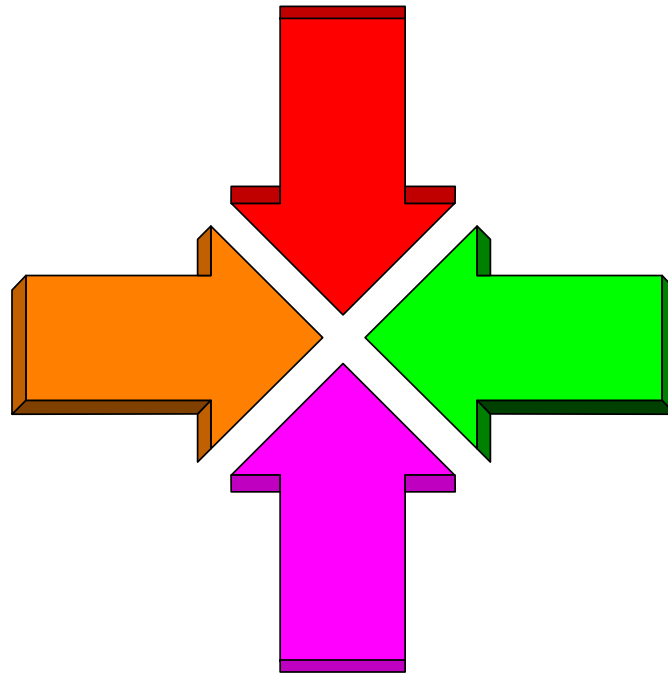


FACILITY CLASS PROFILE POTPOURRI

Vanguard Security Conference 2011 - Session RAA8 - June 2011



Robert S. Hansel

Lead RACF Specialist - RSH Consulting, Inc.

R.Hansel@rshconsulting.com - 617-969-9050 - www.rshconsulting.com

RSH PRESENTER



Robert S. Hansel is Lead RACF Specialist and founder of RSH Consulting, Inc., a firm he 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. He has worked with IBM mainframes since 1977 and in information systems security since 1981. Mr. Hansel began working with RACF in 1986 and has been a RACF administrator, manager, auditor, instructor, developer, and consultant. He has reviewed, implemented, and enhanced RACF controls for major insurance firms, financial institutions, utilities, payment card processors, universities, hospitals, and international retailers. Mr. Hansel is especially skilled at redesigning and refining large-scale implementations of RACF using role-based access control concepts. He has also created elaborate automated tools to assist clients with RACF administration, database merging, identity management, and quality assurance.

Contact and background information:

- 617-969-8211
- R.Hansel@rshconsulting.com
- www.linkedin.com/in/roberthansel

FACILITY CLASS

General purpose, pre-defined RACF general resource class

Intended for use by resource managers with too few profiles to justify a separate resource class

Used by IBM resource managers, 3rd party products, and installation-written routines and exits

Profile purposes:

- **Authorization** - allow use of resources or functions
- **Activation** - existence of profiles activates functions
- **Defaults** - provide default control information

Each resource manager determines whether a particular access or function will be allowed if a profile is not found

3rd party products and installations are encouraged to use national characters in first qualifier so as not to conflict with IBM products

RACF and z/OS are Trademarks of the International Business Machines Corporation

FACILITY CLASS CDT ENTRIES

FACILITY

ID = 19

POSIT = 8

MAXLNTH = 39

FIRST = ANY

OTHER = ANY

KEYQUAL = 0

DFTRETC = 4

DFTUACC = NONE

OPER = NO

GENLIST = ALLOWED

RACLIST = ALLOWED

RACLREQ = NO

SIGNAL = NO

XFACILIT / GXFACILI

ID = 1

POSIT = 8

MAXLNTH = 246

FIRST = ALPHANUM

OTHER = ANY

KEYQUAL = 0

DFTRETC = 8

DFTUACC = NONE

OPER = NO

GENLIST = ALLOWED

RACLIST = ALLOWED

RACLREQ = NO

SIGNAL = YES

RESOURCE MANAGERS USING FACILITY CLASS

RACF

OSA/SF

Integrated Security Services

JES

Unix System Services

CICS

DFSMS

IMS

DITTO / File Manager

APPCMVS

MVS

z/OS Health Checker

WLM & SYSPLEX

Others

BCPii

- **IBM**
- **Third Party**
- **Installation**

System Automation

RACF

Control delegation of security administrative authorities

- List user profiles (base only, not segments), except those with System-level SPECIAL, OPERATIONS, and AUDITOR
 - IRR.LISTUSER - All users
 - IRR.LU.OWNER.*owner* - Users owned by user or group
 - IRR.LU.TREE.*group* - Users owned by groups in scope
 - IRR.LU.EXCLUDE.*userid* - Excludes users in OWNER or TREE
 - ◆ READ - list user profile

- Reset user passwords, except those with System-level SPECIAL, OPERATIONS, AUDITOR, or PROTECTED IDs
 - IRR.PASSWORD.RESET - All users
 - IRR.PWRESET.OWNER.*owner* - Users owned by user or group
 - IRR.PWRESET.TREE.*group* - Users owned by groups in scope
 - IRR.PWRESET.EXCLUDE.*userid* - Excludes users in OWNER or TREE
 - ◆ READ - Resume user, reset password/phase to expired value
 - ◆ UPDATE - Resume user, reset password/phase to non-expired value
 - ◆ CONTROL - Change password prior to MINCHANGE interval

RACF

Control delegation of security administrative authorities (continued)

- **IRR.DIGTCERT.function** - Digital Certificate administration
 - **READ** - Issue DIGTCERT command for own ID
 - **UPDATE** - Issue DIGTCERT command for other IDs
 - **CONTROL** - Issue DIGTCERT command for SITE & CERTAUTH certificates
- **IRR.WRITEDOWN.BYUSER** - MLS security level "write-down" privilege
 - **READ** - Set privilege with explicit use of RACPRIV or writedown
 - **UPDATE** - Set privilege by default upon system entry

IRRDPI00 - **READ**- Load RACF Command Parsing Table

IRR.PGMSECURITY - Determines program protection mode
APPLDATA('BASIC' | 'ENHANCED')

ICHDSM00.SYSCAT - **READ** - List User Catalogs with DSMON

Program object signature verification - APPLDATA('key-ring-reference')

- **IRR.PROGRAM.SIGNING** - Signature key ring
- **IRR.PROGRAM.SIGNATURE.VERIFICATION** - Verification key ring

RACF

Permit use of RACF Callable Services (mostly by unauthorized callers)

- **IRR.RADMIN.command**
 - **READ** - Allow unauth caller to execute RACF command via R_Admin
- **IRR.RADMIN.EXTRACT.PWENV**
 - **READ** - Allow extraction of enveloped passwords
- **IRR.RAUDITX**
 - **READ** - Allow unauth server to use R_AUDITX to generate SMF 83 records
- **IRR.RCACHESERV.cachename**
 - **READ** - Allow unauth server to fetch cache info using R_Cacheserv
 - **UPDATE** - Allow unauth server to use all functions
- **IRR.RDCEKEY**
 - **READ** - Allow unauth server to use R_dcekey to enable DCE server to retrieve or set DCE key
- **IRR.RDCERUID**
 - **READ** - Allow unauth server to use R_dceruid to translate DCE IDs

RACF

Permit use of RACF Callable Services (mostly by unauthorized callers)

- **IRR.RGETINFO.EIM**
 - **READ** - Allow unauth server to use R_GetInfo to retrieve Security Server information

- **IRR.RPKISERV.*function***
 - **READ** - Allow access based on checks against the caller's user ID
 - **UPDATE** - Allow access based on checks against the application's user ID
 - **CONTROL** - Allow access with no subsequent access checks

- **IRR.RPROXYSERV**
 - **READ** - Allow unauth caller to use R_proxyserv

- **IRR.RTICKETSERV**
 - **READ** - Allow unauth server to use R_ticketserv

- **IRR.RUSERMAP**
 - **READ** - Allow unauth server to use R_usermap

RACF

PWDCOPY Utility Functions - READ

- RACF.PASSWORD.MAINTENANCE.EXPORT
- RACF.PASSWORD.MAINTENANCE.IMPORT

RACKILL Utility - UPDATE

- RACKILL

CUTPWHIS Utility - READ

- RACF.PASSWORD.MAINTENANCE.HISTORY.LNGTH

RACTRACE Command - READ

- RACTRACE.RACTRACE

ICHPWX01 Exit Sample - READ

- IRR.ICHPWX01.OVERRIDE

DBShield - GXFACILI - Automatically maintained by RACF

- IRRPLEX_ *sysplex-name* APPLDATA('[NON-]DATA SHARING MODE')
- Checked at IPL and RVARY and alerts operator of invalid sharing actions

INTEGRATED SECURITY SERVICES

Firewall **{Obsolete as of z/OS 1.8}**

- FWKERN.START.REQUEST - READ - Start Firewall
- ICA.CFGSRV - UPDATE - Allow configuration admin

LDAP, EIM Domain, Kerberos

- IRR.PROXY.DEFAULTS - Store default settings in PROXY & EIM segments

SSL

- GSK.SIDCACHE.*cache-owner* - READ - Access session information across Sysplex

Open Cryptographic Service Facility (OCSF)

- CDS.CSSM - READ - Allow a daemon to call OCSF services
- CDS.CSSM.CRYPTO - READ - Allow a daemon to call a
Cryptographic Service Provider (CSP)
- CDS.CSSM.DATALIB - READ - Allow a daemon to call a Data
Library (DL) Service Provider

INTEGRATED SECURITY SERVICES

Enterprise Identity Mapping (EIM) - Remote services

- **IRR.LDAP.REMOTE.AUTH**
 - **READ** - Check own access authority to a resource
 - **UPDATE** - Check another user's access authority to a resource
- **IRR.LDAP.REMOTE.AUDIT**
 - **READ** - Allow remote audit requests

Distributed Computing Environment (DCE)

- **DCEKERN.START.REQUEST - UPDATE - Start DCE**
- **DCESECD.START.REQUEST - UPDATE**
- **DCECDSD.START.REQUEST - UPDATE**
- **DCEDTSTP.START.REQUEST - UPDATE**
- **DCEAUDD.START.REQUEST - UPDATE**
- **DCEPWDD.START.REQUEST - UPDATE**
- **DCEGDAD.START.REQUEST - UPDATE**

DFS / SMB / ZFS

- **DFSKERN.START.REQUEST - UPDATE - Start DFS**

UNIX SYSTEM SERVICES

Control, activate, and manage USS authorities

Resources - READ access required (+ UPDATE for BPX.SERVER)

- BPX.CF Use Coupling Facility sizer tool (`_cpl()`)
- BPX.CONSOLE Use authorized console features (`_console()`, `_console2()`)
- BPX.DAEMON Control use of Daemon system calls
- BPX.DAEMON.HFSCTL Load of any MVS programs - bypass PROGRAM check
- BPX.DEBUG Run ptrace to debug APF programs (BPX1PTR)
- BPX.EXECMVSAPF.*program* Allow non-authorized caller to pass arguments of more than 100 characters
- BPX.FILEATTR.APF Set APF authorization on HFS file
- BPX.FILEATTR.PROGCTL Set program control attribute on HFS file
- BPX.FILEATTR.SHARELIB Set shared library extended attribute
- BPX.JOBNAME Set job name for new process (`_BPX_JOBNAME`)
- BPX.MAP Use storage mapping services (BPX1MMI)
- BPX.UNLIMITED.OUTPUT Override default spooled output limits when spawning
- BPX.POE Use Port-of-Entry for MLS security checks (`_poe`)
- BPX.SERVER Control use of Server system calls
- BPX.SHUTDOWN Special treatment at shutdown (BPX1ENV)
- BPX.SMF Allowed to write SMF record (BPX1SMF)
- BPX.STOR.SWAP Make address space non-swappable (BPX1ENV)
- BPX.SUPERUSER Permit 'su' to superuser
- BPX.WLMSEVER Access to WLM functions (BPX1SIN, BPX1WLM)

Resources - Control options

- BPX.DEFAULT.USER Default uid / gid
- BPX.MAINCHECK Requires loading MVS program marked MAIN
- BPX.NEXT.USER Automatic uid / gid assignment
- BPX.SAFFASTPATH Enable z/OS Unix to allow access without RACF calls
- BPX.UNIQUE.USER Automatic OMVS segment creation with unique uid / gid assignment

DFSMS

Control who can manage catalogs and data using DFSMS/MVS utilities and services

Resources - READ

- STGADMIN.ADR.STGADMIN.*command*
 - STGADMIN.ADR.*command[.parm]*
 - STGADMIN.ANT.*component.function*
 - STGADMIN.ARC.ENDUSER.*cmd[.parm]*
 - STGADMIN.ARC.*command[.parm]*
 - STGADMIN.DFSMSOPT.*function*
 - STGADMIN.DPDSRN.*oldname*
 - STGADMIN.EDG.MASTER
 - STGADMIN.EDG.*function[.parm]*
 - STGADMIN.HMT.*function*
 - STGADMIN.ICK.*command*
- DSS - ADMINISTRATOR
DSS
Data Mover
HSM - End-User 'H' commands
ABARS & HSM
SMS Monitor/Tuner
IDCAMS
RMM Superuser (CONTROL)
RMM (+ UPDATE, CONTROL)
StorWatch HSM Monitor
ICKDSF

DFSMS

Resources - READ

- STGADMIN.IDC.*command[.parm]* IDCAMS
- STGADMIN.IFG.READVTOC.*volser* DFP
- STGADMIN.IGG.*function* IDCAMS - SMS-managed entries
- STGADMIN.IGD.ACTIVATE.CONFIGURATION SMS
- STGADMIN.IGWSHCDS.REPAIR IDCAMS

Other related resources - READ

- IGG.CATLOCK ICF Catalogs
- ICHBLP Bypass Tape Label Processing (+ UPDATE)
- ICHUNCAT.*dsname* CATDSNS - uncatalog dataset
- ICHUSERCAT CATDSNS - use private catalog
- IEC.TAPERING Bypass tape ring removal for read
- IHJ.CHKPT.*volser* Create checkpoints on shared DASD

DITTO / FILE MANAGER

Control use of DITTO's and File Manager's functions to manipulate tape and DASD datasets, including full disk volume processing

Resources - READ (*prefix* = DITTO or FILEM)

- *prefix.FUNCTION.function-code* - If defined, controls use of function
- *prefix.group.function-set*
 - Controls use of sets of functions, excluding those individually defined by FUNCTION
 - *Group*: DISK | TAPE | VSAM | OAM | OTHER
 - *Group* (FILEM only): LOADMOD | BASE* | CICS* | DB2 (* - SEC=YES in FNMnPOPT)
 - *Function-set*: INPUT | OUTPUT | DUPLICATE | UPDATE | ALL (varies by *Group*)

If product is running authorized, users can:

- DITTO.TAPE.MOUNT - READ - Mount tapes without TSOAUTH MOUNT authority
- *prefix*.TAPE.BLP - READ - Use BLP even when JESPARMS do not permit
- *prefix*.DISK.FULLPACK
 - READ - Read and update access to specific volsers*
 - UPDATE - Read access to all volsers, update to specific ones*
 - ALTER - Read and update access to all volsers

* - Also Requires READ or ALTER to associated DASDVOL *vol/ser* profile

MVS - DYNAMIC SERVICES

Control who can make dynamic changes to LLA, APF, LPA, Exits, and Linklist using the related CSV-prefixed Macros

Resources - UPDATE

- **CSVLLA.*lladataset***
- **CSVAPF.*library-name***
CSVAPF.MVS.SETPROG.FORMAT.[DYNAMIC | STATIC]
- **CSVDYLPA.[ADD | DELETE].*modname***
- **CSVDYNEX.LIST**
**CSVDYNEX.*exitname*.[DEFINE | UNDEFINE | ATTRIB | CALL |
RECOVER | *modname*]**
- **CSVDYNL.*linklstname*.[ADD | DEFINE | DELETE | ACTIVATE |
UNDEFINE | TEST]**
CSVDYNL.UPDATE.LNKLST

MVS - HCD

Control who can access IPL and I/O configuration information related to the Hardware Configuration Definition (HCD)

CBD.CPC.IPLPARM - Access IPLADDR and IPLPARM values

- **READ** - Query value
- **UPDATE** - Update values - effects next IPL

CBD.CPC.IOCCDS - Access I/O Configuration Dataset information

- **READ** - Query value
- **UPDATE** - Update values
- **If not defined, console operator must authorize update**
- **Requires UPDATE access to OPERCMDS resource MVS.ACTIVATE to activate a configuration change**

WLM & SYSPLEX

Control who can administer Work Load Manager (WLM) and SYSPLEX policy

Resources

- READ - View policies
- UPDATE - Change policies & use IXCDELETE utility
- ALTER - Define or delete log structure (MVSADMIN.LOGR only)
- MVSADMIN.EWLM.AGENT - Enterprise Workload Manager calls
- MVSADMIN.LOGR - Log Stream policy
- MVSADMIN.WLM.POLICY - Work Load Manager service definition
- MVSADMIN.XCF.ARM - Automatic Restart Management policy
- MVSADMIN.XCF.CFRM - Coupling Facility Resource Mgmt policy
- MVSADMIN.XCF.IXCM2DEL - IXCDELETE Utility
- MVSADMIN.XCF.SFM - Sysplex Failure Management policy
- MVSADMIN.RRS.COMMANDS - Resource Recovery Services
- MVSADMIN.RRS.COMMANDS.*gname.sysname* - Resource Recovery Services

- IXLSTR.*structure-name* - Coupling facility structure
 - ALTER - Maintain structure
- IXCARM.*elemtype.elemname* - ARM entity
 - UPDATE - Permit unauthorized program use of ARM

SYSPLEX - RMF

Control who can access Resource Measurement Facility (RMF) data for Sysplex data services

Resources - READ

- **ERBSDS.SMFDATA** - Access to SMF data in SMF buffers
- **ERBSDS.MON2DATA** - Access Monitor II SMF type 79 data
 - Access not checked for local system's data on MON2 panels
 - Access of NONE prevents use of SDSF DA panel - no info displayed
- **ERBSDS.MON3DATA** - Access Monitor III performance data
 - Not checked for access via LDAP, must disable RMF LDAP requests to protect

BCPii

Control who can query and change the System z hardware configuration for Central Processor Complexes (CPCs) and system images using the Base Control Program internal interface (BCPii)

Resources

- HWI.APPLNAME.HWISERV - READ - Use BCPii
- HWI.TARGET.*netid.nau* - Access CPC by SNA name
- HWI.TARGET.*netid.nau.imagename* - Access system image
- HWI.CAPREC.*netid.nau.caprec* - Access capacity record

Permissions

- READ - Establish communications, retrieve configuration information
- UPDATE - Set, update configuration
- CONTROL - Use hardware management command

Notes:

- If using SNMP, HWI.TARGET.*netid.nau* profile must include `APPLDATA('snmp-community-name')`
- An SNMP Community Name is required for the local CPC
- FACILITY class must be RACLISTed

Tivoli System Automation

Control who can query and change the Coupling Facility (CF) and Cross-system Coupling Facility (XCF) configuration for Central Processor Complexes (CPCs) and system images using SA's enhanced Parallel Sysplex functions that use the BCPii

Resources

- HSA.ET32OAN.HSAET32 - READ - Use the SA functions
- HSA.ET32TGT.*netid.nau* - Access CPC by SNA name
- HSA.ET32TGT.*netid.nau.imagename* - Access system image

Permissions

- READ - Retrieve, get configuration information
- UPDATE - Set, update configuration
- CONTROL - Issue operations management commands

FACILITY class must be RACLISTed

Tivoli System Automation

Control who can manage Enterprise Systems Connection (ESCON) and Fibre Connection (FICON) connectivity in an active I/O configuration using SA's I/O Operations component and related APIs

Resources

- **IHV.command[.function]**

Permissions

- **READ** - Use Display and Query commands
- **UPDATE** - Use most commands, operands, and options
(Excludes Force, Delete, Write, Logrec, Sync, Lock, Reset)
- **CONTROL** - Use all I/O Operations commands, operands, and options

**Authorization is not checked for commands entered at the system console;
CONTROL access is assumed**

OSA/SF

Control who can use Open Systems Adapter Support Facility (OSA/SF) commands

- OSA is an integrated S/390 hardware feature that provides industry-standard connectivity (e.g., Ethernet) directly to clients on LANs and WANs
- OSA/SF is the software that manages the OSA configuration

Resources

- *IOA.command[.function]*

Permissions

- **READ** - View OSA address table and debugging information
- **UPDATE** - Use most commands and all the options
(Excludes Set Parm, Clear Debug, Install, Force, Get/Put File)
- **CONTROL** - Use all OSA/SF commands with all the options

DUMPS

Control who can dump certain types of address spaces (with SYSUDUMP, SYSABEND, and SYSMDUMP statements)

Resources

- IEAABD.DMPAKEY - READ - Programs with System Key < 8
- IEAABD.DMPAUTH - APF Authorized Programs
 - READ - Dump any program unless only EXECUTE authority
 - UPDATE - Dump any program

To prevent possible deadlocks, RACLIST the FACILITY class (could occur even if not protecting dumps)

For additional non-RACF methods of controlling dumps, refer to z/OS MVS Recovery and Reconfiguration Guide

JES

Control who can establish an RJE connection - replaces hard-coded RJE/RJP logon passwords

Resources

- *RJE.jes2-workstation-name*
- *RJP.jes3-workstation-name*

Notes

- RJE signon requires creation of USERID corresponding to workstation name (e.g., RMT1)
 - ID must exist and cannot be REVOKED, else logon fails
 - Assigned password is used to authenticate signon -- cannot be PROTECTED
- Specify NOEXPIRE and NOINTERVAL to prevent password expirations
- Has no relation to USERID assigned to jobs submitted via connection
- Last logon not updated - IDs may be mistaken for obsolete due to inactivity

JES

Determine whether RACF will control use of operator commands transmitted by a remote system via NJE - replaces JES NODE AUTH parameters

Resource

- ***NJE.submitting-nodename-userid***

Notes

- **NJE node identification requires creation of USERID corresponding to remote node name -- if no ID or if ID is REVOKED, operator commands fail**
- **Specify NOPASSWORD to make PROTECTED**
- **Has no relation to USERID assigned to jobs submitted via connection**
- **NODES class 'RUSER' profiles must have UACC of READ or more**
submitting-nodename.RUSER.submitting-nodename-userid
- **NJE nodename ID needs permission to OPERCMDS profiles**

CICS

Control who can bind to a CICS region using MRO

- **DFHAPPL.cics-applid**
 - **UPDATE** - Required for a region to access to its own applid
 - **READ** - Required to connect to the applids of other CICS regions

Control who can connect to a CICS region using the External CICS Interface (EXCI)

- **DFHAPPL.target-cics-applid**
 - **READ** - Required for the EXCI calling region to connect a CICS region
- **DFHAPPL.DFHXCCEIP**
 - **UPDATE** - Required for EXCI calling region using EXEC CICS LINK command
- **DFHAPPL.exci-userid**
 - **UPDATE** - Required for EXCI calling region using INITIALIZE_USER commands

Control who can change the AUTHTYPE on DB2 connection definitions

- **DFHDB2.AUTHTYPE.authname**
 - **READ** - Use authname
 - May need to give access to CICS region's ID for startup processing

Control who can act as a server for a Temporary Storage pool

- **DFHXQ.poolname**
 - **CONTROL** - Act as a pool server

Control who can access a Named Counter pool

- **DFHNC.poolname**
 - **UPDATE** - Connect to a pool server
 - **CONTROL** - Act as a pool server

Control who can access a Coupling Facility Data Table

- **DFHCF.poolname**
 - **UPDATE** - Connect to a pool server
 - **CONTROL** - Act as a pool server

CICS

CICSplex - READ

- Allow a Coordinating Address Space (CAS) and CICSplex System Manager (SM) Address Space (CMAS) to define a subsystem
 - **SUBSYS.*ssid*.[DEFINE | INIT]** (*ssid* - subsystem id)
- Allow connect to a CAS
 - **BBM.*ssid*.CN**
- Allow opening a context window and service point
 - **BBM.*smfid*.PLEXMGR.*context*.TA**
 - **BBM.*smfid*.CPSM.*context*.[TA | TC]**
- Allow use of PlexManager views and actions
 - **BBM.PLEXMGR.*smfid.functions***
- Allow use of views and actions when accessed via CMAS
 - **BBM.CPSM.*context.functions***
- Allow CAS to initialize with external security disabled
 - **BBMSS.ESMTYPE.NONE - UPDATE - BBSECURE ESMTYPE=NONE**

CICS

CICSplex System Manager (SM) Web User Interface (WUI)

- Allow use of WUI functions (does not protect objects they manage - see SM security)
 - EYUWUI.wui-server-applid.VIEW.viewsetname
 - EYUWUI.wui-server-applid.MENU.menuname
 - EYUWUI.wui-server-applid.MAP.mapname
 - EYUWUI.wui-server-applid.HELP.helpmembername
 - EYUWUI.wui-server-applid.EDITOR
 - ◆ READ - Use views and menus in the main interface or export using COVC
 - ◆ UPDATE - Create, update, or remove items in the view editor or import using COVC

CICS

CICS Configuration Manager (CM)

- **CM Configuration parameters**
 - **SAFClass** (Default: FACILITY) API Commands
 - **ObjectSAFClass** (Default: FACILITY) Resource Definition Keys
 - **SAFPrefix** (Default: CCM) API Command resource name prefix
 - **ObjectSAFPrefix** (Default: CCM) Resource Definition Keys resource name prefix
- **Allow use of CM API Commands - READ**
 - *api-saf-prefix.command[.functions]*
- **Allow manipulation of CICS resource definitions**
 - *object-saf-prefix.source/target-cics-config.type-object.name*
 - ◆ **READ** - Inquire target configuration, Copy-from source configuration
 - ◆ **UPDATE** - Update target configuration
 - ◆ **ALTER** - Add, Create, Delete, Import, Remove, Rename, Copy-to target config

IMS

IMS

- **CQS.cqsid** - UPDATE - Access Common Queue Structure (CQS)
- **CQSSTR.structure-name** - UPDATE - Connect to CQS structure

IMS Open Transaction Manager Access (OTMA)

- **IMSXCF.OTMACI** - READ - Access Callable Interface
- **IMSXCF.xcfgname.mqxcfmname** - READ - Join XCF group

IMS Listener Service - Security Exit (sample)

- **TPI.IMSSOCK.trancode** - READ - Access tran via call to TPIAUTH

IMS - Queue Control Facility (QCF)

- **IQC.mvsid.imsid.function**
 - **READ** - Perform Query and Browse
 - **UPDATE** - Perform Load, Unload, and Recover

IMS Connect

- **HWS.ims_connect_name** - UPDATE - Allow connection

APPCMVS

APPCMVS Administration

Control who can perform database token maintenance

- **APPCMVS.DBTOKEN**
 - **READ** - Perform DBRETRIEVE
 - **UPDATE** - Perform DBMODIFY

Control who can assign an ID to a multi-transaction profile

- **APPCMVS.TP.MULTI.genusrid** - UPDATE

Control who can use trace API on TP

- **ATBTRACE.netid.lu_name.tp_name** - READ

z/OS HEALTH CHECKER

Control who can initiate, print, and manage checks

Uses XFACILIT / GXFACILI classes

Resources (depends on use of wildcarding in request)

- READ (HZSQUERY) reqtype MESSAGES, QUERY
- UPDATE (HZSCHECK) reqtype ACTIVATE, UPDATE, DEACTIVATE, RUN
- CONTROL (HZSCHECK, HZSADDCK) reqtype DELETE, REFRESH
- ***HZS.sysname.reqtype***
- ***HZS.sysname.check_owner.reqtype***
- ***HZS.sysname.check_owner.check_name.reqtype***

RACF related health-check resources

- ***HZS.sysname.reqtype***
- ***HZS.sysname.IBMRACF.reqtype***
- ***HZS.sysname.IBMRACF.RACF_GRS_RLN.reqtype***
- ***HZS.sysname.IBMRACF.RACF_SENSITIVE_RESOURCES.reqtype***
- ***HZS.sysname.IBMRACF.RACF_class_ACTIVE.reqtype***
 - ***Class: FACILITY OPERCMDS TAPEVOL TEMPDSN TSOAUTH UNIXPRIV***
- ***HZS.sysname.IBMRACF.RACF_IBMUSER_REVOKED.reqtype***

MISCELLANEOUS - IBM

Vector Facility **{Obsolete - related hardware no longer exists}**

- IEAVECTOR - READ - Control use of Vector Facility

IP Printway

- AOPADMIN - READ - Permit use of Infoprint Server ISPF panels
{Obsolete - with Infoprint 1.5, profile ignored if PRINTSRV profile AOP.ADMINISTRATOR is defined}

Run Time Library Service (RTLS) **{Obsolete - phased out in z/OS 1.12}**

- CSVRTLS.LIBRARY.*library.version* - READ - Use of an RTLS library
- CSVRTLS.CONNECT - UPDATE - Exceed limit of 32 connections to RTLS libraries
- CSVRTLS.NOSECCONNECT.*library.version* - Existence of profile negates security check
 - Note: If using generics to negate security checks, the profile must begin with at least "CSVRTLS.NOSEC"; anything less (e.g., CSVRTLS.*) will be ignored

BatchPipes

- PSP.ASFPIPE.*bpsubsystemname* - READ - Use BatchPipe Subsystem

IBM Extended Facility Support (IXFP)

- IXFP.FORCE.DELETE.FUNC.DEV - READ - Remove RAMAC devices

Graphical Data Display Manager (GDDM)

- ADM.ADMPQM - READ - Access GDDM Print Queue Manager

MISCELLANEOUS - IBM

Dynamic Symbol Update (IEASYMUP)

- IEASYMUP.*symbol-name* - UPDATE - Change symbol value

Batch Local Shared Resources Subsystem (BLSR)

- CSR.BLSRHIPR.*blsr-subsysname* - READ - Place buffers in named hiperspace

Session Manager for z/OS

- E22 user signon exit - ISZE22DM - builds dynamic menus
- SYSTEM statement - SECURITY parameter - subparameters
 - DYNMClass - FACILITY default
 - DYNMResnm - resource name prefix - no default
 - DYNMType - APPL | VTAMAPPL - determines *applid* used in resource name
- [*dynamresnm-prefix*].*applid* - READ - Application appears on dynamic menu

Integrated Cryptographic Services Facility (ICSF)

- CSFTTKE - READ - Allow use of Trusted Key Entry Host Program

Interactive Problem Control System (IPCS)

- BLSACTV.SYSTEM - READ - Access absolute storage & other address/data spaces
- BLSACTV.ADDRSPAC - READ - Access Key 0 visible storage & own data spaces

MISCELLANEOUS - IBM

Data Lookaside Facility (DLF)

- **COFXTAB**
 - **READ** - List table of datasets & jobs eligible for Hiperbatch processing
 - **UPDATE** - Create or modify table entries using COFXUPDT

RACROUTE API on VM

- **ICHCONN**
 - **READ** - Issue 'non-authorized' requests
 - **UPDATE** - Issue 'authorized' requests

IBM Tivoli Output Manager (ITOM) for z/OS

- **Parameter library startup command member - BJT#IN03**
 - **SAF SET ID *saf-id*** - Enables SAF security and establishes first qualifier on resource names
 - **PROTVIEW SAF** - Activate view security
- ***saf-id.stc-id.MENU.MAIN***
 - Permitted level of access determines authority type (USER, AUDITOR, ADMIN) and default access
 - If not defined to RACF, defaults to ADMIN authority with minimum access of READ
- ***saf-id.stc-id.resource-type[.resource-id]***
 - **READ** - USER authority, view resource
 - **UPDATE** - AUDITOR authority, view configuration options
 - **CONTROL** - ADMIN authority, set and change configuration options
 - If not defined to RACF, inherit access authority granted to MENU.MAIN
- ***saf-id.stc-id.SECV*** - **UPDATE** - Bypass view restrictions (checked when PROTVIEW SAF)

MISCELLANEOUS - IBM

Websphere for z/OS

- BBO.TRUSTEDAPPS.*cell-short.cluster-tran* - CONTROL - authenticate a user without a password
- BBO.SYNC.*cell-short.cluster-tran* - READ - temporarily assume the identity of an application ID
 - Used in conjunction with SURROGAT BBO.SYNC.*userid* resource permissions

z/OS Real Storage Manager (RSM)

- IARRSM.LRGPAGES - READ - obtain large pages in real storage

Tivoli Advanced Catalog Management for z/OS (ACM)

- Checks access to each resource, from most to least qualifiers, until a profile is found
 - IBMTIVOLI.ACM.*command.keyword.keyword* - READ - execute command with secondary keyword
 - IBMTIVOLI.ACM.*command.keyword* - READ - execute command with primary keyword
 - IBMTIVOLI.ACM.*command* - READ - execute command
 - IBMTIVOLI.ACM - READ - execute all commands
- ACM utility CKM00010 with SYSIN of 'OPTIONS PERMISSIONS' lists every resource and its associated RACF profile

System Modification Program / Extended (SMP/E)

- GIM.CMD.*command* - READ - execute command
- GIM.PGM.*program* - READ - execute program
- Introduced in IBM Integrity & Security APAR IO11698 (see APAR II14489 for additional information)
- Access is denied unless explicitly permitted

MISCELLANEOUS - IBM

Global Resource Serialization

- ISG.QSCANSERVICES.AUTHORIZATION - READ - use ENQ and GQSCAN when MLACTIVE is active
 - FACILITY class must be RACLISTed

Application Performance Analyzer for z/OS

- CONFIG BASIC statement - SecurityClassName option - FACILITY default
- *system-name.action.object* - READ - Perform monitoring action

NetView Access Services (NVAS)

- *userid_nvas-external-group*
 - Profiles created and maintained by NVAS exit EMSEADEx for NVAS groups marked as 'external'
 - USERDATA fields used to store menu of applications and their characteristics
 - No access permissions required
 - Default class in EMSEADEx is FACILITY (IBM recommends using NVASAPDT for new implementations)

ADJUNCT RACF ADMIN PRODUCTS

IBM Tivoli zSecure - default XFACILIT class {former Consul prefixes - FACILITY class}

- *CKF.function* (\$CNF) - Collect component of Admin, Audit, Visual, Compliance Insight
- *CKG.function* (\$CNG) - Admin
- *CKR.function* (\$C2R) - Admin, Audit, Alert, Visual
- *C2R.function* (\$C2R) - Visual
- *C2X.function* (\$C2X) - Exit Activator
- *C4R.function* (\$C4R) - Command Verifier
- *TOOLKIT.SVC* - zToolkit's SVC

Vanguard Integrity Professionals

- *VRA\$.function* - RACF Administrator
- *VRAADM\$.function* - RACF Administrator
- *VRAPW\$.function* - RACF Administrator - password administration
- *VIP\$.function* - RACF Administrator
- *VSA\$.function* - RACF Analyzer
- *VSR\$.function* - RACF Advisor
- *EZRESET\$.function* - ezRESET
- *\$RIO.function* - Vanguard Security Center

Software Engineering of America - RACF Administrator 2

- *RA2.function*

Allen System Group - ASG-Admin for Security Server

- *DSM.function*

Betasystems - Beta 88 zSecurity Administrator

- *BETA.INIT.subsystem-id*

THIRD-PARTY PRODUCTS

CA Disk Backup and Restore

- SYSPARM - SMSTGADddd - Defines resource name 'ddd' for Storage Admin authority
- STGADMIN.DMS.STGADMIN - READ - (default 'ddd' name) Storage Admin authority
- STGADMIN.DMS.STGADMIN.*command*[*operand*] - READ - Use command & operand
- DISK.SYSPARM.*sysparm* - READ - Override certain system parameters

CA XCOM - Data Transport

- Default Options Table - LUSECURE=YES - Activates security SAF calls
- XCOM.*applsec*.[IP | LU].*destname*.[SEND | RECEIVE].[L | R] - READ - Initiate transfer

CA - SOLVE:CPT

- T09MCMDS macro - SECNAME=*entity* - defines resource name
- \$SKTVIEW.CICS.COMDAUTH - default resource name
 - READ - Display session, server and global statistics
 - UPDATE - Start and stop transactions, sessions, servers and applications

CA Netmaster product series & CA Solve: product series

- JCL Parameter - SEC=NMSAF - Activates NMSAF security component
- NMSAF - SXCTL parameter file - RCLASS=*classname* - Defines class - default FACILITY
- NMSAF - SXCTL parameter file - MODELGROUP *resource model* - defines resources to be checked
- *resource*[*region*] - READ - Use functions associated with model set
- NETMASTR.[ADMIN | OPER | NOPER | MON][*region*] - READ - default resources & models

THIRD-PARTY PRODUCTS

CA TCPaccess X.25 Server

- **SYSTEM** command - **SEC=YES** - Activates security SAF calls
- **TASK** command - **SAFCLASS** parameter - Defines class - default FACILITY
- **OMX.CONSOLE** - **READ** - Access console

CA ESP Workload Manager (batch scheduler)

- **SAFCLASS class PREFIX(prefix)** parameter - samples recommend FACILITY and PREFIX(ESP)
- *prefix.function* - **READ / UPDATE** depending on function

CA Vantage Storage Resource Manager (hierarchical storage manager)

- **VKGPARMS DD** parameters - **SECURRES (Y)** - (default) Use FACILITY class
- **SYSSSM.FUNC** - **ALTER** - Perform all functions
- **SYSSSM.FUNC.function-code** - **READ** - Perform specific function

CA TRILOGexpert TriTune

- **TUNSSP00** parameter - **SECCLASS=classname** - default FACILITY
- **TUNSSP00** parameter - **SECPREFIX=profile-prefix** - default TRITUNE
- *profile-prefix.servername.function.[resource]* - **READ** - Perform function on target resource

CA Sysview

- **SAFSECX** exit variable - **&GRCLASS=classname** - default FACILITY
- *SV.function.system.[qualifiers...]* - **READ / UPDATE** depending on function

THIRD-PARTY PRODUCTS

Cole Software - Extended Debugging Controller (XDC)

- XDC.AUTH - READ - Run in authorized mode (can bypass security controls)
- XDC.FASM.*addrspace*
 - READ - Read foreign address space contents
 - UPDATE - Zap or debug a foreign address space
- XDC.ZAP.*memitem* - UPDATE - Zap memory location or module
- XDC.GZAP - ALTER - Zap common storage (replace with XDC.ZAP profiles)
- XDC.LOSTLOCKS - READ - continue debug even after code locks are lost

RocketSoftware - MVS Extended Information (MXI)

- MXICMD.*function*

Mainstar - Catalog RecoveryPlus

- MAINSTAR.CR+.*function* - READ - Perform function

Hitachi Data Systems - Business Continuity Manager

- STGADMIN.YKA.BCM.COMMANDS - READ - Use control-type commands
- STGADMIN.YKA.BCM.YKQUERY - READ - Use query-type commands

THIRD-PARTY PRODUCTS

Innovation Data Processing

- **Fast Analysis of Tape Surfaces (FATS)**
 - **FATS.function** - READ - Control use of functions, including BLP
 - **Must apply ZAP to activate function calls**
- **Fast Analysis of Tape and Recovery (FATAR)**
 - **FATAR.DATASET.SECBYPAS** - READ - No access checked for input
 - **FATAR.function** - READ - Control use of functions, including BLP
 - **Must apply ZAP to activate function calls**
- **FDR Plug and Swap (FDRPAS)**
 - **FDRPAS.function** - READ - Perform function
- **FDRCRYPT**
 - **FDRCRYPT.keyname** - Store encryption key
- **FDRERASE**
 - **FDRCRYPT.function** - READ - Perform function

ASPG - Megacryption

- **MGCKEYS.DEK.xxxx** - RACF keyboxes (conventional, symmetric keys)
- **MGCKEYS.PKR.xxxx** - RACF encryption keyrings (asymmetric)
- **MGCKEYS.SIG.xxxx** - RACF signature keyrings (asymmetric)

THIRD-PARTY PRODUCTS

Data Direct - SequeLink Server

- SECURITYCLASS parameter - FACILITY default
- Instrumentation Interface (II)
 - SQLNKACC - READ - Issue II display-type commands
 - SQLNKAUT - READ - Issue server commands
- Service Security
 - *servicename* - READ - access service in connection request

Compuware

- STROBE
 - Must activate access filter in initialization parameters by clearing DISABLE from FILTER= parm
 - Using PROFILE= initialization parameter, can set first qualifier to suffix other than STROBE
 - \$STROBE.*sysid.type.jobname* - READ - Monitor address space of specified type & name
 - \$STROBE.MANAGER - READ - Execute STROBE in batch
 - \$STROBE.ADMIN - READ - Perform administration functions, includes all access
- Enterprise Common Components - License Management System
 - CPWR.PRODUCT.LICENSE.LM010001 - CONTROL - enables entry of operator commands
 - Access is granted to LMSINIT Started Task

Information Builders - iWay Software - iWay Server for MVS

- IBI.CONSOLE.*authority* - READ - Use LOGON, OPERATOR, or DETAIL authority

THIRD-PARTY PRODUCTS

Softworks - Catalog Solution for z/OS {bought by EMC - now obsolete}

- `SOFTWARE.CSL.access.command` - READ - Issue command at intended access

EMC - Catalog Solution for z/OS

- `EMC.CSL.access.command` - READ - Issue command at intended access

Dino-Software - T-Rex (Access Method Services/Extended)

- `AMSE.access.command` - READ - Issue command at intended access (READ / UPDATE)

ActionSoftware - eventACTION

- `MZCA.GLOBAL` - UPDATE - Enable user to function as a Global Administrator

TeraCloud Corp - SpaceFinder

- `SPACEFINDERWORKBENCH.function` - READ - Perform function

AQM Solutions - InTune (formerly from BMC)

- `BBINTUNE.server-id.function[.resource]` - READ - Access, administer, & monitor jobs

THIRD-PARTY PRODUCTS

BMC - Mainview

- **BBM.*product.context.function*** - Perform windows-mode functions
 - BBSECUR DD member BBMTSP00 parameter NEXT='FACILITY'
- **BOOLEBBI** - Activates VTAM terminal logon panel
- **BOOLEBBV** - Alternate Access AutoLogon
- **BBMSS.ESMTYPE.NONE** - UPDATE - Allows product to run with security disabled

BMC - Extended Buffer Management

- **BMCXBM.*function***

BMC - VSAM Recovery Services - ALTER

- **BMCRUV.SUBSYS.*ssid***
- **BMCRUV.COMMAND**
- **BMCRUV.REPOSITORY**
- **BMC.RU(TM).FOR.VSAM.ALLOW.ALL.ACCESS** - Access for undefined resources

THIRD-PARTY PRODUCTS

BMC - Integrated Operations Architecture (IOA)

- Parameter IOASECP DEFMCHKI=\$\$IOAEDM,SECTOLI=YES,IOAClass=FACILITY
- \$\$SECIOA.qname - Activate security (pre-6.3 - discrete profile)
- \$\$IOAEDM.qname - Use Extended Mode Security
- \$\$function.qname.qual - Perform function

BMC - Control-M

- Parameter CTMSECP DEFMCHKM=\$\$CTMEDM,SECTOLM=YES
- \$\$SECCTM.qname - Activate security (pre-6.3 - discrete profile)
- \$\$CTMEDM.qname - Use Extended Mode Security
- \$\$function.qname.qual - Perform function

BMC - Control-M/Analyzer

- Parameter CTBSECP DEFMCHKB=\$\$CTBEDM,SECTOLB=YES
- \$\$SECCTB.qname - Activate security (pre-6.3 - discrete profile)
- \$\$CTBEDM.qname - Use Extended Mode Security
- \$\$function.qname.qual - Perform function

THIRD-PARTY PRODUCTS

BMC - Control-D & Control-V

- Parameter CTBSECP DEFMCHKD= \$\$CTDEDM,SECTOLD=YES
- \$\$SECCTD.qname - Activate security (pre-6.3 - discrete profile)
- \$\$CTDEDM.qname - Use Extended Mode Security
- \$\$function.qname.qual - Perform function

BMC - Control-M/Tape

- Parameter CTTSECP DEFMCHKT= \$\$CTBEDM,SECTOLT=YES
- \$\$SECCTT.qname - Activate security (pre-6.3 - discrete profile)
- \$\$CTTEDM.qname - Use Extended Mode Security
- \$\$CTTBYSEC.qname - Bypass security
- \$\$CTTBLP.qname.volser - Use BLP
- \$\$CTTBYPASS.qname.volser - Use EXPDT=98000 to bypass dataset access check
- \$\$function.qname.qual - Perform function

BMC - Control-O

- Parameter CTOSECP DEFMCHKO= \$\$CTOEDM,SECTOLO=YES
- \$\$SECCTO.qname - Activate security (pre-6.3 - discrete profile)
- \$\$CTOEDM.qname - Use Extended Mode Security
- \$\$function.qname.qual - Perform function

THIRD-PARTY PRODUCTS

Phoenix Software International - EJES TP Monitor

- PHNX.SYSTCMD.*tp-monitor-function* - READ - Perform function
- PHNX.SYSTSEC.*tp-monitor-user-type* - READ - Assume user type

Fisher International Systems - Interactive Output Facility (IOF)

- IOF.*function*

Triangle Systems - ISFManager for RACF

- TS9MASTR APPLDATA('surrogat-id') - SPECIAL user used to create profiles
- TS9OWNER APPLDATA('owner-id') - OWNER of profiles created via ISFManager
- TS9MGR.*function*
 - READ - Audit existing profiles
 - UPDATE - Change existing profiles
 - ALTER - Create profiles

THIRD-PARTY PRODUCTS

Teradata - Teradata Director Program

- *TDPid.dbc_user_name* - READ - Use the Teradata database logon ID

NewEra Software - The Control Editor

- *NEZ.NSEPARM.subsysname* - READ - make dynamic updates

Relational Architects International - RAI Dialog Facility

- *SDW* - READ - Execute all commands
- *SDW.command* - READ - Execute specific command

CCA Software Pty Ltd - NIMISPF (NATURAL Interface Monitor)

- NIM Table-Of-Constants (TOC) module NIMTPTOC
 - Resource Class Name Default FACILITY
 - Resource Prefix Default \$NIMSAF
- *resource-prefix.service* - READ - Access a service

Tectia - SSH Tectia Server for z/OS

- *SSZ.MOUNT* - READ - Transfer off-line dataset (e.g., tape, DASD not-mounted)

THIRD-PARTY PRODUCTS

Compute (Bridgend) Ltd - Selcopy

- SELCOPY/i INI file
 - ResourceClass= Default FACILITY
 - *Feature=* Resource name (e.g., UserTSO=SELCOPYI.TSO)
- *feature-resource-name* - READ - Use the feature

Williams Data Systems - Zen IP Monitor

- *IMPLEX.stackname* - READ - Allow monitoring of IP stack

THIRD-PARTY PRODUCTS

Syzygy - SyzCmdZ

- RCLASS parameter - FACILITY default
- SYZCMDZ
 - READ - Issue system display commands
 - UPDATE - Use special SyzCmdZ functions
 - ALTER - Issue modify and management-level system commands and use advanced SyzCmdZ functions
- *application.command* - application: COMMANDZ, MVS, JESx, OMVS, HMC, TCP, HSM, TDMF, EMAIL
 - READ - Issue display commands
 - UPDATE - Issue modify commands
 - CONTROL - Issue management-level commands

Trident Services - Operating System / Environment Manager (OS/EM)

- *JOBCLASS.jobclass* - READ - submit jobs in the associated job class
- *COMMAND.operator-command*
- *JES2.\$jes-command*
- *JCL.parm.value* - READ - Specify JCL parameter value
- *FEMCNTL.sysid.command* - READ - Manage OS/EM functions and user exits
- *OSEM.sysid.ADMIN.function* - READ - Use ISPF administration dialog functions
- *DISCRETE.PROFILE.class* - READ - Define RACF discrete profile in specific class
- *EXTERNAL.TAPE* - READ - Access undefined tape dataset bypass PROTECTALL
- *BYPASS.JOB.LIMITS* - READ - Bypass JES job limits
- *EXTEND.jes-limit* - READ - Exceed JES output and time limits

INSTALLATION CUSTOMIZATIONS

JES2 - Exit 6 - READ

- **JOBCLASS.*jobclass*** - READ - Allow use of job class
- **JOB.CPU.TIME.EXTEND** - READ - Exceed job CPU time limits
- **STEP.CPU.TIME.EXTEND** - READ - Exceed job step CPU time limits
- **WAIT.TIME.EXTEND** - READ - Exceed job wait time limits

DADSM - IGGPRE00 Exit

- **\$DASDI.*volser*** - UPDATE - Create datasets on non-SMS DASD
- **\$DASDI.NOVOLCHK** - UPDATE - Authority to all volsers

SAF Router Exit

- **\$SUBMIT.*userid*** - READ - Pre-SURROGAT submit **{obsolete}**

IND\$FILE Wrapper

- **IND\$FILE.[GET | PUT].*dsname*** - READ - Transfer file

STILL RESEARCHING

DSL.\$CONTROL (DTS Software - DLIMIT ?)

TPI.RACINIT

SSO.ADMIN (CA eTRUST ?)

SSO.USER (CA eTRUST ?)

FILEAID.xxx (Compuware - Fileaid ?)

PBCA.OPER.DASDCNFG

CADSDISP

DECDTF

HIPER (Compuware - Hiperstation)

REFERENCES

"Understanding Your FACILITY Class Profiles", Technical Support, Mark Hahn, January 1999
"FACILITY Class Overview", Kurt Meiser, June 1999
"Security's Multi-Purpose FACILITY Class", zJournal, Robert Hansel & Mark Hahn, April/May 2006
"RACF Protection for IND\$FILE", Xephon RACF Update, Jan De Decker, August 2004

GC18-9378 - File Manager for z/OS Customization Guide
GC19-2444 - IMS System Definition
GA22-7800 - UNIX System Services Planning
GA22-7509 - z/OS Planning for Multilevel Security and the Common Criteria
GC26-9598 - DITTO/ESA Installation and Customization Guide
GC28-1469 - MVS Programming: Batch Local Shared Resources Subsystem Guide
GC34-6777 - CICS Configuration Manager for z/OS User's Guide
GC35-0033 - Device Support Facilities User's Guide
GG66-3218 - RACF Security Administrator's Quick Reference
GI10-0670 - z/OS Program Directory for CBPDO Installation and Server Pac Reference
S544-5744 - z/OS Infoprint Server Customization
SA22-7458 - IBM BatchPipes OS/390 Users Guide and Reference
SA22-7522 - z/OS ICSF Systems Programmer Guide
SA22-7532 - z/OS JES2 Initialization and Tuning Guide
SA22-7549 - z/OS JES3 Initialization and Tuning Guide
SA22-7592 - z/OS MVS Initialization and Tuning Reference
SA22-7594 - z/OS MVS Interactive Problem Control System (IPCS) Commands
SA22-7599 - z/OS MVS Planning: APPC/MVS Management

REFERENCES

- SA22-7601 - z/OS MVS Planning: Operations
- SA22-7602 - z/OS MVS Planning: Workload Management
- SA22-7613 - z/OS MVS Programming: Callable Services for High-Level Languages
- SA22-7618 - z/OS MVS Programming: Sysplex Services Reference
- SA22-7625 - z/OS MVS Setting Up a Sysplex
- SA22-7683 - Security Server RACF Security Administrator's Guide
- SA22-7691 - z/OS Security Server RACF Callable Services
- SA22-7693 - z/OS Cryptographic Services PKI Service Guide and Reference
- SA22-7802 - UNIX System Services Command Reference
- SA22-7803 - UNIX System Services Programming: Assembler Callable Services Reference
- SA22-7821 - C/C++ Run-Time Library Reference
- SA22-7875 - z/OS Security Server Enterprise Identity Mapping (EIM) Guide and Reference
- SA22-7935 - Open Systems Adapter-Express Customer's Guide and Reference
- SA22-7994 - IBM Health Checker for z/OS User's Guide
- SA22-7997 - z/Series Platform Test Report for z/OS and Linux Virtual Servers
- SA23-2211 - z/OS ISCF Trusted Key Entry PCIX Workstation User's Guide
- SC18-7619 - IMS Queue Control Facility (QCF) User's Guide
- SC18-7829 - Open Transaction Manager Access Guide and Reference
- SC18-9200 - IBM Tivoli Output Manager for z/OS User's Guide
- SC19-1238 - File Manager for z/OS Customization Guide
- SC23-8511 - Application Performance Analyzer for z/OS Customization Guide
- SC23-9816 - IBM Tivoli Advanced Catalog Management for z/OS User's Guide
- SC24-5899 - z/OS Open Cryptographic Services Facility Application Programming

REFERENCES

- SC24-5910 - z/OS DCE Configuring and Getting Started
- SC24-5916 - Distributed File Service (DFS) Customization
- SC24-5922 - z/OS Security Server Firewall Technologies
- SC24-6150 - z/VM Security Server RACROUTE Macro Reference
- SC26-7405 - z/OS DFSMSrmm Implementation and Customization Guide
- SC26-7407 - z/OS DFSMS: Implementing System-Managed Storage
- SC26-7409 - z/OS DFSMS: Managing Catalogs
- SC26-7410 - z/OS DFSMS: Using Data Sets
- SC27-1292 - IMS Common Queue Server Guide and Reference
- SC31-7186 - IBM TCP/IP for MVS IMS TCP/IP Application Development Guide and Reference
- SC33-0871 - GDDM System Customization and Administration
- SC33-7988 - z/OS Hardware Configuration Definition User's Guide
- SC33-7990 - z/OS Resource Measurement Facility User's Guide
- SC34-2571 - Tivoli System Automation for z/OS Planning and Installation
- SC34-5651 - MQSeries® for OS/390 System Setup Guide
- SC34-6018 - CICSplex SM for CICS TS z/OS Web User Interface Guide
- SC34-6249 - CICS Transaction Server for z/OS CICS RACF Security Guide
- SC34-6252 - CICS Transaction Server for z/OS CICS DB2 Guide
- SC34-6287 - Session Manager for z/OS Facilities Reference
- SC34-6693 - Session Manager for z/OS Technical Reference
- SC35-0418 - z/OS DFSMSHsm Implementation and Customization Guide
- SC35-0421 - z/OS DFSMSHsm Storage Administration Guide

REFERENCES

SC35-0427 - z/OS DFSMS Object Access Method Planning, Installation, and Storage Administration Guide for Tape Libraries

SC35-0428 - z/OS DFSMS Advanced Copy Services

SG24-7308 - IBM Tivoli System Automation for z/OS Enterprise Automation

SG24-7384 - Security in WebSphere Application Server Version 6.1 and J2EE 1.4 on z/OS

SH19-4502 - NetView Access Services Customization

Enterprise Workload Manager z/OS Support Redpaper

z/OS Planned Outage Avoidance Checklist Redpaper

APAR OA25485 - New Function - FACILITY Class for RSM Large Page Access

SPECIAL THANKS TO ...

The following individuals contributed valuable information used to prepare this presentation:

Tony Babonas, AllState

Mark Hughes, RiteAid

Simon Dodge, SiCon, Inc.

Bob Kleamovich, CA

John McCandiss, McKesson Corporation

Rob van Hoboken, IBM

Russ Hardgrove, IBM

Terry Baker, Metavante

Mark Nelson, IBM

Free Alexis Val, Euroclear SA/NV

Joel Tilton, Publix

Jerry Seefeldt, NewEra Software

John Trimble, Sallie Mae

Dan Sloth, BankData

Scott Harder, ASPG

Gayle Sweitzer, Acxiom

Brian Westerman, Syzygy, Incorporated

Mike Onghena, IBM

Mike Kearney, IBM

Debra Spivey, Labcorp

Dave Constable

Scott Johnson, Fidelity Nat'l Information Service

David Freedman, William Data Systems

... and others who chose not to be listed