RSH CONSULTING

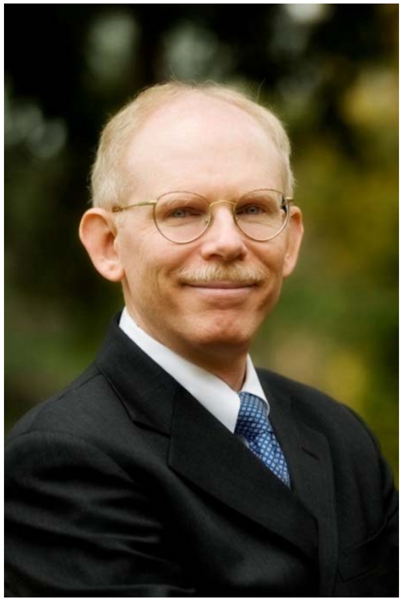
APPL Class

October 2015

RSH Consulting - Robert S. Hansel

RSH Consulting, Inc. is an IT security professional services firm established in 1992 and dedicated to helping clients strengthen their IBM z/OS mainframe access controls by fully exploiting all the capabilities and latest innovations in RACF. RSH's services include RACF security reviews and audits, initial implementation of new controls, enhancement and remediation of existing controls, and training.

- www.rshconsulting.com
- 617-969-9050



Robert S. Hansel is Lead RACF Specialist and founder of RSH Consulting, Inc. He began working with RACF in 1986 and has been a RACF administrator, manager, auditor, instructor, developer, and consultant. Mr. Hansel is especially skilled at redesigning and refining large-scale implementations of RACF using role-based access control concepts. He is a leading expert in securing z/OS Unix using RACF. Mr. Hansel has created elaborate automated tools to assist clients with RACF administration, database merging, identity management, and quality assurance.

- 617-969-8211
- R.Hansel@rshconsulting.com
- www.linkedin.com/in/roberthansel
- http://twitter.com/RSH_RACF

Topics

- Overview
- CDT Entry
- APPL Profile
- RACF Callers
- Monitoring
- Violations
- Performance
- Best Practices

Overview

- Profiles in the APPL class typically govern who can enter an application
  - Resources are often related to an application's VTAM Application ID (APPLID)
- APPL class
  - Predefined - provided with RACF
  - Independent - not tied to any particular product
  - Stand-alone - member class with no companion grouping class; unique POSIT
- APPL resource authorization checking
  - Access is checked during RACINIT and RACROUTE REQUEST=VERIFY or VERIFYX processing if the RACF Caller specifies a value for parameter APPL=
    - Global Access Table is not checked in these requests
    - APPL= can be specified on other RACROUTE calls (e.g., FASTAUTH), but this is used for information only and not authorization checking
    - PassTickets uses the APPL= value to determine the applid used in its resource names
  - Access can also be checked via a RACROUTE REQUEST=AUTH,CLASS='APPL' ...
  - READ permission is typically sufficient for application entry
  - If no profile protects an APPL resource, access is typically allowed

CDT Entry

- ID = 8
- POSIT = 3

- MAXLNTH = 8
- FIRST = ALPHA
- OTHER = ALPHANUM
- KEYQUAL = 0

- DFTRETC = 4
- DFTUACC = NONE
- OPER = NO

- GENLIST = ALLOWED
- RACLIST = ALLOWED
- RACLREQ = NO

APPL Profile

```
RLIST APPL CICSPLFA AUTH
CLASS      NAME
-----      ----
APPL       CICSPLFA

LEVEL  OWNER      UNIVERSAL ACCESS   YOUR ACCESS  WARNING
-----  --------   ----------------   ---- ------  -------
 00    CICSGRP         NONE               READ     NO

INSTALLATION DATA
---------------------------------------------------
CICS LIFE APPL PRODUCTION REGION

APPLICATION DATA
----------------
RACF-INITSTATS(DAILY)
...

USER      ACCESS    ACCESS COUNT
----      ------    ------ -----
LIFEGRPA   READ
ACCTPAY    READ
INTAUDIT   READ
TECHSPT    READ
CICSUSER   READ
```

RACF Callers - Partial List

- CICS
- IMS
- TSO
- FTP
- NSS
- CIM
- ICSF Trusted Key Entry
- RMF Distributed Data Server
- z/OS UNIX
- Websphere Application Server (WAS)
- NetView
- Rational Developer for System Z
- Tivoli Workload Scheduler (TWS)
- Omegamon
- 3rd party products (e.g., CA-7)
- VTAM Session Managers
- APPC/MVS

RACF Callers

- CICS
  - APPL *applid* - resource is determined by one of these SIT parameters
    - APPLID=*applid* - Region’s application ID
    - APPLID=(*generic-applid,specific-applid*) - XRF generic application ID (when XRF=YES)
    - GRNAME=*grname* - TOR Group ID (CICSplex)
  - The following users need access to the APPL resource for their respective region
    - SIT DFLTUSER=*userid* - CICS Default User
    - SIT PLTPIUSER=*userid* - Program Load Table Post-Initialization (PLTPI) User
    - EXEC CICS START TRANID(*userid*) - Started Transaction Users
    - CSD TERMINAL USERID=*userid* - Preset Terminal Users
    - CSD TDQUEUE USERID=*userid* - Automatic Transaction Initiation (ATI) Users
    - CSD CONNECTION and SESSION USERID=*userid* - IDs assigned to remote CICS regions
  - For MRO only, the APPLID of the Terminal Owning Region (TOR) is passed to the Application and File Owning Regions (AORs and FORs) for user ACEE creation
    - AORs and FORs can have different APPLIDs than the TOR, and users need not be permitted access to them
    - Users can be forced to logon only to TORs by assigning different APPLIDs to the AORs and FORs and not permitting users access to these APPLIDs

RACF Callers

- IMS
  - Resource is specified by SAPPLID parameter in member DFSDCxxx if its PROCLIB
    - Defaults to the IMSID name specified in the IMSCTRL macro or start-up procedure
  - If Resource Access Security (RAS) security is activated, all authorized IMS dependent region USERIDs must be permitted access (e.g., MPP, BMP, CICS)
- IMS Database Recovery Facility: Extended Functions IMSCMD function
  - If the IMSCMD Security field in the RECONID record is set to APPL (instead of NONE or IMS), access to a resource in the APPL class is used to govern command authority
  - RACF Class field in the RECONID record specifies the name of the APPL resource
  - READ allows a user to issue IMS commands that display IMS system information
  - UPDATE allows a user to issue IMS commands that alter IMS system resources
- NetView -resource is *domain-id*, which the manuals specify as CNM01
- Rational Developer for System Z - resource is specified by APPLID parameter in member FEJJCNFG of its PARMLIB; default is FEKAPPL
- RMF Distributed Data Server - resource is GPMSERVE
  - RMF XP - GPM4CIM component - resource is GPM4CIM

RACF Callers

- TSO (beginning with z/OS 1.10)
  - APPL checking is activated by setting PARMLIB member IKJTSOnn parameter VERIFYAPPL to YES (default setting is NO)
  - Resource is either …
    - **TSO*ssss*** - where '*ssss*' is the SMF system ID from PARMLIB member SMFPRMnn
    - ***VTAM-generic-name*** - name specified by the GNAME parameter of the Terminal Control Address Space (TCAS) started task when VTAM generic resources are being used for TSO
- FTP - resource is the jobname of the FTP server (e.g., FTPSERVE)
- Network Security Services (NSS) server - resource is NSSD
- Common Information Model (CIM) server - resource is CFZAPPL
- Omegamon II for CICS - Common User Access (CUA) interface - if configured to use RACF, default resource is CTDC2n (older versions use KC2nnAP)
- ICSF Trusted Key Entry - resource is CSFTTKE
- Kerberos - kpasswd command - resource is SKRBKDC
- Hardware Configuration Definition (HCD) - resource is CBDSERVE

RACF Callers

- Abend-AID - if configured to use RACF, resource is the viewing server's name
- BMC - MAINVIEW - APPL resources

BBVLOGON	- Alternative Access application entry
BBVEXCP	- EXCP terminal sessions used with Alternative Access
vtamnode	- VTAM major nodename used with Alternative Access

RACF Callers

- CA-7 - resource is specified by the optional APPL parameter in the SECURITY control statement; if not specified, no RACROUTE APPL= value is passed
- CA ROSCOE - (EXTSEC=RACF and ACFEXT=YES) resource is its *applid*
- CA Chorus for DB2 Database Management
  - CA Database Management Solutions for DB2 for z/OS - resource is DB2TOOLS
  - CA Chorus Investigator Object Migrator function (Migrate) - resource is CHORWEBS
- CA NetMaster NM for TCP/IP
  - Specify value for APPL= in security exit
  - Default resource if not specified is *region job name*
- CA Chorus for Storage Management - resource is VANTAGE
- CA Spool - resource is ESF
- CA SYSVIEW for CA Insight DPM for DB2 - resource is *xnet_applid* specified in the CA DB2 Tools Xnet INITPARM dataset parameter PASSNAME
- CA Chorus Software Manager (CSM)
  - Configuration parameter - IJO="$IJO -DmsmApplid=*applid*"
  - Default resource is CSMAPPLM

RACF Callers

- z/OS UNIX
  - Resource - OMVSAPPL
  - Used for the following services when APPL= not otherwise specified
    - __login
    - pthread_security_np
    - __passwd - when ...
      - There is no password or password phrase change specified
      - The calling process did not call pthread_security_np
  - In certain cases for the following services, the value used for the APPLID can be changed by altering APPLID related fields in the mapping macro BPXYTHLI
    - pthread_security_np
    - __passwd
  - Following C functions allow APPLID other than OMVSAPPL to be specified
    - __login_applid
    - __passwd_applid
    - pthread_security__applid_np
  - Most authorization checks use LOG=NONE

RACF Callers

- Websphere Application Service (WAS)
  - APPL only checked if the checkbox "Use APPL profile to restrict access to the server" on the SAF authorization options panel in the administrative console
    - Resource name is the "SAF profile prefix" defined using the z/OS Profile Management Tool
    - Default resource is CBS390 (some manuals erroneously list it as CB390)
  - z/OS Management Facility (z/OSMF) started task ID will need access to the APPL resource of the WAS server it uses; default appears to be BBNBASE
  - Websphere Liberty Profile (WLP) - APPL resource name is specified by the profilePrefix attribute in the <safCredentials> config element; default is BBGZDFLT
- Tivoli Workload Scheduler (TWS - formerly OPC) - Job Scheduler
  - Resource is TWS's *applid*
  - Uses APPL access for internal access authorization as well as entry control - the UACC and permissions establish a user's default access authority to TWS resources
    - READ allows all view type TWS functions
    - UPDATE allows TWS job management functions
    - If no profile is defined, UPDATE access is assumed
    - Overridden if a function is more explicitly controlled via a profile in the IBMOPC class

RACF Callers

- Some VTAM Session managers can optionally use access to APPL profiles to dynamically build a menu of allowed applications for each user
  - **IBM - CL/Supersession**
    - Requires the following entries in TLVPARM DD library (e.g., &rhilev.RLSPARM)
      - Member KLVINNAM - CLASSES=dynaplst (name of member with security options)
      - Member dynaplst - VGWAPLST EXTERNAL=APPL (APPL class is the default)
    - Resource names are defined by APPLDEF commands or session profiles
  - **IBM - Session Manager for z/OS**
    - E22 user signon exit - ISZE22DM - builds dynamic menus
    - SYSTEM statement - SECURITY parameter - subparameters
      - DYNMClass - FACILITY default (set to APPL)
      - DYNMResnm - resource name prefix - no default (do not use with APPL class)
      - DYNMTYPE - APPL | VTAMAPPL - determines applid used in resource name
    - *[dynmresnm-prefix*.]*applid* - READ - Application appears on dynamic menu
  - **MacKinney - VTAM/Switch**
    - GSFDFCT Control Table parameter AXRACF is used to activate this feature and select the associated resource class - APPL is the default class
  - **CA TPX**
    - Only applies to 'dynamic' users (those not defined as 'static' users in the TPX database)
    - Set "Load Profiles at Startup" to "Y" in the Performance Parameters panel (TEN0101)
    - Set "Resource Class:" to "APPL" TPX System Options Table Detail Panel (TEN0090)
    - Set "Profile Selection:" to "PROF" TPX System Options Table Detail Panel (TEN0090)
    - *tpx-profile-name* - READ - Display and allow access to application(s) defined to a TPX profile

RACF Callers

- APPC/MVS
  - Protect conversations between partner Logical Units (LUs) by restricting access to the luname
  - LUs are defined in VTAM
  - APPL resources
    - *local-luname*
    - *Generic-resource-name* Specified in GRNAME parameter on VTAM LUADD statements
  - Can use conditional permissions limiting access to a local LU based on the partner LU from which a request is originating

    PERMIT *local-luname* CLASS(APPL) WHEN(APPCPORT(*partner-luname*)) …
  - The ID specified in the GENERIC_ID keyword on the Transaction Program (TP) profile (i.e., definition) of multi-trans TPs must be permitted to access protected APPL LU resources
  - Access to the luname is also checked during RACROUTE REQUEST=SIGNON for managing APPC LU6.2 Persistent Verification (PV) requests

Monitoring

- SETROPTS AUDIT(APPL)

- SETROPTS LOGOPTIONS(FAILURES(APPL))
  - ALL or SUCCESSES not recommended for performance degradation reasons

- SETROPTS APPLAUDIT
  - Enables auditing of APPC transactions
  - AUDIT settings on associated APPL class profile determine what logging is to be done
  - Can produce excessive SMF data if the APPL profile specifies AUDIT(SUCCESS(READ) or ALL(READ)) and the application does not support persistent verification

- RDEFINE / RALTER APPL *profile* AUDIT(…) GLOBALAUDIT(…) as appropriate

Access Violation

- RACINIT and RACROUTE Return Code
  - 34 The user is not authorized to use the application

- ICH408I Message

  USER(userid) GROUP(group) NAME(user-name)

  LOGON/JOB INITIATION - NOT AUTHORIZED TO APPLICATION *applname*

- CICS - "DFHCE3545 Application authorization failed. Sign-on is terminated."

- SMF Unload Records
  - JOBINIT - Job Initiation (Logon)
    - Field containing APPL value - INIT_APPL - starting in position 282
    - Authorized Access Event - RACINITI (CICS logon)
    - Violation Event - INVAPPL Not a valid application
  - INITOEDP - Initialize Unix Process (dub) - does not show APPL (e.g., FTP logon)
  - ACCESS - Generated for authorized access to APPL resource (if logged)

Performance Enhancement

- SETR RACLIST(APPL) is highly recommended because it improves performance for all logons, especially those for the on-line applications
  - Note: SETR RACLIST(APPL) REFRESH causes VLF to drop all saved ACEEs

- Reduce RACF database I/O by skipping date and time of last access updates to user profiles for all but the first logon of the day by adding the following APPLDATA field value to APPL profiles (beginning with z/OS 1.11)

  RALTER APPL *profile* APPLDATA('RACF-INITSTATS(DAILY)')

  - To enable use of this performance feature with RACROUTE calls that lack an APPL= value, code an IRRRIX01 exit to add an APPL= value (e.g., NOAPPL) to any REQUEST=VERIFY and VERIFYX without an APPL and then define a corresponding APPL profile to RACF with the APPLDATA entry above

Best Practices

- Define all known APPL resources
  - Consider using RACFVARS to reduce number of profiles

- Restrict access just for sensitive applications and lunames or for those applications the general user population does not need (e.g., AORs/FORs, test regions, Omegamon)

- Define catch-all profile ** UACC(READ) AUDIT(ALL) to record new APPLs for remediation

- RACLIST the APPL class

- Synchronize with VTAM Session Managers - use the APPL class for building menus if feasible