNL.lnklstname.function** to control its functions. UPDATE access to the profile is also required to authorize the specified dynamic linklist definition.

OpenEdition/MVS

OpenEditon/MVS, or Unix Server, as it is now known, has increased its use of RACF (originally OMVS segments within the user and group profiles) and now supports the fol-lowing resources within the FACILITY class:

- **BPX.SUPERUSER:** Read access allows standard users to gain superuser authority for OMVS resources.
- **BPX.DAEMON:** Daemon programs (similar in function to MVS subsystems) needing to validate passwords before changing the UID and GID of spawned (spun) address spaces (commonly: RLOGIND, TELNETD, FTPD and IBMWBSRV).
- **BPX.SERVER:** Enables users (such as OMVS daemons) to customize the security environment of a thread. The thread may execute under a RACF identity other than that of the daemon. The users normally are server programs that need to associate a surrogate MVS identity (for example, IBMWBSRV).
- **BPX.DEFAULT.USER:** Specifies the userid employed for assigning UID if the user signing onto OMVS has no OMVS segment. Similarly, if the user's default connect group has no OMVS segment, this same profile will be checked for a groupid, which will be used to supply the GID value for the group.

Sysplex (XCF) Administration

When multiple system images work together in a coupled environment, policies are built by the installation to make things run smoother in case one of the system images should fail. Maintenance to the various policies is controlled by more FACILITY class profiles: **MVSADMIN.XCF.policy-or-service** such as ARM (Automatic Restart Management) or LOGR (creation/deletion of Logstream structures). With these profiles READ access allows the policies to be reviewed and reported, while UPDATE allows the user to change which policy is active.

There is also a set of profiles named **IXLSTR.structure-name** where, for example, IXLSTR.IEFAUTOS controls Auto Tape Switching. See Figure 3.

SUMMARY

Remember as you are reviewing these profiles to ensure that the following steps are considered:

- Global profiles (e.g., * or ** in RACF) should not be used, as this will imply more protection than is desired. Instead, use a profile containing the base portion of the service name (e.g., MVSADMIN.*.**) to protect that subset of FACILITY class services.
- UACC and ID(*) accesses are generally NONE.
- The profile is not in WARN mode (sort of defeats the purpose).
- Ensure that any profile not matching those in the table is accounted for as either a new IBM service or an OEM vendor-defined profile.

As you can see, the FACILITY class is very useful and provides a wealth of system service controls. The question becomes, "Are you using it effectively?" Vendors other than IBM most likely use resource definitions not matching those listed, so check the SECURITY chapter of each product to update your list of FACILITY class users. In many cases, products or OS/390 services will write an SMF record to document usage of some services controlled by FACILITY class profiles. However, it is also an option to set the security profiles to record successful READ access to the resources. ts

Mark S. Hahn is an IT consultant for IBM Corporation. He has been in mainframe computer security and audit for more than 20 years. An avid student of parmlib as well as MVS control and audit services, he presents at computer security and audit conferences worldwide.