RSH CONSULTING

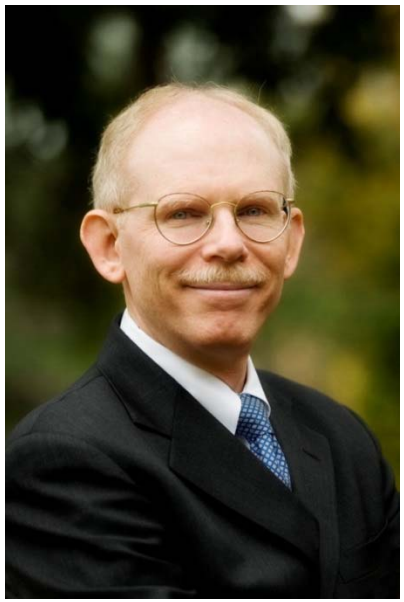
FACILITY Class

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

© 2015 RSH Consulting, Inc. All Rights Reserved.

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
Jerry Seefeldt, NewEra Software
Phil Peters, IBM
Marc van der Meer, IBM
Stuart Sabel, Premera Blue Cross

John Trimble, Navient
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
Tuco Bonno, State of South Carolina
Russell West, Compass Computing Resources
Blair Snyder, American Express
Daniel Burk, Jack Henry & Associates

… and others who chose not to be listed

© 2015 RSH Consulting, Inc. All Rights Reserved.

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

© 2015 RSH Consulting, Inc. All Rights Reserved.

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

© 2015 RSH Consulting, Inc. All Rights Reserved.

Resource Managers Using FACILITY Class

- RACF
- Integrated Security Services
- z/OS Unix
- DFSMS
- DITTO & File Manager
- MVS
- WLM & SYSPLEX
- BCPii
- System Automation
- OSA/SF
- JES
- CICS
- IMS
- APPCMVS
- z/OS Health Checker
- Others
  - IBM
  - Third Party
  - Installation

© 2015 RSH Consulting, Inc. All Rights Reserved.

RACF

- Control delegation of security administrative authorities
  - List user profiles (base only, not segments), except those with System-level SPECIAL, OPERATIONS, and AUDITOR
    - READ - list user profile
    - 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
  - Reset user passwords, except those with System-level SPECIAL, OPERATIONS, AUDITOR, or PROTECTED IDs
    - 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
    - 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

© 2015 RSH Consulting, Inc. All Rights Reserved.

RACF

- Control delegation of security administrative authorities (continued)
  - IRR.DIGTCERT.*function* - Digital Certificate administration
    - READ - Issue RACDCERT command for own ID
    - UPDATE - Issue RACDCERT command for other IDs
    - CONTROL - Issue RACDCERT 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' | *'warning')*

- 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

© 2015 RSH Consulting, Inc. All Rights Reserved.

RACF

- Permit use of RACF Callable Services (mostly by non-APF-authorized callers)
  - IRR.RADMIN.[*command* | SETROPTS.LIST]
    - READ - Execute RACF command via R_admin (still requires normal RACF command authority)
  - IRR.RADMIN.EXTRACT.[PWENV|PPENV]
    - READ - Extract enveloped passwords or phrases
  - IRR.RAUDITX
    - READ - Use R_auditx to generate SMF 83 records
  - IRR.RCACHESERV.[*cachename* | ICTX | ICRX]
    - Suffixes relate to function codes: X'0001'-X'0005', X'0006' (ICTX); X'0007' (ICRX)
    - READ - Use R_cacheserv Fetch and Retrieve-type options
    - UPDATE - Use all R_cacheserv options
    - To use function code X'0007' (ICRX), the FACILITY class must be RACLISTed
  - IRR.RDCEKEY
    - READ - Use R_dcekey to enable DCE server to retrieve or set DCE key
  - IRR.RDCERUID
    - READ - Use R_dceruid to translate DCE Ids
  - IRR.RGETINFO.[EIM | REALM]
    - READ - Use R_GetInfo to retrieve Security Server information

© 2015 RSH Consulting, Inc. All Rights Reserved.

RACF

- IRR.RPKISERV.*function*[.*ca-domain*] - Use R_PKIServ for PKI certificates
  - 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 - Use R_proxyserv to store and retrieve LDAP directory data
- IRR.RTICKETSERV
  - READ - Use R_ticketserv and R_GenSec with function code X'0001'
- IRR.GSSERV
  - READ - Use R_GenSec with function code X'0002'
- IRR.RUSERMAP
  - READ - Use R_usermap with function codes X'0001' to X'0006'
- IRR.IDIDMAP.[MAP | DELMAP | LISTMAP | QUERY]
  - READ - Create, delete, or list a distributed identity for own ID
  - UPDATE - Create, delete, or list a distributed identity for other users
- IRR.CHANGELOG - READ - Permit LDAP Server to retrieve RACF change log records

© 2015 RSH Consulting, Inc. All Rights Reserved.

RACF

- PWDCOPY Utility Functions
  - RACF.PASSWORD.MAINTENANCE.EXPORT - READ
  - RACF.PASSWORD.MAINTENANCE.IMPORT - UPDATE
- RACKILL Utility
  - RACKILL - UPDATE
- CUTPWHIS Utility
  - RACF.PASSWORD.MAINTENANCE.HISTORY.LNGTH - READ
- RACTRACE Command
  - RACTRACE.RACTRACE - READ
- ICHPWX01 Exit Sample
  - IRR.ICHPWX01.OVERRIDE - READ
- DBShield - GXFACILI class - Automatically maintained by RACF
  - IRRPLEX_sysplex-name APPLDATA('[NON-]DATA SHARING MODE')
  - Checked at IPL and RVARY and alerts operator of invalid sharing actions

© 2015 RSH Consulting, Inc. All Rights Reserved.

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
- 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

© 2015 RSH Consulting, Inc. All Rights Reserved.

Integrated Security Services

- Communications Server - SSL
  - GSK.SIDCACHE.*cache-owner* - FACILITY - READ - Access session information across Sysplex
  - GSK.ENABLE.SSLV3.DEFAULT - XFACILIT - Re-enable if defined (APAR OA46489)
  - GSK.ENABLE.SSLV2.DEFAULT - XFACILIT - Re-enable if defined (APAR OA46489)

- Enterprise Key Management Foundation (EKMF)
  - Components
    - z/OS EKMF Agent - Started Task
    - Key Management Workstation (KMW)
  - CRYPTO.DKMS.AUDITOFF - READ - Turn off SMF auditing; both Agent and user need access
  - CRYPTO.DKMS.CCFNOCVF - READ - Allow NOCV keys to be defined to ICSF from the KMW; both Agent and user need access
  - CRYPTO.DKMS.KMGPCCMD
    - READ - Browse RACF key rings; Agent requires READ
    - UPDATE - Allow key ring administration
    - CONTROL - Allow addition, alteration, and deletion of certificates
  - CRYPTO.DKMS.KMGPRACF - READ - Allow a user to start the Agent
  - CRYPTO.DKMS.KMGPRACF.*taskid* - READ - Allows logging on to a specific Agent via KMW
  - CRYPTO.DKMS.LNKCRYOFF - READ - Allow Agent to use unencrypted sessions - setup only

© 2015 RSH Consulting, Inc. All Rights Reserved.

Integrated Security Services

- DFS / SMB / ZFS
  - DFSKERN.START.REQUEST - UPDATE - Start DFS
- Distributed Computing Environment (DCE) {No longer shipped with z/OS as of 1.13}
  - 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

© 2015 RSH Consulting, Inc. All Rights Reserved.

Cryptographic Services

- Integrated Cryptographic Services Facility (ICSF) - FACILITY Class
  - CSFTTKE - READ - Allow use of Trusted Key Entry Host Program
- Open Cryptographic Service Facility (OCSF) - FACILITY Class
  - CDS.CSSM - READ - Allow daemon to use OCSF services
  - CDS.CSSM.CRYPTO - READ - Allow daemon to use Cryptographic Service Provider (CSP)
  - CDS.CSSM.DATALIB - READ - Allow daemon to use Data Library (DL) Service Provider

© 2015 RSH Consulting, Inc. All Rights Reserved.

Cryptographic Services

- Integrated Cryptographic Services Facility (ICSF) - XFACILIT Class
  - CSF.[C|P]KDS.TOKEN.CHECK.LABEL.WARN - Activate Key Token Authorization in Warn
  - CSF.[C|P]KDS.TOKEN.CHECK.LABEL.FAIL - Activate Key Token Authorization in Fail
  - CSF.[C|P]KDS.TOKEN.CHECK.DEFAULT.LABEL - Activate CSFKEY CSF-[C|P]KDS-DEFAULT
  - CSF.[C|P]KDS.TOKEN.NODUPLICATES - Activate Duplicate Key Token Checking
  - CSF.CSFKEYS.AUTHORITY.LEVELS.WARN (also see …FAIL permissions)
    - READ - Allow a user to create, write to, or delete a label
  - CSF.CSFKEYS.AUTHORITY.LEVELS.FAIL
    - UPDATE - Allow a user to create a label
    - CONTROL - Allow a user to write to or delete a label
  - CSF.CSFSERV.AUTH.CSFOWH.DISABLE - Disable One Way Hash (OWH) checking
  - CSF.CSFSERV.AUTH.CSFRNG.DISABLE - Disable Random Number Generation (RNG) checking
  - CSF.PKAEXTNS.ENABLE.WARNONLY - Enables PKA Key Management Extension in Warn
  - CSF.PKAEXTNS.ENABLE - Enables PKA Key Management Extension in Fail
  - CSF.SSM.ENABLE - Equivalent to coding Special Secure Mode option SSM(YES)
  - CSF.XCSFKEY.ENABLE.AES - Enables Symmetric AES Key Label Export
  - CSF.XCSFKEY.ENABLE.DES - Enables Symmetric DES Key Label Export

© 2015 RSH Consulting, Inc. All Rights Reserved.

z/OS Unix

Control, activate, and manage z/OS Unix 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.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.UNLIMITED.OUTPUT Override default spooled output limits when spawning
- BPX.WLMSERVER Access to WLM functions (BPX1SIN, BPX1WLM)

© 2015 RSH Consulting, Inc. All Rights Reserved.

z/OS Unix

Resources - Control options

- BPX.DEFAULT.USER — Default uid / gid {Obsolete after z/OS 1.13}
- BPX.MAINCHECK — Requires loading MVS program marked MAIN
- BPX.NEXT.USER — Automatic uid / gid assignment
- BPX.PRIVPATHOK — Temporary problem determination aid - Security APAR OA43650
- BPX.SAFFASTPATH — Enable z/OS Unix to allow access without RACF calls - only HFS File Systems
- BPX.UNIQUE.USER — Automatic OMVS segment creation with unique uid / gid assignment

© 2015 RSH Consulting, Inc. All Rights Reserved.

DFSMS

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

- STGADMIN Resources - READ (EDG - UPDATE, CONTROL, & ALTER)

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

© 2015 RSH Consulting, Inc. All Rights Reserved.

DFSMS

- IGG.CATLOCK - READ - ICF Catalogs
- ICHBLP - READ - Bypass Tape Label Processing (+ UPDATE)
- ICHUNCAT.dsname - READ - CATDSNS - uncatalog dataset
- ICHUSERCAT - READ - CATDSNS - use private catalog
- IEC.TAPERING - READ - Bypass tape ring removal for read
- IHJ.CHKPT.volser - READ - Create checkpoints on shared DASD
- IDA.VSAMEXIT.*exitname* - READ - Invoke exit (Security APAR UA76704)

© 2015 RSH Consulting, Inc. All Rights Reserved.

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*[.*ssid*] - If defined, controls use of function
  - *prefix.group.function-set*[.*ssid*]
    - 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 | IMS (* - requires SEC=YES in FNMnPOPT)
    - Function-set: INPUT | OUTPUT | RDONLY | DUPLICATE | UPDATE | ALL - varies by Group

- If product is running APF-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 (for update) to associated DASDVOL *volser* profile

© 2015 RSH Consulting, Inc. All Rights Reserved.

DITTO & File Manager

- File Manager - SAF-controlled auditing
  - Uses RACROUTE REQUEST=AUTH,STATUS=ACCESS
  - *n* = 1 (FM/IMS), 2 (FM/DB2), 3 (FM/CICS)
  - Activate auditing - FACILITY Class
    - FILEM.PARMLIB.[BASE | IMS | DB2 | CICS] - READ - PARMLIB(FMN[0|*n*]PARM) governs logging - SAF_CTRL=NO | YES
    - FILEM.SAFAUDIT.[BASE | IMS | DB2 | CICS] - READ - SAF-controlled logging
    - Only checks .SAFAUDIT. if not authorized to .PARMLIB.
  - Control where SAF-controlled log records are written - FACILITY Class
    - FILEM.AUDIT[*n*][.*ims-ssid* | *db2-ssid*].OPTION - READ - Use "create audit trail" option
    - FILEM.AUDIT[*n*][.*ims-ssid* | *db2-ssid*].TOSMF - READ - Write audit records to SMF
    - FILEM.AUDIT[*n*][.*ims-ssid* | *db2-ssid*].TODSN
      - READ - Write audit records to user dataset
      - UPDATE - Use "demand logging' function
  - Control auditing of functions - XFACILIT class - READ
    - FILEM.AUDIT[3][.*cics-applid*].*function-code*.[ALL | UPDATE | FUNCTION].resource
      - Log every read or modify | modify | information
      - ALL and UPDATE log every individual dataset record read and/or modified
      - Websphere Queue names must be prefixed with MQ Queue Manager name
      - CICS resources other than files are named: [TS | TD][:*cicsapplid*]:*resource-name*
    - FILEM.AUDIT1.*ims-ssid*.*function-code.database* - Log use of function for specified database
      - CONTROL - Create audit trail in Edit function only if user selects 'Create audit trail' option
    - FILEM.AUDIT2.*db2-ssid*.*function-code*[.*resource-type*].*resource* - Log use of function for specified resource
      - CONTROL - Change auditing requirement for current resource name

© 2015 RSH Consulting, Inc. All Rights Reserved.

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]
    CSVDYNL.*linklstname*.TEST - READ
    CSVDYNL.UPDATE.LNKLST

© 2015 RSH Consulting, Inc. All Rights Reserved.

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.IOCDS - 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

© 2015 RSH Consulting, Inc. All Rights Reserved.

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 stream structures & remove, delete, and unregister resouces managers with RRS
  - 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 (current system only)
  - MVSADMIN.RRS.COMMANDS.*logging-group-name*.*sysname* - Resource Recovery Services (across Sysplex)
  - IXGZAWARE_CLIENT - UPDATE - Configure log stream to send data to zAware
  - IXLSTR.*structure-name* - Coupling facility structure
    - ALTER - Maintain structure
  - IXCARM.*elemtype*.*elemname* - ARM entity
    - UPDATE - Permit unauthorized program use of ARM

© 2015 RSH Consulting, Inc. All Rights Reserved.

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.MON2DATA.*exit-name* - Allow use of data reduction exit
  - ERBSDS.MON3DATA - Access Monitor III performance data
    - Not checked for access via LDAP, must disable RMF LDAP requests to protect
  - ERBSDS.MON3DATA.*exit-name* - Allow use of data reduction exit

- To allow use of the exits, the FACILITY class must be RACLISTed

© 2015 RSH Consulting, Inc. All Rights Reserved.

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

© 2015 RSH Consulting, Inc. All Rights Reserved.

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

© 2015 RSH Consulting, Inc. All Rights Reserved.

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

© 2015 RSH Consulting, Inc. All Rights Reserved.

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

© 2015 RSH Consulting, Inc. All Rights Reserved.

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 user only has EXECUTE authority
    - UPDATE - Dump any program unless there is a open dataset protected by PADS

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

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

© 2015 RSH Consulting, Inc. All Rights Reserved.

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

© 2015 RSH Consulting, Inc. All Rights Reserved.

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

© 2015 RSH Consulting, Inc. All Rights Reserved.

JES

- Verify a user is allowed to use a JOB CLASS

- Resources - option activation
  - JES.JOBCLASS.OWNER - If defined, authorization is checked for job owner
  - JES.JOBCLASS.SUBMITTER - If defined, authorization is checked for job submitter

- JESJOBS profiles determine what classes may be used

© 2015 RSH Consulting, Inc. All Rights Reserved.

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.DFHXCEIP
    - 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

© 2015 RSH Consulting, Inc. All Rights Reserved.

CICS

- 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

© 2015 RSH Consulting, Inc. All Rights Reserved.

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 - both …
    - BBSECURE parameter - ESMTYPE=NONE
    - BBMSS.ESMTYPE.NONE - UPDATE

© 2015 RSH Consulting, Inc. All Rights Reserved.

CICS

- CICSPlex System Manager (SM) Web User Interface (WUI)
  - Allow use of WUI functions (does not protect objects they manage - see SM security)
    - READ - Use views and menus in the main interface or export using transaction COVC
    - UPDATE - Create, update, or remove items in the View Editor or import using COVC
    - 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
  - Access the WUI User Editor (UPDATE) and manage WUI user group profiles
    - EYUWUI.*wui-server-applid*.USER - UPDATE

- CICS Batch Application Control
  - $CBK.*cics-applid*.[ADMIN | EXECUTE].*accessType.objectType.objectName*
    - READ - View objects
    - UPDATE - Create, update, and delete objects (ADMIN) or execute objects (EXECUTE)

© 2015 RSH Consulting, Inc. All Rights Reserved.

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

© 2015 RSH Consulting, Inc. All Rights Reserved.

CICS

- CICS Transaction Gateway (CTG)
  - CTG.RRMS.SERVICE
    - UPDATE - Allow CTG task ID to use Recoverable Resource Management Services (RRMS)
    - CONTROL - Permit refresh of CTGRRMS services
- CICS Deployment Assistant for z/OS
  - CPH.DISCOVER.MVS.*mvs-sysid* - READ - Permit server ID to invoke discovery

© 2015 RSH Consulting, Inc. All Rights Reserved.

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 Connect
  - HWS.ims_connect_name - UPDATE - Allow connection
- IMS Connect Extensions - XFACILIT class
  - CEX.IPV4.*icon-name.nnn.nnn.nnn.nnn.port#*
  - CEX.IPV6.*icon-name.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.port#*
    - READ - Control access to OTMA transaction or DRDA request based on client IP address
    - IP address nodes must be padded with leading zeros as required
- IMS Listener Service - Security Exit (sample)
  - TPI.IMSSOCK.trancode - READ - Access transaction via call to TPIAUTH
- IMS Command Control Facility (CCF)
  - CCF.*option* - READ - Update options or issue commands

© 2015 RSH Consulting, Inc. All Rights Reserved.

IMS

- IMS Queue Control Facility (QCF)
  - IQC.mvsid.imsid.function
    - READ - Perform Query and Browse
    - UPDATE - Perform Load, Unload, and Recover
- IMSplex Common Service Layer (CSL) Structured Call Interface (SCI)
  - CSL.imsplex_name - UPDATE - Register with SCI
- IMS Database Recovery Control (DBRC) facility
  - INIT.RECON command parameter CMDAUTH(SAF,*safhlq*) - activates authorization checking and defines the profile HLQ
  - *safhlq.command.modifier.qualifier* - READ - Execute command
- IMS Repository Server (RS)
  - SAF_CLASS parameter in FRPCFG member of the IMSPROCLIB dataset - Recommends XFACILT
  - Access Levels - READ | UPDATE | CONTROL | ALTER - Not clearly documented
  - FRPREP.CATALOG - Access catalog repository
  - FRPREP.*repository* - Access repository
  - FRPMEM.*repository.product.type.membername* - Access repository member
  - FRPAUD.*repository.product.type.*TYPE - Modify AUDIT levels

© 2015 RSH Consulting, Inc. All Rights Reserved.

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

© 2015 RSH Consulting, Inc. All Rights Reserved.

z/OS Health Checker

- Control who can initiate, print, and manage checks
- XFACILIT class
- 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_AIM_STAGE.*reqtype*
  - HZS.*sysname*.IBMRACF.RACF_CERTIFICATE_EXPIRATION.*reqtype*
  - HZS.*sysname*.IBMRACF.RACF_GRS_RLN.*reqtype*
  - HZS.*sysname*.IBMRACF.RACF_ICHAUTAB_NONLPA.*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*
  - HZS.*sysname*.IBMRACF.RACF_UNIX_ID.*reqtype*
  - HZS.*sysname*.IBMRACF.ZOSMIGV2R1_DEFAULT_UNIX_ID.*reqtype*

© 2015 RSH Consulting, Inc. All Rights Reserved.

IBM Tivoli Output Manager (ITOM) for z/OS

- Control who can view and manage reports
- Parameter library startup command member - BJT#IN03
  - SAF SET ID *saf-id* - Enables SAF security & specifies 1st qualifier on resource names
  - PROTVIEW SAF - Activate levels of view security
- *saf-id.stc-id*.MENU.MAIN - READ - Access ITOM
  - Access permitted (READ | UPDATE | CONTROL) sets default permission to undefined resources
  - If not defined to RACF, defaults to READ access
- *saf-id.stc-id*.MENU.VIEW - READ - Access View Menu
- *saf-id.stc-id*.MENU.ADMIN - UPDATE - Access Administrator Menu
  - ITOM User's Guide v2.1 and before erroneously list the MENU.ADMIN resource as also being named MENU.ADMN
- *saf-id.stc-id.resource-type*[.*resource-id*]
  - READ - View resource
  - UPDATE - View configuration options
  - CONTROL - Create, change, and delete resources and configuration options
- *saf-id.stc-id*.SECV
  - UPDATE - Bypass view restrictions (checked when PROTVIEW SAF)

© 2015 RSH Consulting, Inc. All Rights Reserved.

Fault Analyzer

- Control who can use Fault Analyzer to create dumps and access dump files
- XFACILIT class
- Access is checked using RACROUTE REQUEST=AUTH,STATUS=ACCESS
- Recovery Fault Recording (RFR)
  - IDI_SDUMP_ACCESS - ALTER - Create RFR SVC Dump (SDUMP)
  - IDIRFR_TDUMP_HLQ.*rfr-dsn* - ALTER - Create RFR Transaction Dump (TDUMP)
- History File Fault Dataset - permit access if dataset profile does not grant access
  - Profiles:
    - IDIHIST_GROUP_DSN.*current-connect-group.hist-dsn*
    - IDIHIST_USERID_DSN.*userid.hist-dsn*
  - Both profiles may be checked to see if user has sufficient access; _GROUP_ is checked first
  - Access levels:
    - READ - View saved report or perform re-analysis
    - UPDATE - Update user notes or create a new fault entry in the history file
    - ALTER - Delete entries
  - Manual suggests using GLOBAL entries with &RACUID and &RACGPID; however, such entries would be ignored due to use of STATUS=ACCESS unless the following profiles are created
    - IDIHIST_GROUP_DSN.*.** UACC(NONE)
    - IDIHIST_USERID_DSN.*.** UACC(NONE)

© 2015 RSH Consulting, Inc. All Rights Reserved.

Software Configuration Library Manager (SCLM)

- Control who can update, manage, and migrate software
- SAF functionality introduced by APAR OA26997 (?)
- XFACILIT class
- Activated by setting system variable &SCLMSEC to 'ACTIVE'
- SCLM.[SECDSN | SECSUB | SECSVC].OFF.*project.alternate*
  - UACC(READ) - Turns off specific security features
  - Requires SCLM module FLMSEC01 to be authorized
- SCLM.SECDBG.ON.*project.alternate* - READ - Display security debug information
- SCLM.DSN.*project.alternate.dsn*
  - UACC(READ) - Associates datasets with a project
- SCLM.SUB.*project.alternate.subproject.type*
  - Subprojects are defined using the FLMPROJ macro
  - READ - Display information
  - UPDATE - Modify project objects
  - ALTER - Move and overwrite project objects
- SCLM.SVC.*project.alternate.service*
  - READ - Use the process

© 2015 RSH Consulting, Inc. All Rights Reserved.

Rational Developer for System z

- Debug security
  - AQE.AUTHDEBUG.WRITEBUFFER - UPDATE - Debug read-only CICS transactions
- Class for FEK.-prefixed profiles
  - RSED configuration file - rsed.envvars - statement - _RSE_FEK_SAF_CLASS=*classname* - Default FACILITY
- Log file securty - MODIFY LOGS command
  - FEK.CMD.LOGS.AUDIT.*stc_name* - READ - Collect audit logs of RSED Started Task
  - FEK.CMD.LOGS.SERVER.*stc_name* - READ - Collect server logs of RSED Started Task
  - FEK.CMD.LOGS.USER.*userid* - READ - Collect user logs of USERID
  - FEK.CMD.LOGS.OWNER.*userid* - READ - Change from RSED Started Task ID to USERID
- Push-to-client configuration updates (version 8.0.3 and later) - Access denied if no profile
  - RSED configuration file - pushtoclient.properties - options activate checks
  - FEK.PTC.CONFIG.ENABLE.*sysname.devgroup* - READ - Client accepts configuration updates for group
  - FEK.PTC.PRODUCT.ENABLE.*sysname.devgroup* - READ - Client accepts product updates for group
  - FEK.PTC.REJECT.CONFIG.UPDATES.*sysname*[.*devgroup*] - READ - User can reject configuration updates
  - FEK.PTC.REJECT.PRODUCT.UPDATES.*sysname*[.*devgroup*] - READ - User can reject product updates
  - Client administrators require access to FEK.PTC._.ENABLE._- resources to define and manage push-to-client metadata

- Rational ClearCase - z/OS Extensions
  - BCC.REMOTE.BUILD.*role* - READ - Submit rccbuid command requests

© 2015 RSH Consulting, Inc. All Rights Reserved.

IBM - Miscellaneous

- 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 - as of 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

- 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

© 2015 RSH Consulting, Inc. All Rights Reserved.

IBM - Miscellaneous

- 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
  - [*dynmresnm-prefix*.]*applid* - READ - Application appears on dynamic menu
- 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
- IBM Tivoli Storage Productivity Center for Replication for System z
  - ANT.REPLICATIONMANAGER - CONTROL - Use various commands
  - Task needs to be restarted after profile is defined or changed

© 2015 RSH Consulting, Inc. All Rights Reserved.

IBM - Miscellaneous

- 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
- IBM 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
  - Access is denied unless explicitly permitted

© 2015 RSH Consulting, Inc. All Rights Reserved.

IBM - Miscellaneous

- 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)
- Hourglass (acquired from Princeton Softech)
  - HOURGLASS_CX_ADMIN - READ / UPDATE - View / Update control elements for all users
  - HOURGLASS_CX_USER - READ / UPDATE - View / Update control elements for own ID
  - HOURGLASS_CX_REFR - UPDATE - Initiate dynamic refresh via option 2 save/activate
- MVS - IOSCDR macro
  - IOSCDR - UPDATE - Retrieve I/O hardware information

© 2015 RSH Consulting, Inc. All Rights Reserved.

IBM - Miscellaneous

- Data Lookaside Facility (DLF)
  - COFXTAB
    - READ - List table of datasets & jobs eligible for Hiperbatch processing
    - UPDATE - Create or modify table entries using COFXUPDT

- BatchPipes
  - PSP.ASFPPIPE.*bpsubsystemname* - READ - Use BatchPipe Subsystem
  - PSP.ASFPPD.*bpsubsystemname* - READ - Use large BatchPipes - exceeding MAXBUFNO parameter
  - PSP.ASFPFIT.*bpsubsystemname* - READ - Use BatchPipeWorks Subsystem
  - PSP.ASFPAFIT.*bpsubsystemname* - READ - Use BatchPipeWorks Subsystem - Authorized users

- RACROUTE API on VM
  - ICHCONN
    - READ - Issue 'non-authorized' requests
    - UPDATE - Issue 'authorized' requests

- Common Information Model (CIM)
  - MRCLASS.CLUSTER - UPDATE - Allow use of CIM providers for the OS management Cluster classes

© 2015 RSH Consulting, Inc. All Rights Reserved.

IBM - Miscellaneous

- IBM Tivoli Directory Server
  - GLD.XCF.GROUP.*groupname* - READ - Allow LDAP to run in a Sysplex group - serverSysplexGroup name

- IBM Tivoli Asset Discovery for z/OS
  - TPARAM DD - Configuration parameter SECURITY=SYSTEM activates RACF authorization checking
  - TPARAM DD - HSISANP2 member parameter AUTH_HLQ defines the *safhlq* (example uses TADZ)
  - *safhlq*.DB.*database* - READ - View reports
  - *safhlq*.MENU.[ASSET | DISC | ADMIN | CUSTOM] - READ - Access menu

- Debug Tool for z/OS
  - EQADTOOL.AUTHDEBUG - READ - Debug programs in protected storage
  - EQADTOOL.BROWSE.[CICS | MVS]
    - READ - Use tool in browse-mode for either CICS regions or non-CICS jobs
    - UPDATE - Use tool in non-browse mode
  - EQADTOOL.DTCDDELETEALL - UPDATE - Use DTCD transaction to delete debug profiles
  - EQADTOOL.DTCIINACTALL - UPDATE - Use DTCI transaction to deactivate debug profiles
  - EQADTOOL.DTSTMODCICSK - UPDATE - Use DTST transaction to modify CICS-key storage
  - EQADTOOL.DTSTMODUSERK - UPDATE - Use DTST transaction to modify USER-key storage
  - EQADTOOL.DTCNCHNGEANY - UPDATE - Use DTCN tranaction to create, modify, or delete debug profiles

© 2015 RSH Consulting, Inc. All Rights Reserved.

IBM - Miscellaneous

- DB2 Query Monitor
  - Consolidation and Analysis Engine (CAE) role is determined by access to the following profiles
    - CQM.CAE.ADMINISTRATOR - UPDATE
    - CQM.CAE.OPERATOR - UPDATE
      - READ - Viewer
  - Query Monitor functions - READ
    - CQM.ACCESS.*qmid* - Access Query Monitor subsystem
    - CQM.ACTIVATE.*qmid.db2-ssid* - Activate monitoring
    - CQM.DEACTIVATE.*qmid.db2-ssid* - Deactivate monitoring
    - CQM.REFRESH.PROFILE.*db2-ssid* - Refresh monitoring profile
    - CQM.CHANGE.PROFILE.*db2-ssid* - Change monitoring profile
    - CQM.HOSTV.*qmid* - View host variable information
    - CQM.SQLTEST.*qmid* - View SQLTEST information

- IBM Tools Base for z/OS - IMS Tools Knowledge Base
  - SAF and Resource Class parameters in configuration dataset member FPQCONFG - FACILITY recommended
  - FPQREP.[CATALOG | HKT_REGISTRY | HKT_INPUT | HKT_O0000000 | BSN_SENSOR | IAV_AUTODIR]
    - READ - Use tool
    - UPDATE - Create, reorganize, and update repositories and add reports

- IBM Tivoli Allocation Optimizer for z/OS IBM User's Guide
  - GLO.ADMIN.*subsystem-id* - UPDATE - Perform update functions

© 2015 RSH Consulting, Inc. All Rights Reserved.

Adjunct RACF Administration Products

- IBM Security zSecure - default XFACILIT class {former Consul prefixes - FACILITY class}
  - CKF.*function* ($CNF) - Collect component of Admin, Audit, Visual, Compliance Insight
  - CKG.*function* ($CNG) - Admin
  - CKNADMIN.*keyword.node* - Command routing
  - CKNDSN.*dstype.node.system.dsname* - Command routing
  - CKNDSN.CKRCMD.*node.system*.CKRCMD - Command routing
  - CKNUMAP.*source-nodename.source-userid.target-nodename* - Command routing
  - CKR.*function* ($C2R) - Admin, Audit, Alert, Visual
  - C2P.*function* - Alerts
  - C2R.*function* ($C2R) - Visual
  - C2X.*function* ($C2X) - Exit Activator
  - C4R.*function* ($C4R) - Command Verifier
  - TOOLKIT.SVC - zToolkit's SVC
  - B8R.*keyword.function* ($B8R) - RACF Offline (option B8ROPT specifies class; XFACILIT is the default)
- Software Engineering of America - RACF Administrator 2
  - RA2.*function*
- Allen System Group - ASG-Admin for Security Server
  - DSM.*function*

© 2015 RSH Consulting, Inc. All Rights Reserved.

Adjunct RACF Administration Products

- Vanguard Integrity Professionals
  - VRA$.*function* - RACF Administrator
  - VRAADM$.*function* - RACF Administrator
  - VRAUD$.*class*[.*field*] - RACF Administrator
  - VRAPW$.*function* - RACF Administrator - password administration
  - VIP$.*function* - RACF Administrator
  - VSA$.*function* - RACF Analyzer
  - VSR$.*function* - RACF Advisor
  - VCL$.*function* - Vanguard Cleanup
  - VRO$.*function* - Vanguard Offline
  - EZRESET$.*function* - ezRESET
  - $RIO.*function* - Vanguard Security Center

- Betasystems - Beta 88 zSecurity Administrator
  - BETA.INIT.*subsystem-id*

© 2015 RSH Consulting, Inc. All Rights Reserved.

Third-Party Products - CA

- CA Disk Backup and Restore
  - SYSPARM - SMSTGAD*ddd* - 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
  - Default Options Table - FACILITY=*classname* - (new with v11.6) Default is FACILITY
  - XCOM.*applsec*.[IP | LU].*destname*.[SEND | RECEIVE].[L | R] - READ - Initiate transfer

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

- 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

© 2015 RSH Consulting, Inc. All Rights Reserved.

Third-Party Products - CA

- CA Workload Automation SE (a.k.a. CA 7)
  - SECURITY statement parameter EXTERNAL=AGENT - Activates control over agent job submission and command execution
  - SECURITY statement parameter AGCLASS=*classname* - Optional - Default is FACILITY
  - *ca7-instance-id*.AGENTUSR.*agent-userid.agent-name* - READ - Allows agent job submissions and command executions

- CA Workload Automation CA 7 Web Client
  - SYSIN DD - CA7SRVR Option - FACILITY=*class* - (default) FACILITY class
  - CA7SRVR.ACCESS - READ - Use web client
  - CA7SRVR.VIEW.GLOBAL - UPDATE - Change global views
  - CA7SRVR.COMMAND.GLOBAL - UPDATE - Change global command lists
  - CA7SRVR.PROFILE.*userid* - UPDATE - Delete information from user's CA7PROF dataset
  - CA7SRVR.CA7.GLOBAL - UPDATE - Change list of CA 7 instances

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

© 2015 RSH Consulting, Inc. All Rights Reserved.

Third-Party Products - CA

- 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
  - VKGPARMS DD parameters - TAPADMIN(*tapeauthname*) - no default
  - *tapeauthname* - READ - Perform any action against tape datasets

- CA TRILOGexpert TriTune
  - TUNSSP00 parameter - SECCLASS=*classname* - default FACILITY
  - TUNSSP00 parameter - SECPREFX=*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

- CA Mainframe Application Tuner
  - TUNSSP00 parameter - SECCLASS=*classname* - default FACILITY
  - TUNSSP00 parameter - SECPREFX=*profile-prefix* - default CAMAT
  - TUNSSP00 parameter - SERVERID=*servername*
  - *profile-prefix.servername.function*[.*resource*] - READ - Perform function on target resource

© 2015 RSH Consulting, Inc. All Rights Reserved.

Third-Party Products - CA

- CA CMDB Connector for z/OS (CMDB - Configuration Management Database)
  - PARMLIB(SXPMD0*i*) defines the resource names
  - CONNECTR.CMDBADM - READ - Administer the product
  - CONNECTR.CMDBUSER - READ - Discover and export Configuration Items (CIs)

- CA Database Configuration Manager for IMS for z/OS (a.k.a., Mainframe Configuration Manager)
  - CFM.SETUP - READ - View authorization profiles

- CA Database Management Solutions for IMS for z/OS
  - CA Mainframe Extended Terminal Manager for IMS for z/OS - Enhanced Transaction Verification (ETV)
    - Uses IMS' Command Authorization exit (DFSCCMD0)
    - Protects Transaction/LTERM authorization and Transaction/password authorization previously secured by Security Maintenance Utility (SMU)
    - SAF ETV parameters
      - SAFPREFIX=*prefix* - sets first qualifier of the resource name
      - TRANLTRM - Activates SAF call to perform ETV processing for Transaction/LTERM names.
      - TRANPSWD - Activates SAF call to perform ETV processing for Transaction/PASSWORD n
    - *prefix*.LTRM.*ims-transaction-code.lterm-name* - READ - Execute transaction from this LTERM
    - *prefix*.PSWD.*ims-transaction-code.password* - READ - Execute transaction specifying this password

© 2015 RSH Consulting, Inc. All Rights Reserved.

Third-Party Products - CA

- 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
    - NETMSTR.PKTTRACE.*region* - READ - access SmartTrace
  - $RMSXSAF member - NeTwork Partitionaing Facility (NPF) resource list - User ID Access Maintenance System (UAMS) record
    - $RMMENU.*menu-id.option-code* - READ - Access menus
    - $RMDB.*system-image.system-version.class-number.definition-name.action-type* - READ - Access Knowledge Base
    - $RMCMD.*system-image.system-version.class-number.component-hame.command* - READ - Access Automation Services command
    - $RMSYCMD.*system-command.operand1.operand2...* - READ - Access system command
    - $RMNMCMD.*product-command* - READ - Access product command
    - $RMICS.*action.parameter-group-name* - READ - Access Customizer Prameter Groups

- CA OPS/MVS
  - Parameter EXTSECURITY=YES activates external security
  - Parameter EXTSECLASS=*classname* - default FACILITY
  - Parameter EXTSECPREFIX=*profile-prefix* - default OP$MVS
  - *profile-prefix.function*
    - READ - Perform list functions
    - UPDATE - Perform activate, deactivate, start, stop functions

© 2015 RSH Consulting, Inc. All Rights Reserved.

Third-Party Products - BMC

- 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

© 2015 RSH Consulting, Inc. All Rights Reserved.

Third-Party Products - BMC

- 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

© 2015 RSH Consulting, Inc. All Rights Reserved.

Third-Party Products - BMC

- 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

© 2015 RSH Consulting, Inc. All Rights Reserved.

Third-Party Products - RocketSoftware

- RocketSoftware - MVS Extended Information (MXI)
  - MXICMD.*function*
- RocketSoftware - Mainstar Catalog RecoveryPlus (CR+)
  - MAINSTAR.CR+.*function* - READ - Perform function
- RocketSoftware - Database Backup and Recovery for DB2 on z/OS
  - DBR.ACCESS.*db2-subsystem-id* - READ - Use DBR with DB2 subsystem
- RocketSoftware - Database Backup and Recovery for IMS
  - RIS.ACCESS.*ims-subsystem-id-or-group* - READ - Use DBR with IMS subsystem

© 2015 RSH Consulting, Inc. All Rights Reserved.

Third-Party Products - RocketSoftware

- RocketSoftware - Mainstar ASAP {Obsolete - Replaced by Backup and Recovery Manager}
  - MAINSTAR.ASAP.RACF.ON - Activates RACF Protection & READ- Permits access to BRM
  - MAINSTAR.ASAP.FILTER.*filter* - UPDATE - Use of filters UNIV and GLOBAL
  - MAINSTAR.ASAP.APPL.*applname* - UPDATE - Access to ASAP application records
  - MAINSTAR.ASAP.RSP.OPERCMDS.MONITOR - READ - Issue RSP commands

- RocketSoftware - Backup and Recovery Manager Suite (Formerly Mainstar ASAP)
  - BRM.ACD.RACF.ON - Activates RACF Protection & READ- Permits access to BRM
  - BRM.ACD.FILTER.*filter* - UPDATE - Use of filters UNIV and GLOBAL
  - BRM.ACD.APPL.*applname* - UPDATE - Access to ASAP application records
  - BRM.ACD.RSP.OPERCMDS.MONITOR - READ - Issue RSP commands
  - MAINSTAR.BRM.CATSCRUB - READ - Use Catalog Scrub command

© 2015 RSH Consulting, Inc. All Rights Reserved.

Third-Party Products - EMC

- EMC - Mainframe Enablers - Product Suite
  - EMC.ADMIN.CMD.*command* - XFACILIT - UPDATE - Execute ResourcePak Base commands
  - EMC.ADMIN.CMD.AUTOSWAP - XFACILIT
    - READ - Display AutoSwap information
    - UPDATE - Perform AutoSwap management functions
  - EMC.ADMIN.CMD.EMCSNAP.*cmd*[.*option*] - XFACILIT - READ - Execute TimeFinder/Clone Snap Facility command
  - EMC.ADMIN.CMD.QOS-[SPC | DCP] - XFACILIT - READ - Use Quality of Service utility functions
  - EMC.ADMIN.GROUP.EMCSNAP.*grpname* - XFACILIT
    - READ - Use TimeFinder/Clone Snap Facility group
    - UPDATE - Create/Delete TimeFinder/Clone Snap Facility group
  - EMC.ADMIN.POOL.EMCSNAP.*poolname* - XFACILIT
    - READ - Use TimeFinder/Clone Snap Facility pool
    - UPDATE - Use TimeFinder/Clone Snap Facility CONFIGPOOL commands
  - EMC.ADMIN.SCF.CTRL.*name* - XFACILIT - UPDATE - Assign a name to an EMC controller
  - EMC.ADMIN.CMD.TF.*command* - XFACILIT
    - READ - Query TimeFinder/Mirror information
    - UPDATE - Execute TimeFinder/Mirror management commands
  - EMC.CG.API.ADDDEL - FACILITY - UPDATE - Add/Delete Consistency Groups devices
  - EMC.CG.API.TRIP - FACILITY - UPDATE - Envoke Consistency Groups program ECGTRIP
  - EMC.DEVC.*12digitserialnumber.ssid.dev#* - XFACILIT
    - READ - Clone from device using TimeFinder/Clone Snap Facility
    - UPDATE - Clone to device using TimeFinder/Clone Snap Facility
  - EMC.UTL.ECGUTIL - FACILITY - UPDATE - Run Consistency Groups CLEAN utility

© 2015 RSH Consulting, Inc. All Rights Reserved.

Third-Party Products - EMC

- EMC - z/OS Storage Manager
  - Parameters
    - SECURITY_LEVEL - WARN | FULL activates authorization checking; WARN is test
    - SECURITY_NORULE - ALLOW | FAIL - determines action if no profile (RC=4)
  - EMC.EZSM.*plug-in_ID.transaction_class.opcode_name*
    - READ - Transaction class REPORT
    - UPDATE - Transaction class CNFGUPDT, DATAUPDT
    - ALTER - Transaction class SYSCMD

© 2015 RSH Consulting, Inc. All Rights Reserved.

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

© 2015 RSH Consulting, Inc. All Rights Reserved.

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
    - FDRERASE.*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)

© 2015 RSH Consulting, Inc. All Rights Reserved.

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

© 2015 RSH Consulting, Inc. All Rights Reserved.

Third-Party Products

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

© 2015 RSH Consulting, Inc. All Rights Reserved.

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
- 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

© 2015 RSH Consulting, Inc. All Rights Reserved.

Third-Party Products

- Teradata - Teradata Director Program
  - TDP*id*.*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)

© 2015 RSH Consulting, Inc. All Rights Reserved.

Third-Party Products

- Syncsort (Williams Data Systems) - Zen IP Monitor
  - IMPLEX.*stackname* - READ - Allow monitoring of IP stack

- Syncsort (Williams Data Systems) - Zen Trace & Solve - Exigence (ZTS)
  - WDS.ZEN.ADMIN
  - WDS.ZEN.COMMAND.MVS.*command*
  - WDS.ZEN.COMMAND.VTAM.*command*
  - WDS.ZEN.COMMAND.USS.*command*
  - WDS.ZEN.COMMAND.ZEN.*command*
  - WDS.ZEN.MASTER
  - WDS.ZEN.MVSCMD
  - WDS_EXIA
    - UPDATE Product Administration
    - READ Trace delete commands and all VIT functions
  - WDS_EXIN
    - ALTER Trace define, redefine, start, strop, import, export
    - CONTROL Trace browse, view, status, summary
    - UPDATE Terminal characteristics and Audit log display
    - READ Explain function
  - Permission to either WDS_EXIA or WDS_EXIN is required to access the product

© 2015 RSH Consulting, Inc. All Rights Reserved.

Third-Party Products

- TIBCO - Managed File Transfer Platform Server
  - Parameters
    - BOSSID=[*bos-prefix* | ANY | blank] - ANY or blank deactivate security (sample prefix $FUSION)
    - CCC_*function*_FACILITY=[*ccc-resource-name* | $CCC.*function*] - FUNCTIONs - BROWSE, ALTER, ADMIN, TRANSFER
    - EXTENDED_SECURITY_RESOURCE=[*ex-prefix* | $CFUSION]
    - EXTENDED_SECURITY_CHECK=(ENFORCE | WARN | NO , ENFORCE | WARN | NO) - check authority to (server,node)
  - *bos-prefix*
    - READ - ISPF/REXX Administrator
    - CONTROL - Profile Administrator
  - *bos-prefix*.READ
    - Access only checked if no access to *prefix* resource
    - READ - View all transfers and update transfers where local ID matches user's ID
  - *ccc-resource-name*
    - READ - Perform function
  - *ex-prefix*.TRANSFER.AUTH.[TSO | BATCH]
    - Checked if first EXTENDED_SECURITY_CHECK parameter is set to ENFORCE or WARN
    - READ - Perform transfer
  - *ex-prefix.*TRANSFER.*nodename*.INIT.[SEND | RECEIVE]
    - Checked if second EXTENDED_SECURITY_CHECK parameter is set to ENFORCE or WARN
    - READ - Perform transfer to specified node
  - *ex-prefix.*TRANSFER.IPADDR.INIT.[SEND | RECEIVE]
    - READ - Perform transfer to an IP address or IP name

© 2015 RSH Consulting, Inc. All Rights Reserved.

Third-Party Products

- Informatica - PowerExchange
  - DBMOVER configuration file statements
    - SECURITY=([0 | 1 | 2],[N | Y]) - '2' activates logon and authorization checking
    - DM_SUBTASK=[N | Y] - 'Y' activates DATAMAP access checks
    - DM_RESOURCE=*res-suffix* - Default is DATASET
    - RACF_CLASS=*classname* - Default is FACILITY
  - DTL.DATAMAP.*res-suffix*
    - READ - Allows users to read data maps
    - UPDATE - Allows users to define, delete, and modify data maps
  - DTL. TASKCTRL.[DISPLAY| STOPTASK] - READ - Execute related command
  - DTL.DBWRITE.ADABAS.DB*dbid*.FN*file_num* - UPDATE - Write data to ADABAS file
  - DTL.DBREAD.DATACOM.D*database_id.short_table_name* - READ - Read from Datacom table
  - DTL.DBWRITE.IMS[.*ims_id*] - UPDATE - Access IMS database via DL/1 batch or ODBA
  - DTL.CMD.[LISTENER | CONDENSE].*service_name.command_name* - READ - Run pwxcmd commands
  - CAPX.REG.*dbtype.dbid.registration_name*
    - READ - View capture registrations
    - UPDATE - Add, edit, and delete capture registrations abd extraction maps
  - CAPX.CND.*dbid.extraction_map_name* - READ - Extract change data

- Hitachi Data Systems - Business Continuity Manager
  - STGADMIN.YKA.BCM.COMMANDS - READ - Use control-type commands
  - STGADMIN.YKA.BCM.YKQUERY - READ - Use query-type commands

© 2015 RSH Consulting, Inc. All Rights Reserved.

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

© 2015 RSH Consulting, Inc. All Rights Reserved.

Third-Party Products

- Attachmate - Verastream Bridge Integrator
  - Provide sample CICS code for performing application access checks
  - Code parameter - RESCLASS=*classname* - Default FACILITY
  - $ATTMBR.cics-region-applid.3270-bridge-netnam.3270-bridge-term-id.3270-tran-id - READ - Execute tran

- CCOM - Virtual File Store (VPS) for OS/390 {No longer in business; product defunct)
  - VTS.ADMIN.*ispf-function*
    - READ - Perform functions 1 and 2 on main menu
    - UPDATE - Perform all functions
  - Administrative IDs must also be specified in the AdminID*nn* configuration parameters

- StorageTeck - StorageTek Tape Analytics (STA)
  - SMC.ROLE.STORAGETAPEANALYTICSUSER - READ - Assume StorageTapeAnalyticsUser role

- Sun Oracle - Extended High Performance Data Mover (ExHPDM)
  - Startup Parameter File - SAF(CLASS(*classname*)) - Default FACILITY
  - SOV.STREAM.*stream_name* - READ - Access to specified stream
  - SOV.CLASS.*stream_class_name* - READ - Access to specified stream class

© 2015 RSH Consulting, Inc. All Rights Reserved.

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}

© 2015 RSH Consulting, Inc. All Rights Reserved.

Freeware Programs

- IND$FILE Wrapper (Xephon RACF Update - August 2004)
  - IND$FILE.[GET | PUT].*dsname* - READ - Transfer file
- List SETROPTS Options (Xephon RACF Update - August 1998)
  - JEDSP.SETROPTS - READ - List options
- SETPW - CBT Tape (SETPW2)
  - RACFPW.CHANGES - READ - Reset passwords for other users
- NODSI - CBT Tape
  - NODSI - READ - Manipulate ENQed datasets
- ZDOSU - github
  - ZDEVOPS.AUTH.* - READ - Temporarily activate OPERATIONS and SPECIAL

© 2015 RSH Consulting, Inc. All Rights Reserved.

Researching - Contact RSH to Assist

- 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)
- STARTOOL (Serena - Startool IOO and FDM)
- TSSO
- LARGEREG
- $TM.[ACH | AUTO | CERT | DBA | PTCL].USER
- CRPTNB01 (nuBridges Protect / Encryption?)
- SARA (SAR - obsolete? - now CA-View)

© 2015 RSH Consulting, Inc. All Rights Reserved.

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
- GC27-3622 - Debug Tool for z/OS 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
- SA22-7521 - z/OS ICSF Administrator's Guide
- 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

© 2015 RSH Consulting, Inc. All Rights Reserved.

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
- SC19-1238 - File Manager for z/OS Customization Guide
- SC19-3011 - IMS Commands, Volume 3: IMS Component and z/OS Commands
- SC19-3020 - IMS System Administration
- SC19-3632 - IMS Connect Extensions for z/OS User's Guide
- SC19-4370 - IBM Tools Base for zOS - Configuration Guide for IMS
- SA23-1399 - z/OS MVS Setting Up a Sysplex

© 2015 RSH Consulting, Inc. All Rights Reserved.

References

- SC23-5191 - IBM Tivoli Directory Server Administration and Use for z/OS
- 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
- 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
- SC27-4049 - IBM Tivoli Storage Productivity Center Messages Guide
- SC27-4072 - IBM Tivoli Output Manager for z/OS Administrator's Guide
- SC27-4091 - IBM Tivoli Storage Productivity Center for Replication for System z Installation and Configuration Guide
- SC31-7186 - IBM TCP/IP for MVS IMS TCP/IP Application Development Guide and Reference
- SC32-9127 - IBM Tivoli Allocation Optimizer for z/OS IBM User's Guide
- 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
- SC33-7998 - z/OS Common Information Model User's Guide
- SC34-2571 - Tivoli System Automation for z/OS Planning and Installation
- SC34-4817 - Software Configuration and Library Manager (SCLM) Guide and Reference

© 2015 RSH Consulting, Inc. All Rights Reserved.

References

- 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
- SC34-6321 - CICS Batch Application Control for z/OS User's Guide
- SC34-6693 - Session Manager for z/OS Technical Reference
- SC34-7220 - CICS Transaction Gateway z/OS Administration
- SC35-0418 - z/OS DFSMShsm Implementation and Customization Guide
- SC35-0421 - z/OS DFSMShsm Storage Administration Guide
- 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
- SG24-7779 - Batch Modernization on z/OS
- SG24-8181 Key Management Deployment Guide: Using the IBM Enterprise Key Management Foundation
- SH19-4502 - NetView Access Services Customization

- REDP-4460 - IBM Redpaper Synchronizing IBM RACF Data by using IBM Tivoli Directory Integrator
- 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
- IBM Tivoli Asset Discovery for z/OS Reporting Guide

© 2015 RSH Consulting, Inc. All Rights Reserved.