Security zSecure
Version 2.1.0

Quick Reference

SC27-5646-00

Security zSecure
Version 2.1.0

Quick Reference

SC27-5646-00

Note
Before using this information and the product it supports, read the information in "Notices" on page 113.

This edition applies to version 2, release 1 of IBM Security zSecure Admin (product number 5655-N16), IBM Security zSecure Audit (product number 5655-N17), IBM Security zSecure Alert (product number 5655-N21), IBM Security zSecure Command Verifier (product number 5655-N19), IBM Tivoli Compliance Insight Manager Enabler for z/OS (product number 5655-N22), and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this publication

This guide summarizes the commands and parameters that are detailed in the IBM Security zSecure™ documentation set. This book is for quick reference only. For complete information, see the appropriate manual.

Intended audience

The target audience for this book includes security administrators and mainframe system programmers. Readers of this book should have a working knowledge of RACF® or ACF2 systems administration and be comfortable using the Interactive System Productivity Facility (ISPF).

What this publication contains

This publication contains the summary of commands and parameters are for the following manuals, which describe the commands in detail and provide information about how to use them:

- *IBM Security zSecure Admin and Audit for RACF User Reference Manual*, LC27-5639
- *IBM Security zSecure Audit for ACF2 User Reference Manual*, LC27-5640
- *IBM Security zSecure Audit for Top Secret User Reference Manual*, LC27-5641
- *IBM Security zSecure Alert User Reference Manual*, SC27-5642
- *IBM Security zSecure Command Verifier User Guide*, SC27-5648
- *IBM Security zSecure CARLa-Driven Components Installation and Deployment Guide*, SC27-5638

Access to publications and terminology

This section provides:

- A list of publications in the "IBM Security zSecure library."
- Links to "Online publications" on page viii.
- A link to the "IBM Terminology website" on page viii.

IBM® Security zSecure library

The following documents are available online in the IBM Security zSecure library:

- *IBM Security zSecure Release information*

  For each product release, the release information topics provide information about new features and enhancements, incompatibility warnings, and documentation update information for the IBM Security zSecure products. You can obtain the most current version of the release information at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.htm.
- *IBM Security zSecure CARLa-Driven Components Installation and Deployment Guide*, SC27-5638

  Provides information about installing and configuring the following IBM Security zSecure components:
  - IBM Security zSecure Admin
  - IBM Security zSecure Audit for RACF, CA-ACF2, and CA-Top Secret

  - IBM Security zSecure Alert for RACF and ACF2
  - IBM Security zSecure Visual for RACF
  - IBM Tivoli® Compliance Insight Manager Enabler for z/OS®
- *IBM Security zSecure Admin and Audit for RACF Getting Started*, GI13-2324

  Provides a hands-on guide introducing IBM Security zSecure Admin and IBM Security zSecure Audit product features and user instructions for performing standard tasks and procedures. This manual is intended to help new users develop both a working knowledge of the basic IBM Security zSecure Admin and Audit for RACF system functionality and the ability to explore the other product features that are available.
- *IBM Security zSecure Admin and Audit for RACF User Reference Manual*, LC27-5639

  Describes the product features for IBM Security zSecure Admin and IBM Security zSecure Audit. Includes user instructions to run the features from ISPF panels, RACF administration and audit user documentation with both general and advanced user reference material for the CARLa command language and the SELECT/LIST fields. This manual also provides troubleshooting resources and instructions for installing the zSecure Collect for z/OS component. This publication is only available to licensed users.
- *IBM Security zSecure Audit for ACF2 Getting Started*, GI13-2325

  Describes the IBM Security zSecure Audit for ACF2 product features and provides user instructions for performing standard tasks and procedures such as analyzing Logon IDs, Rules, and Global System Options, and running reports. The manual also includes a list of common terms for those not familiar with ACF2 terminology.
- *IBM Security zSecure Audit for ACF2 User Reference Manual*, LC27-5640

  Explains how to use IBM Security zSecure Audit for ACF2 for mainframe security and monitoring. For new users, the guide provides an overview and conceptual information about using ACF2 and accessing functionality from the ISPF panels. For advanced users, the manual provides detailed reference information including message and return code lists, troubleshooting tips, information about using zSecure Collect for z/OS, and details about user interface setup. This publication is only available to licensed users.
- *IBM Security zSecure Audit for Top Secret User Reference Manual*, LC27-5641

  Describes the IBM Security zSecure Audit for Top Secret product features and provides user instructions for performing standard tasks and procedures.
- *IBM Security zSecure Alert User Reference Manual*, SC27-5642

  Explains how to configure, use, and troubleshoot IBM Security zSecure Alert, a real-time monitor for z/OS systems protected with the Security Server (RACF) or CA-ACF2.
- *IBM Security zSecure Command Verifier User Guide*, SC27-5648

  Explains how to install and use IBM Security zSecure Command Verifier to protect RACF mainframe security by enforcing RACF policies as RACF commands are entered.
- *IBM Security zSecure CICS Toolkit User Guide*, SC27-5649

  Explains how to install and use IBM Security zSecure CICS® Toolkit to provide RACF administration capabilities from the CICS environment.
- *IBM Security zSecure Messages Guide*, SC27-5643

  Provides a message reference for all IBM Security zSecure components. This guide describes the message types associated with each product or feature, and lists all IBM Security zSecure product messages and errors along with their

severity levels sorted by message type. This guide also provides an explanation and any additional support information for each message.

- *IBM Security zSecure Quick Reference*, SC27-5646

  This booklet summarizes the commands and parameters for the following IBM Security zSecure Suite components: Admin, Audit, Alert, Collect, and Command Verifier. Obsolete commands are omitted.

- *IBM Security zSecure Visual Client Manual*, SC27-5647

  Explains how to set up and use the IBM Security zSecure Visual Client to perform RACF administrative tasks from the Windows-based GUI.

- *IBM Security zSecure Documentation CD*, LCD7-5373

  Supplies the IBM Security zSecure documentation, which contains the licensed and unlicensed product documentation. The *IBM Security zSecure: Documentation CD* is only available to licensed users.

- *Program Directory: IBM Security zSecure CARLa-Driven Components*, GI13-2277

  This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of IBM Security zSecure CARLa-Driven Components: Admin, Audit, Visual, Alert, and the IBM Tivoli Compliance Insight Manager Enabler for z/OS. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure documentation website at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html.

- *Program Directory: IBM Security zSecure CICS Toolkit*, GI13-2282

  This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of IBM Security zSecure CICS Toolkit. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure documentation website at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html.

- *Program Directory: IBM Security zSecure Command Verifier*, GI13-2284

  This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of IBM Security zSecure Command Verifier. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure documentation website at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html.

- *Program Directory: IBM Security zSecure Admin RACF-Offline*, GI13-2278

  This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of the IBM Security zSecure Admin RACF-Offline component of IBM Security zSecure Admin. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure documentation website at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html.

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security zSecure library
The product documentation site (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html) displays the welcome page and navigation for the library.

IBM Security Systems Documentation Central
IBM Security Systems Documentation Central provides an alphabetical list of all IBM Security Systems product libraries and links to the online documentation for specific versions of each product.

IBM Publications Center
The IBM Publications Center site (http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss) offers customized search functions to help you find all the IBM publications you need.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

Related documentation

If you are using IBM Security zSecure products in a RACF environment, you can find RACF user and reference information in several IBM manuals. The RACF commands and the implications of the various keywords can be found in the *RACF Command Language Reference* and the *RACF Security Administrator's Guide*. Information about writing other RACF exits can be found in the *RACF System Programmer's Guide*. Information about auditing RACF can be found in the *RACF Auditor's Guide*. You can access this documentation from the z/OS internet library available at http://www.ibm.com/systems/z/os/zos/bkserv/.

For information about incompatibilities, see the **Incompatibility** section under **Release Information** on the IBM Security zSecure documentation website at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html.

Table 1. Further information about RACF administration, auditing, programming, and commands

Manual	Order Number
z/OS V1 Security Server RACF Command Language Reference	SA22-7687
z/OS V1 Security Server RACF System Administrator's Guide	SA22-7683
z/OS V1 Security Server RACF Auditor's Guide	SA22-7684
z/OS V1 Security Server RACF System Programmer's Guide	SA22-7681
z/OS MVS™ System Commands	SA22-7627

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical training

For technical training information, see the following IBM Education website at http://www.ibm.com/software/tivoli/education.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. Introduction

This guide summarizes the commands and parameters that are detailed in the IBM Security zSecure documentation set. This book is for quick reference only. For complete information, see the appropriate manual.

General information

The summary of commands and parameters are for the following manuals, which describe the commands in detail and provide information about how to use them.

Note: Obsolete commands have been omitted.

- *IBM Security zSecure Admin and Audit for RACF User Reference Manual Version 2.1.0*
- *IBM Security zSecure Audit for ACF2 User Reference Manual Version 2.1.0*
- *IBM Security zSecure Audit for Top Secret User Reference Manual Version 2.1.0*
- *IBM Security zSecure Alert User Reference Manual Version 2.1.0*
- *IBM Security zSecure Command Verifier User Guide Version 2.1.0*
- *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide Version 2.1.0*

Command description

The commands that are described in this guide use the following conventions:

BOLD CAPS
: Name of a command.

italics Name of a variable.

UNDERLINED
: Default value.

Regular text (or CAPS only)
: Name of a keyword.

[ ] Optional.

{ } You must choose one of the enclosed terms.

| Choose only one of the separated terms.

***** The preceding command can be repeated more than once.

... The preceding value can be repeated more than once.

Chapter 2. ISPF commands

zSecure users can enter primary commands at the command prompt (===>) on panels.

Commands valid on repeat group display panels

The panels display `acl`, `unix_acl`, `unix_default_acl`, `unix_fdefault_acl`, `acf2_acl`, `connects`, `db2_acl`, `racf_db2_acl`.

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command
■	■	■	■	**ACL**
■	■	■	■	[EFFECTIVE]
■	■	■	■	[EXPLODE]
■	■	■	■	[NORMAL]
■	■	■	■	[ORIGIN | NOORIGIN]
■	■	■	■	[RESOLVE]
■	■			[SCOPE | NOSCOPE]
■	■	■	■	[SORT { ID | USER | ACCESS }]
■	■			[UNIVERSAL | NOUNIVERSAL]
■	■	■		[TRUST]

Commands valid on record level and repeat group display panels

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command
■	■	■	■	**FIND** { *value* | '*value*' | "*value*" | '*value*'C | "*value*"C } [*begincolumn* [*endcolumn*]] [FIRST | PREVIOUS | LAST | NEXT] [ASIS | CAPS]
■	■	■		**FORALL** *command*
■				**MODIFY** [ON | OFF]
■	■	■	■	**PRT**
■	■	■	■	**REFRESH**
■	■	■	■	**RFIND**
■	■	■	■	**SET**
■	■	■	■	**SORT** [[column | 'column header' | "column header"] [A | D]]*

Commands valid anywhere

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command
■				**ACCESS**
		■		**ACF2**
■	■	■	■	**CHANGES**
■	■	■	■	**CKXDEBUG**
■	■	■	■	**C2RIMENU**
■	■	■	■	**HELP**
■	■	■	■	**MSG** [msgid]
■	■			**RACF**
■	■	■	■	**RESET**

Commands valid on menus, not on profile, repeat group, SMF, and audit display panels

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command
■	■	■	■	**CARLA**
■	■	■		**CKNSERVE**
		■		**FDE**
■	■	■	■	**FIELDS**
■	■	■	■	**RESULTS**
■	■	■	■	**SETUP**
■	■	■	■	**STARTPAN**
■	■	■	■	**SYSPREV**
■	■	■	■	**SYSPRINT**
■	■			**TEMPLATE**

Chapter 3. CARLa Auditing and Reporting Language commands

zSecure users can use CARLa commands to create security administration and auditing reports with zSecure.

ALLOCATE (explicit allocation mode)

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	TYPE= { ACF2 | ACF2LID | ACF2RULE | ACF2INFO |
	■	■	■	SMF | SMFSTREAM |
	■	■	■	CKFREEZE | UNLOAD |
■	■			RACF |
■	■	■	■	CKRCMD | CKRTCMD | INPUT | OUTPUT | <*deftype*> }
■	■	■	■	[COMPLEX=*complex*] [VERSION=*version-identifier*]
■	■	■	■	[DD=*file*]
■	■	■	■	{ DSN=*dsn* | *dsn(mem)* [MOD | VOL=*volser* UNIT=*unit*] |
■	■	■	■	DSNPREF=*prefix* |
■	■	■	■	CMSFILE='*fn ft fm*' |
■	■	■	■	PATH='*pathname*' [FILEDATA=RECORD] [MOD] |
■	■	■	■	FILEDESC=n [PIPE={ Y | YES }] |
■	■	■	■	GETPROC=*procedure* |
■	■	■	■	ACTIVE |
■	■	■	■	[PRIMARY | BACKUP] [ACTIVE | INACTIVE] | SMF }
■	■	■	■	[DELETE]
■	■	■		[FUNCTION={ MAIN |
				BASE=*ddname*
■				MERGE }]
■	■	■	■	[NJENODE=*complex*]
■	■	■	■	[ZSECSYS=*system-name*] [ZSECNODE=*node-name*]
■	■			[RRSFNODE=complex]
■	■	■	■	[SUBSYS=(name [,exit [,parm1 [,parm2]]]])
■	■	■	■	[SVC99]

ALLOCATE (implicit allocation mode)

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[DDCKRCMD={ *file* | CKRCMD }]
■	■			[DDPFXDB={ *pfx* | CKRACF }]
■	■	■	■	[DDPFXSMF={ *pfx* | CKRSMF }]
■	■	■		[DDUNLIN={ *file* | CKRUNLIN }]

ALLOCATE (live allocation mode)

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[DATABASE | DB =(1,*n*,...)]
■	■			[PRIMARY | BACKUP]
■	■	■	■	[ACTIVE | INACTIVE]
■	■	■	■	[SMF]

ALLOCATE (global allocation mode)

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[CKRCMD_EXEC=[TSO | EX | REQ]]
■	■	■	■	[CLEANUP | NOCLEANUP]
■	■	■	■	[DDCARLA={ *file* | CKRCARLA }]
■	■	■	■	[DDCKR2PASS={ *file* | CKR2PASS }]
■	■	■	■	[DDCKRTSPRT={ *file* | CKXT@PRT }]
■	■	■	■	[DDUNLOUT={ *file* | CKRUNLOU }]
■	■	■	■	[ERRDD={ *file* | SYSTERM }]
■	■	■	■	[INDD={ *file* | SYSIN }]
■	■	■	■	[LETRAPON | LETRAPOFF | NOLE]
■	■	■	■	[NOBSAMBPAM]
■	■	■	■	[NOCLOSE]
■	■	■	■	[NODCBE]
■	■	■	■	[NODUMP]
■	■	■	■	[NOESTAE]
■	■	■	■	[OUTDD={ *file* | SYSPRINT }]
■	■	■	■	[STORAGEGC]
■	■	■	■	[TEXTPIPE=*n*]

BDAMQSAM

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			

BUNDLE

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[BUNDLEBY=*variablename*]
■	■	■	■	[BUNDLEMAILTO=*expression*[1]]

[1]Other operands as in **NEWLIST/OPTION** commands except for MAILTO, CC, BCC. See for a description of *expression* the **DEFINE** command; the field in the expression must be BUNDLEBY.

CAPS

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	

COMPAREOPT

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	TYPE=
■	■	■	■	NAME=
■	■	■	■	[BASE=]
■	■	■	■	[BY=]
■	■	■	■	[COMPARE=]
■	■	■	■	[SHOW=]

CONVERSION

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[TYPE=type] *conversionname*
■	■	■	■	REPLCHAR(*replacement*[2] [, *replacement*[2]] ...) ...

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[WHERE *clause*]

[2]*replacement* **::=**

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	({ QUAL*n* | LASTQUAL | SUBSTRING({ QUAL*n* | LASTQUAL } ,*startpos* [,*length* | :*endpos*]) } ,*char*)

COPY

Note: The order of the first two keywords on the copy command is fixed.

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■				{ PERMIT=*id* {TOUSER=*id2* | TOGROUP=*id2* | TOPERMIT=*id2*} | USER=*id* TOUSER=*id2* | GROUP=*id* TOGROUP=*id2* } [NEWDCEUUID='*new uuid*'] [NEWDATA='*new installation data*'] [NEWDFLTGRP='*group*'] [NEWKERBNAME='*new kerbname*'] [NEWNAME='*newname*'] [NEWOMVSGID='*new gid*'] { [NEWOMVSHOME='*new home directory*'] | [NEWOMVSPROGRAM='*new shell command*'] | NEWOMVSUID=*new uid*] } | NOOMVS [NEWOWNER=*owner*] [NEWPHRASE='*phrase*'] [NEWPASSWORD(*password*)] [NEWSNAME='*new sname*'] [NEWUNAME='*new uname*'] [FROMGROUP=*idlist*] [TOGROUP=*idlist*] [PROTECTED] [REVOKE] }

DEBUG

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[ABEND] [ACTION] [CPIC] [EMAIL] [FIELD] [GUARD] [INDEX] [LICENSE]
■	■	■	■	[PERFORM] [READALL] [RESTRICT] [SEGMENT] [SVC99]
■	■	■	■	[RESTRICT]

DEFAULT

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[COMPAREOPT_SHOW=(*list*)] [OWNER=*id*] [SYSTEM=*id*]

DEFINE

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[HELPPANEL=*helppanel*]
■	■	■	■	[TYPE=type] *varname* [(*modifiers*)]
■	■	■	■	{{MIN | MAX | AVG | SUM | CPRX} (field)
■	■	■	■	| {COUNT | SUMCOUNT | FREQ | BOOLEAN} [(*target variable*)]
■	■	■	■	| {COMPARE_RESULT | COMPARE_CHANGES}
■	■	■	■	| AS *expression*[1] | TRUE
■	■			| SUBSELECT({ACL(...) | CONNECTS(...) | CUSTOM_DATA(...) | USR(...)})}
■	■	■	■	[WHERE *clause*]

The resulting *varname* is a statistic if the MIN, MAX, AVG, SUM, CPRX, COUNT, SUMCOUNT, FREQ, or BOOLEAN keyword is used.

[1]***expression* ::=**

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	{{fieldname | *definename*[3] | :object_reference | basefieldname:id_or_deftype_reference } | CONVERT(*field*,*input-format*,*internal-format*) | EXTRACTDN(*field*,*level*) PARSE(*field*, [*start separator*][, *end separator*]) RACF_SECTION(*relsec*)[4] SMF_FIELD(*offset*,*length*)[4] SMF_SECTION(*triple*,*offset*,*length*)[4] SUBSTRING(*field*,*startpos*[,*length* | :*endpos*]) WORD(*field*,*number*[,*separator*])}
■	■	■		*object_reference* ::= {*targetfieldname*[5] | *type.targetfieldname*}[5]
■	■	■	■	*id_or_deftype_reference* ::= {*id_reference* | *deftype_reference*}
■	■	■		*id_reference* ::= {*targetfieldname* | *type.targetfieldname*}[6]
■	■	■		*deftype_reference* ::= *type.keyfieldname.targetfieldname*[7]
■	■	■	■	[3]*definename* cannot be a statistic)
■	■	■	■	[4]Only in type=SMF

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
		■		[5]For ACF2, *targetfieldname* can be only `NAME`, `NON-CNCL`, `READALL`, `RESTRICT`, `SECURITY`, or `STC`
■	■			[6]Currently, *type* can be only RACF
■	■	■	■	[7] *type* must be a DEFTYPE newlist

The following fields can be used in the subselect clause. Those fields followed by = need a comparison operator and a value. The special operators AND, OR, NOT, and parentheses can be used to clarify and define the logical relation between clauses.

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Fields
■	■	■	■	`ACL` `( ACCESS= GROUP= ID= USER= WHENCLASS= WHENPROF= )`

■	■			`CONNECTS`
				`( USER= GROUP= GRPADSP GRPAUD GRPAUTH GRPGRPACC GRPOPER`
				`GRPRESUMEDT= GRPREVOKE= GRPREVOKEDT= GRPSPEC GRPUACC )`

■	■	■	■	`CUSTOM_DATA` `(CSKEY= CSTYPE= CSVALUE= )`

■	■	■	■	`USR`
				`( CNGAUTHOR= CNGCHGDATE= CNGMULTI= CNGREQUEST=`
				`CNGSCHEDULE= CNGSTATUS= USRDATA= USRFLG= USRNM= )`

DEFTYPE

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Variables and keywords
■	■	■	■	`[ ABBREV2=`*`abbreviation`*` ] TYPE=<`*`deftype`*`>`
■	■	■	■	`[ DETAILHELPPANEL=`*`panel`*` ] [ HELPPANEL=`*`panel`*`]`
■	■	■	■	`[ NOWARN ]`

DISPLAY

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Variables and keywords
■	■	■	■	Command syntax identical to the **`SORTLIST`** command.

DSUMMARY

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Variables and keywords
■	■	■	■	Command syntax identical to the **SUMMARY** command

ENDBUNDLE

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	

ENDMERGE

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	

FILEOPTION

Also valid on **NEWLIST/OPTION**.

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[{ DD | DDNAME | FILE | F } =*ddname*] [CAPS] [COMPRESS=GZIP] [ENCODING= {EBCDIC | UTF-8}] [FILEFORMAT= {TEXT | XML}] [LINELEN=*value*] [MAXPAGE=*nn*] [NULLS | NONULLS] [OVERPRINT=*nn*] [PAGELEN=*nn* | NOPAGE] [PAGETEXT= { *'string'*| *"string"* | *`string`* | *:var* }] [SMTPCLASS=*sysoutclass*] [SMTPNJENODE=*nodename*] [SMTPWRITER=*name*] [SUBTITLE= { *'string'*| *"string"* | *`string`* | *:var* }] [TITLE= { *'string'*| *"string"* | *`string`* | *:var* }] [TOPTITLE= { *'string'*| *"string"* | *`string`* | *:var* }] [XML_DATADICT | NOXML_DATADICT] [XML_DTD | NOXML_DTD] [XML_STYLESHEET = { NO | URI ({ 'uri' | "uri" | `uri` }) | IMBED([DDNAME=*ddname*],[MEMBER=*member*]) }]

IMBED | INCLUDE

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[{ DDNAME | FILE } =*file*] [ESM=*list*] [FILEDESC=*number*] [ISPFVAR=*name*] [LICENSE=*list*] [MEMBER=*name*] [MARGINS=(*nn*,*ll*)] [NODUP] [NOLIST] [PATH='*pathname*']

LANGUAGE

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	*lan* [CCSID] [DBCS] [FORMAT name(('*builtin*', '*translation*') [,('*builtin* ', '*translation*')]...) TYPE *type* NEWLIST name | name.display FIELD name [:*occur*] PREFIXLEN=(x) STRING=('*CARLa_text*', '*translation*') SUBTITLE=('*CARLa_text*', '*translation*') TITLE=('*CARLa_text*', '*translation*') TOPTITLE=('*CARLa_ text*', '*translation*')

LIMIT

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[FOCUS=*focus* | (*focus*, *focus*,...) [SMF=*nn*] [SMFIN=*nnnnn*] [SMFDD=*nn*] [ABEND] [ID=*id*]* [IN=*nn*] [MSG=*nn*] [OUT=*nn*] [GENERIC | DISCRETE] [ID=*id*] [SMFIN= *n*] [INDEXBIAS={2 | *nn*}]

LIST

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	Command syntax identical to the **SORTLIST** command

MARGINS

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	MARGINS(*nn*,*mm*)

MENU

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	CFS= *panel*

MERGE

Command is terminated by **ENDMERGE**.

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■				[MERGE] *options*[1] [ENDMERGE]

[1]*options* **::=**

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■				[DEFINE] [INCLUDE | IMBED] [MERGERULE] [SELECT] [EXCLUDE]

MERGELIST

Must be followed by **NEWLIST** statements. Terminate with **ENDMERGE**.

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[NAME=*mergelistname*] [{ DD | DDNAME | FILE | F } =*ddname*]

MERGERULE

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■				{ DEFAULT { A CO CN D } ... | SOURCEID=(*id*...){ *options* }... | SOURCECLASS=(*class*...){ A D }... } options are: [AUTHORITY={ CURRENT | FLAG | LOW | HIGH | {SOURCE | MERGESOURCE} }] [{ CKGRACF | CNGRACF } ={YES | NO}] [CONNECT={ IFANY | IFBOTH | IFGROUP | IFUSER | NONE }] [DATA={ CURRENT | FLAG | {SOURCE | MERGESOURCE} }] [OWNER=*owner*] [RENAME=*name*] [SUPGROUP=*group*]

MOVE

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■				{ PERMIT=*id* | NOTIFY=*id* | USER=*id* [REVOKE] } [FROMGROUP=*idlist*] [TOGROUP=*idlist* [ALLPERMITS]] [NEWNOTIFY=*id*]

NEWLIST

See also **OPTION**.

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[ALLOWRESTRICT]
■	■	■	■	[CMD]
■	■	■	■	[COMPAREOPT=*compareopt*]
■	■	■	■	[DETAIL]
■	■	■	■	[ESM=*list*]
■	■	■	■	[ISPFTAB=*name*]
■	■	■	■	[LICENSE=*list*]
■	■	■	■	[NAME=*name*]
■	■	■	■	[NODUP]
■	■	■	■	[PROFLIST=*name* | NOTPROFLIST=*name*]
■	■	■	■	[RETAIN]
■	■	■	■	[SCOPE=*id*]
■	■	■	■	[SEGMENT=*segment*]
■	■	■	■	[SNMP]
	■	■	■	[SUPPRESS_IF_COMPARE | SUPPRESS_IF_COMPARE=HIDE | SUPPRESS_IF_COMPARE=SHOW]
■	■	■	■	[SYSLOG]
■	■	■	■	[TYPE=
		■		{ ACF2_CLASMAP | ACF2_FDE | ACF2_INFO | ACF2_INFOLINE |
		■		ACF2_INFORULE | ACF2_LID | ACF2_RULE |
		■		ACF2_RES_INFORULE | ACF2_RULELINE |
	■	■	■	AUDIT | CICS_PROGRAM | CICS_TRANSACTION |COMPLIANCE | CONSOLE |
	■	■	■	CSM | DASDVOL | DB2_DATABASE | DB2_JAR | DB2_PACKAGE | DB2_PLAN |
	■	■	■	DB2_ROUTINE | DB2_SEQUENCE | DB2_STOGROUP | DB2_TABLE |
	■	■	■	DB2_TABLESPACE |DSN | EXIT | IMS_PSB | IMS_TRANSACTION |
	■	■	■	IOAPP | IP_AUTOLOG | IP_INTERFACE | IP_FTP_REGION | IP_NETACCESS |
	■	■	■	IP_PORT | IP_RESOLVER | IP_ROUTE | IP_RULE | IP_STACK | IP_VIPA |

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	IP_TELNET_PORT | IP_TELNET_REGION | IP_VIPA |
	■	■	■	JOBCLASS | MEMBER | MOUNT | MSG | PC | PPT | SENSDSN |
	■	■	■	SMF | SMFOPT | SUBSYS | SVC | UNIX | VSM |
	■	■		TRUSTED |
■	■	■	■	CICS_REGION | CONCERN_TEXT | DB2_REGION | DEFTYPE | DYNEXIT |
■	■	■	■	FIELD | FIELD_OVERRIDE | IMS_REGION | NEWLIST | RESOURCE |
■	■	■	■	SYSTEM | UNIX | ZSECNODE |
■	■	■		REPORT_AC1 | REPORT_SENSITIVE | REPORT_STC |
■	■			AUTAB | CLASS | DSNT | RACF | REPORT_NONDEFAULT |
■	■			REPORT_OUTOFGROUP | REPORT_PADS | REPORT_PROFILE |
■	■			REPORT_REDUNDANCY | REPORT_SCOPE | ROUTER | RRNG | RRSFNODE |
■	■			SETROPTS | SETROPTS_CLASS | SPT | TEMPLATE | VM_DEV | VM_MDISK |
■				ACCESS | MERGE | RACF_ACCESS] }
■	■	■	■	[WTO]
				NEWLIST TYPE=RACF specific parameters
■	■			**Parameters valid for any resource class:** [ACL(...) | USR(...) | CUSTOM_DATA(...)] [DB=number] [RBA= hex] [GENERIC | DISCRETE] [WARNING | NOWARNING] [CLASS={ class | (class [,class] *) }] [HEXKEY=value] [MEMBERCLASS=class] [MEMBERKEY=key] [NOCATEGORY] [NODATA] [NOSECLEVEL] [{PROFILE | KEY} =name | { MASK | FILTER }=mask | {MATCH | BESTMATCH} =name] [QUAL=id] [SCAN={val|'val'|(val,...)} [FIELD=field]] [segment(fieldtest)]* [SEGMENT=segment | predefseg | NOpredefseg]
■	■			**Parameters valid for DATASET class:** [ERASE | NOERASE] [GROUPDSN | USERDSN] [MODEL | NOMODEL] [PADS] [TAPEDSN | NOTAPEDSN] [VSAM | NONVSAM]
■	■			**Parameters valid for TAPEVOL class:** [AUTOTAPE | NOAUTOTAPE] [SINGLEDS | NOSINGLEDS] [TVTOC | NOTVTOC]
■	■			**Parameters valid for USER and non-RDS CONNECT class:** [ADSP | NOADSP] [AUDITOR | NOAUDITOR] [GRPACC | NOGRPACC] [OPERATIONS | NOOPERATIONS] [REVOKE | NOREVOKE] [SPECIAL | NOSPECIAL]

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**Parameters valid for USER class only:** [ADSP | NOADSP] [AUDITOR | NOAUDITOR] [GRPACC | NOGRPACC] [GRPADSP | NOGRPADSP] [GRPAUD | NOGRPAUD] [GRPGRPACC | NOGRPGRPACC] [GRPOPER | NOGRPOPER] [GRPREVOKE | NOGRPREVOKE] [GRPSPEC | NOGRPSPEC] [NOCLAUTH] [OIDCARD | NOOIDCARD] [OPERATIONS | NOOPERATIONS] [PASSWORD | NOPASSWORD] [PROTECTED | NOPROTECTED] [PWHASHED] [RESTRICTED | NORESTRICTED] [REVOKE | NOREVOKE] [SPECIAL | NOSPECIAL] [UAUDIT | NOUAUDIT]
■	■			**Parameters valid for GROUP and non-RDS CONNECT** class: [TERMUACC | NOTERMUACC] [UNIVERSAL | NOUNIVERSAL]

OPTION

Also valid on **NEWLIST/BUNDLE**. See also **FILEOPTION**.

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[ALLOWRESTRICT]
■	■	■	■	[AUTODETAILSELECT | NOAUTODETAILSELECT]
■	■	■	■	[AUTOSELECT | NOAUTOSELECT]
■	■	■	■	[BCC=*email-address-list*[1]]
■	■	■	■	[BUNDLEBY=*varname*]
■	■	■	■	[CAPS]
■	■	■	■	[CC=*email-address-list*[1]]
■	■	■	■	[CMDTOFILE | NOCMDTOFILE]
■	■	■	■	[COMPAREOPT=*compareopt*]
■	■	■	■	[{DDNAME | FILE } = *name*]
■	■	■	■	[DETAILINHERIT | NODETAILINHERIT]
■	■	■	■	[DETAILSUMINHERIT | NODETAILSUMINHERIT]
■	■	■	■	[DISPLAYTOFILE] [EGN | NOEGN] [EMPTY= '*string*']
■	■	■	■	[EMPTYLIST = { *'string'* | "*string*" | `*string*` | :ISPFvar | HIDE | SHOW }]
■	■	■	■	[{ERRORMAILTO | EMT}=*email address list*] [FIRST_PER_NAME]
■	■	■	■	[FROM=*email-address-list*[1]] [HEADER= { COLUMN | NO | NONE | PREFIX }]
■	■	■	■	[HELPPANEL=*panelname*]
■	■	■	■	| {HELPDETAILPANEL | DETAILHELPPANEL | DETHELPPANEL}=*panelname*]
■	■	■	■	[{LINELEN | LINELENGTH | LL}=*value*]

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[MAILFONTSIZE = [1 | 2| 3| 4| 5 | 6 | 7]] [MAILTO = { email-address-list | :deftype.field }]
■	■	■	■	[MASKTYPE=*type*] [MAXPAGE =*number*] [MSGRC=(*msgno*,*level*)] [MY_CCSID=*number*]
■	■	■	■	[NOACTION] [NOAUTODETAILSELECT] [NOAUTOSELECT] [NODETAILINHERIT] [NODETAILSUMINHERIT] [NOMAIL] [NOMODIFY] [NOPAGE]
■	■	■	■	[NOSUMINHERIT] [OUTLIM=nn]
■	■	■	■	[NOWARNING]
■	■	■	■	[NULLS | NONULLS]
■	■			[ONLYAT]
■	■	■	■	[OUTPUTFORMAT={TEXT | EMAILDEFAULT | ATTACH}] [OVERPRINT=*n*]
■	■	■	■	[PAGEALIGN=*n*] [PAGELENGTH =*n*] [PAGERESET]
■	■	■	■	[PREFIXLEN=nn] [REQUIRED]
■	■	■	■	[REPLYTO=*email-address-list*[1]]
■	■	■	■	[SERIALIZATION([ENQ([CKRDSN],[SYSDSN]) | NOENQ] [FAIL | WAIT
■	■	■	■	[MAXWAIT(*minutes*)]] [UNIT] [VOLSER]
■	■	■	■	[ServerToken=*ServerToken*]
■				[SETROPTS_REFRESH_ON_END] [SMTPCLASS= *sysoutclass*]
■	■	■	■	[SMTPMAILFROM=*email-address-list*[1]] [SMTPNJENODE=*nodename*]
■	■	■	■	[SMTPTOFILE | NOSMTPTOFILE]
■	■	■	■	[SMTPWRITER=*name*]
■	■	■	■	[SNMPTO= { *destination* [:*port* | 162] | (*destination* [:*port* | :162] [,*destination* [:*port* | :162]] *) }]
■	■	■	■	[SNMPTOFILE | NOSNMPTOFILE]
■	■	■	■	[SUMHELPPANEL=*panelname*] [SUMINHERIT | NOSUMINHERIT]
■	■	■	■	[SYSLOGTOFILE | NOSYSLOGTOFILE]
■	■	■	■	[TOPTITLE | TITLE | SUBTITLE | PAGETEXT] [UNRESTRICTED] [WTOTOFILE | NOWTOTOFILE]

■	■	■	■	[1]*email-address-list* should conform to RFC2822 but might have to be quoted to satisfy CARLa syntax:
				`address-list ::= '(address [, address]*)' | 'address' |`
				`address-without-blanks-or-quotes`
				`address ::= mailbox | groupname : [ mailbox-list ] ;`
				`mailbox-list = mailbox | (mailbox [, mailbox]* )`
				`mailbox ::= name-addr | addr-spec`
				`name-addr = [atext | " qtext " ] < [ @ domain [ , @ domain ]* : ]`
				`addr-spec >`
				`addr-spec ::= atext [. atext]* | " qtext "  @ domain`
				`domain ::=  atext [. atext]* | "[" [dtext]* "]"`

PRINT

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	See **OPTION**.

REMOVE

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■				{ { PERMIT=*id* | NOTIFY=*id* | USER=*idlist* | GROUP=*idlist* }
■				[FROMGROUP=*idlist*] [TOGROUP=*idlist* [ALLPERMITS]]
■				[NEWNOTIFY=*id* | REVOKE | REDUNDANT | REDUNDANT_PERMIT] }

REPORT

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			[{ PERMIT=*id* | SCOPE=*id* }* [ACCESS=*level*]]
■	■			[NONREDUNDANT | REDUNDANT | NONDEFAULT | OUTOFGROUP]
■	■			[PADS] [PROFILES] [RESOURCE]
■	■	■		[AC1] [DATASETS] [SCRATCH] [SENSITIVE] [STC]
■	■	■		**Parameters valid with any report:** [BY=([ID,] [KEY,] [DSN,] [MEMBER,] [REASON,])] (default sort order) [PAGEBY=([ID,] [KEY ,] [DSN,] [MEMBER,] [REASON,])] (default sort order)

SELECT and EXCLUDE

Multiple **SELECT** and **EXCLUDE** commands can be present. Records that match any of the **SELECT** commands and none of the **EXCLUDE** commands are processed. Within a single command, the special operators AND, OR, NOT, and parentheses can be used to clarify and define the logical relation between clauses. See also Chapter 4, "CARLa SELECT/LIST fields," on page 27.

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[LIKELIST=*newlistname*]
■	■	■	■	[MISSING(*field*)]
■	■	■	■	IFDEFINED(*field*)

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax	
■	■	■	■	[EXISTS(*field*)][*fieldtest*]* ***fieldtest* can be:**	
■	■	■	■	*fieldname* = valuelist	*fieldname* == *fieldname*
■	■	■	■	*fieldname* < *value*	*fieldname* << *fieldname*
■	■	■	■	*fieldname* > *value*	*fieldname* >> *fieldname*
■	■	■	■	*fieldname* <= *value*	*fieldname* <<== *fieldname*
■	■	■	■	*fieldname* >=*value*	*fieldname* >>== *fieldname*
■	■	■	■	*fieldname* ¬= *valuelist*	*fieldname* ¬== *fieldname*
■	■	■	■	*fieldname* < > *valuelist*	*fieldname* <<>> *fieldname*
■	■	■	■	*fieldname*(*valuelist*)	*fieldname*=:(*scanvaluelist*)

SHOW

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[CKRSITE | ZAP]
■	■	■	■	[CLASSES | CLASS] [ICHNCV00] [TEMPLATES | TEMPLATE]

SIMULATE

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[CNGRACF | CKGRACF] [{ CNGRACF | CKGRACF } CLASS=*class*]
■	■	■	■	[{ CNGRACF | CKGRACF } COMPLEX=*complex*]
■	■	■	■	[{ CNGRACF | CKGRACF } COMPLEX=*complex* CLASS=*class*]
■	■			{ DMSPARMS { RACFALWZ*val* | RACFBKUP*val* | RACFPRED*val* | RACFSUPP*val* | RACFPROC*val* | RACFNEWN*val* | RACFDVOL*val* | RACFUSID*val* | SECURVOL*val* } |
	■	■	■	POLICY [C1 | C2 | B1] |
■	■			RACF_ACCESS | ACCESS_FALLBACK_DEFAULT
■	■	■	■	[ACCESS=[READ|UPDATE]] [SENSITIVITY {*acc cls name* | LINKLIST | PROCLIB } | [<*Site-text-string*> PRIO={2|3|4|5|6|7|8|9} [ID=S<*id*>] CONCERN='concern text']] |
■	■	■	■	SHARED | NONSHARED | SYS=*list* | VOL=*list* |
■	■	■	■	SMF=*number* SYSTEM=*smfid* FORMAT=fmt |
■	■	■	■	TODAY=*date* |
■	■	■	■	[RESOURCE_LOCATION=*name*] |
■	■	■	■	RESTRICT |
The syntax of the rest of this command is similar to **RACF** commands:					

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			RDEF FACILITY IRR.PGMSECURITY APPLDATA (*'mode'*) |
■	■			SETROPTS [NO]TAPEDSN] [[NO]EGN] [NOERASE | ERASE({ ALL | [NO]SECLEVEL })] [NOMODEL | MODEL([[NO]USER] [[NO]GROUP] [[NO]GDG])] [NOPROTECTALL | PROTECTALL({ WARNING | FAILURES })] [NO]WHEN(PROGRAM) }

SMFCACHE

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	[ON | OFF | MINIMAL]
	■	■	■	[RECORDS=*number*]
	■	■	■	[JOBRECORDS=*number*]
	■	■	■	[VERBOSE]

SORTLIST

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	{ *fieldname* | *varname*[8] | :*object_reference*[9] | *basefieldname*:*id_or_deftype_reference*[9] [([*format*] [*length*] [*'header'* | *"header"*] [*mods*] [*dmods*] [*nmods* | *rmods*])] |
■	■	■	■	| operator | string [([*format*] [*length*] [*'header'* | *"header"*])] }*

See Chapter 4, "CARLa SELECT/LIST fields," on page 27 for possible values of *fieldname* and *basefield*.

For an explanation of the conditional field include, see Conditional field include.

For the possible values of *format, mods, dmods, nmods*, and *rmods*, see the "Format names", *mods, dmods, nmods*, and *rmods* in the tables that follow.

[8]*varname* cannot be a statistic. See "DEFINE" on page 9.

[9]*:object_reference* is explained at "DEFINE" on page 9.

Note: The **LIST** command in **NEWLIST** TYPE=RACF or TYPE=ACF2_LID does not support any indirect references.

Conditional field include:

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	{ *fields_and_operators* | *conditional_include* } *

where

conditional_include ::= (*symbolic=value ? fields_and_operators*)

and

fields_and_operators ::= { *fieldname* \| *varname* \| etcetera } *

and

symbolic must be a variable defined with the **SYMBOLIC** statement

and

value must be an appropriate value that could have been assigned to the *symbolic* variable

Format names:

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			$ACL $AsymKeyUsage $CFSYN $CMDAUTH $CONNECT $CUSTOM $CUSTOM_DATA
■	■			$DOM $LOGCMDR $LOGDAYS $LOGTIME $LOGZONE $MEMLST $MFORM
■	■			$SymKeyExp $MSGLEVL $NO $RACLINK $RESFLG $RETPD $SYN $TIMEOUT
■	■			$XRFSOFF $USRDATA $YESNO ACLACCESS ACLID ACLIDACCESS ACLVIA CSVALUE
■	■			KEYUSAGE_RACF KEYUSAGE_X509 RACFLEVEL SLKEY_COMPACT USRDATA WHEN
■	■	■	■	$AUDITLVL $CASE $CHAUDIT $CHMOD $CONDQT
■	■	■	■	$DATE $EXTATTR $MONITOR $QUOTED ACCESS ACCESS_NZ
■	■	■	■	ACF2DATE ACF2DATETIME ACSI ADDRESS AFC ASIS AUDAC AUDIT
■	■	■	■	AUTHORITY BLANK$HDR BLANK$NO BLANK$STR CATEGORY CHAR CHR$NOFF
■	■	■	■	CMDAUTH CONNECTID CONTENTS CONVSEC DATE DATETIME
■	■	■	■	DATETIMEZONE DATE$STR DEC DEC$ABBREVIATE DEC$BLANK DEC$NO DOM
■	■	■	■	DSTYP DUMP[(length)] EUDATE EXTATTR FILEAUDIT FILEMODE FILETYPE
■	■	■	■	FLAG FLAG2NICE FLDLEN GID HDR$BLANK HEX IP IPSQ IPV4OR6
■	■	■	■	IPV4OR6SQ JULDATE L1ASIS
■	■	■	■	L1CHAR LOGDAYS LOGTIME LOWERCASE MFORM MONITOR MONTH MONTHDAY
■	■	■	■	MSGLEVL MVSMSGLEVEL NUM OCTAL OPERUND PGMRNAME PORT PRINTABLE
■	■	■	■	RESFLG ROUTCDE SECLEVEL SECURPASS_DATE SECURPASS_RC
■	■	■	■	SECURPASS_REQUEST SIGNEDDEC SMFTIME
■	■	■	■	SMFTIMESTAMP SMFTIMESTAMPZONE STR$BLANK TIME TOD TSOOPT
■	■	■	■	UDEC UDEC$ABBREVIATE UID UPPERCASE UPT USDATE
■	■	■	■	WEEKDAY XSD_DATETIME YEAR YESNO

***mods*=General output format modifiers**

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	ALLOWRESTRICT [BOTH | FIRST] CONDPAGE(*nnn*) CONVERSION(*conversionname*) DESCENDING
■	■	■	■	DETAIL INDENT KEY NODETAIL NOMODIFY NONDISPLAY NOPREFIX NOSORTLIST
■	■	■	■	NOTEMPTY PAGE PREFIX TITLE TOPTITLE TRUNCATE UNIVERSAL
■	■	■	■	VARLEN WORDWRAP WRAP

dmods=Display output format modifiers

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	BOLD CH CT ET FP LID LI NT PAS SI WASL WT

nmods=Non-Repeat group format modifiers

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	EXPLODE NORETAIN RETAIN

rmods=Repeat group format modifiers

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	EFFECTIVE EXPLODE FIRSTONLY HEADER HORIZONTAL(entrylength) MORE
■	■	■	■	NODUP NOORIGIN NOSCOPE ORIGIN RESOLVE SCOPE SORT

STANDARD

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	STANDARD *standardname* [DESCRIPTION('*description*')] [VERSION(*version*)] [ESM({RACF|ACF2|TSS|NONE})]
				{ DOMAIN *domainname* SELECT(*type* [(*selclause*)] ...), [DESCRIPTION('*desc*'),] [SUMMARY(*type*(*field*...))] | DEFINE TYPE=*type*... * | INCLUDE MEMBER=*member* RULE_SET *SET* [DESCRIPTION('*desc*'),]

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
				RULE *rulename* DOMAIN(*name*), [DESCRIPTION('*desc*'),] [SET(*set*)] [EXEMPT('*type*(*selclause*))] { TEST *testname* *type*{=count | (*fieldnamerelopercompliantvalue*)} [DESCRIPTION(*desc*)] [NONCOMPLIANT] [OTHERWISE(UNDECIDED | *nested TEST*...)] } * ENDRULE [*rulename*] } * ENDSTANDARD [*standardname*]

The following nesting rules apply:

- DOMAINs must occur within a STANDARD.
- TESTs must occur within a RULE.

SUMMARY

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	*summarylevel* [* *summarylevel*]*
■	■	■	■	*summarylevel* ::= [*statistic*]* *keyfieldname*[10] [*statistic* | *keyfieldname*[11]]*
■	■	■	■	keyfield ::= { *fieldname* | *definedname*[12] | *:object_reference* | *basefieldname*:*id_or_deftype_reference*[13] }

[10] *keyfieldname*: If a repeated field is used, no further `keyfields` are allowed

definedname: This field cannot be a statistic. See "DEFINE" on page 9.

basefieldname:*id_or_deftype_reference*: These fields are explained at "DEFINE" on page 9.

SUPPRESS

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
		■		[ACF2]
■	■	■	■	[ACCESS_GDG_VERSION] [ACCESS_JESSPOOL_JOBID] [ACCESS_JESSPOOL_DSID]
	■	■	■	[AUTORESOURCE]

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	[DBIDCACHE]
■	■	■	■	[{CATALOG| CAT}=*catname*]* [CKFREEZE | IOCONFIG] [ID=*id*] [FMTABEND]
■	■	■	■	[{MSG | MESSAGE}=*list*] [MSGTIMER] [MYACCESS<*level*] [NOT_MY_LIST_SCOPE]
■	■	■	■	[SMF]
■	■	■	■	[SOFTEOF] [UNIXCACHE]
■	■	■	■	[{VOLUME | VOL | VOLSER}=*volser*]*
■	■			[CONNECTOWNER] [DELDSD] [DELETEDATASETS] [DELETENOSCRATCH]
■	■			[DELETEUNCATALOGED] [ECKD]
■	■			[FALLBACK] [ICHCNX00] [ICHNCV00] [ICHRRNG]
■	■			[INDEX] [INDEXCUTOFF] [RACF] [REASON=list] [SETROPTSREFRESH]
■				[ADDSD] [COPYALIAS] [COPYCUSTOMDATA | COPYCSDATA] [COPYUSERDATA | COPYUSRDATA] [MANAGERACFVARS]

list values for REASON:

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax			
■	■			ALTER-M	GRPOPERATIONS	NOPROFILE	SELFCONNECT
■	■			CKGOWNR	GRPSPECIAL	OWNER	UACC
■	■			GLOBAL	ID(*)	PWDCHANGE	WARNING
■	■			GRPAUDIT	UNPROTECTED		

SYMBOLIC

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	*type* name=*value*

UNLOAD

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[{ DDNAME | FILE }=*ddname*] [COMPLEX=*name*]

VERIFY

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■		[ALL] [BY=*list* { MSG | {VOL | VOLUME | VOLSER} | DSN DATASET | PGM PROGRAM PROG | ID PERMIT}]

Options for security database *without* CKFREEZE:

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■		[CONNECT] [GROUPTREE]
■	■	■		[PADS]
	■			[PASSWORD]

Options for security database *with* CKFREEZE:

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■		[STC]
■				[ALLNOTEMPTY] [ONVOLUME] [INDICATED]
■	■	■		[NOTEMPTY | GENERIC] [PERMIT] [PROTECTALL] [PROGRAM]
■	■	■		[PROGRAMNONEMPTY]
■	■	■		[PGMEXIST]
	■			[SENSITIVE]
	■			[TSOALLRACF]

Additional sorting option:

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	[BY=([MSG,] [VOL,] [DSN,] [PGM,] [ID, | PERMIT,])] (default sort order)

Chapter 4. CARLa SELECT/LIST fields

zSecure users can use the fields that are supported within NEWLISTs to generate reports on a specific type of information.

Type=ACCESS: Access Monitor records access allowed

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■				access_allowed access_count access_count_big access_flags_raw access_generic access_global access_is_group access_phrase_changed access_privtrus access_profile access_proftype access_ptkt_replay access_pwd_changed access_result access_special access_undefined_user access_used_exit appl attrib_operations attrib_special class collect_datetime complex ddname flags_raw intent intent_raw jobname last_datetime last_datetime_runtz last_tod recno record record_length recordlength rectype req_checkauth req_command req_generic req_privcsa req_propagated req_racfind req_racfind_specified req_status_access req_verify req_verify_alreadyenc req_verify_method resource seclabel sim_class sim_generic sim_profile sim_proftype sim_result sim_via sim_via_groups system userid utoken_poe utoken_poeclass utoken_poe_raw

Type=ACF2_CLASMAP: ACF2 CLASMAP settings

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
		■		clasmap_codesource clasmap_entitylen clasmap_len_used clasmap_log clasmap_mixed clasmap_musid clasmap_posit clasmap_profint clasmap_resclass clasmap_rescode clasmap_signal clasmap_used collect_datetime complex system ver

Type=ACF2_FDE: ACF2 field definition entries

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
		■		bitmap chgauth complex counter datatype description display_group fieldname header length listauth masked multivalued nodefault offset outfmt outlength pseudo record_type required rescode timestamp trivial zero

Type=ACF2_INFO: ACF2 InfoStorage records

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
		■		assize complex cputime deflabel descript division dsn exclude fileproc group hexrule home include inf info_class key lid memlimit mmaparea nextkey omvspgm percentage_used primary procuser record_length residence_type resource seclabel secondry shmemmax smf_key source stored_by stored_when role sysid threads timestamp type typecode uid ver waaccnt waaddr1 waaddr2 waaddr3 waaddr4 wabldg wadept waname waroom

ACF2_INFORULE, ACF2_INFOLINE: ACF2 resource rules

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
		■		access_level active change class complex data evaluation_id extended_key hexrule info_class key member nextkey nextkey_depth norulelng nosort owner percentage_used prefix rchange reccheck recname record_length resource_class resource_mask role roleset rule_entry rule_header sequence_number service service_effective shift smf_key source stored_by stored_when timestamp type typecode uid until user userdata verify xref

Type=ACF2_LID: ACF2 Logonid records

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
		■		acc-cnt acc-date acc-srce acc-time account acctpriv acf2cics acf2_uid_group active allcmds any_uid_string attr2 audit auditconcern auditpriority authsup1 authsup2 authsup3 authsup4 authsup5 authsup6 authsup7 authsup8 authsup_effective autoall autodump autonopw autoonly bdt cancel char cics cicscl cicisid cicskey cicskeyx cicsopt cicspri cicsrsl cmd-long cmd-prop complex console consult cre-tod csdate cswho dft-dest dft-pfx dft-sout dft-subc dft-subh dft-subm dg84dir dialbyp dsnscope dumpauth expire group grplogon grp-opt grp-user homenode idle idms idmsprof idmsprvs ims inactivated intercom jcl job job_effective jobfrom kerbcur kerbcurv kerbpre kerbprev kerb-vio last_update ldev lds leader lgn-acct lgn-dest lgn-msg lgn-perf lgn-proc lgn-rcvr lgn-size lgn-time lgn-unit lid lidscope lidtemp lidzmax lidzmin line logshift mail maint maxdays maxdays_effective mindays mindays_effective mode mon-log monitor mount msgid multsign musass musdlid musid musidinf musopt muspgm musupdt name no-inh no-omvs no-smc no-stats no-store nomaxvio non-cncl nospool notices operator password password_chdate password_expired pause pgm phone pmt-acct pmt-proc ppgm pp-trc pp-trcv prefix priv-ctl program prompt prvpswd1 prvpswd2 prvpswd3 prvpswd4 prv-tod1 prv-tod2 prv-tod3 prv-tod4 pswa1tod pswa1val pswdaes1 pswdcvio pswd-dat pswd-exp pswd-inv pswd-mix pswd-mx8 pswd-src pswd-tim pswd-tod pswd-upp pswd-vio pswd-xtr pswd-xtv pticket pwp-date pwp-vio pwpallow pwpallow-effective r221pswd readall recover refresh restrict rsrcvld rstdacc rulevld scplist security sec-vio shift smsinfo source srf stc subauth suspend suspended_for_passlmt syncnode synerr syspexcl tape-blp tape-lbl tdiskvld timestamp trace tso tso_effective tso-trc tsoacct tsocmds tsofscrn tsoperf tsoproc tsorba tsorgn tsosize tsotime tsounit uid uidscope unicntr upd-tod user vax ver vld-acct vld-proc vldrstrct vldvmact vm vmacct vmbatch vmbatmon vmd4auth vmd4fsec vmd4rset vmd4targ vmidlemn vmidleop vmsaf vmesm vmsfs vmxa vsesrf wtp zone

Type=ACF2_RES_INFORULE: ACF2 resident resource rules

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
		■		class collect_datetime complex hexdir hexrule key match_order match_order_index resource_class rule_entry rule_header sequence_number system type typecode

Type=ACF2_RULE, ACF2_RULELINE: ACF2 rule records

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
		■		active change complex data dd dsn_mask evaluation_id hexrule key library member mode nextkey nextkey_depth norulelng nosort owner path percentage_used permissions pgm prefix program rchange record_length resowner role roleset rule_entry rule_header sequence_number shift source stored_by stored_when timestamp uid until user userdata volume

Type=AUDIT: System setting audit concerns

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	area areaparm auditconcern auditpriority collect_datetime complex concern parmname parmvalue system

Type=AUTAB: Authorized caller table

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			[attr | auth] collect_datetime complex [order | org] program racinit raclist system ver

Type=CICS_PROGRAM: CICS programs

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	api_subset asid auditconcern auditpriority cedf class collect_datetime complex data_key data_location enabled jobid jobname jvm jvmclass jvmprof lang_ded lang_def openapi_ded openapi_def pgm_type program qualified_resource reload resident resource resource_location rmt_dynamic rmt_name rmt_system rmt_transid stepname sysidnt system threadsafe_ded threadsafe_def vtam_applid
	■			racf_acl racf_class racf_profile racf_uacc

Type=CICS_REGION: CICS regions

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	ai_console ai_exit asid cics_level class_appc class_cmd class_db2 class_dct class_ejb class_fct class_jct class_pct class_ppt class_psb class_res class_sur class_trn class_tst collect_datetime complex csd_disp csd_dsn csd_readonly default_user dli_psbchk ejbrole_prefix gmtext gmtran gntran grplist hpo hpo_svcno jobid jobname keyring pgm_llacopy pgm_lpa pgm_prvmod pgm_rentpgm pltpi_sec pltpi_user [region_user | region_userid] sec_appc sec_cmd sec_cmdsec sec_db2 sec_dct sec_ejb sec_esm sec_fct sec_jct sec_pct sec_ppt sec_prefix sec_psb sec_res sec_ressec sec_sur sec_trn sec_tst sec_unixfile ssl_encrypt stepname stor_cmdprot stor_cwakey stor_prot stor_taskchk stor_tctuakey stor_tctualoc stor_termchk stor_traniso svcno sysidnt system trace_confdata trace_conftxt ver vtam_applid vtam_genapplid vtam_grname
	■	■	■	auditconcern auditpriority

Type=CICS_TRANSACTION: CICS transactions

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	asid auditconcern auditpriority class collect_datetime complex data_clear data_freeze data_key data_location enabled jobid jobname ots_timeout priority program qualified_resource queue_local rcvy_action rcvy_dtime rcvy_dump rcvy_restart rcvy_runaway rcvy_runaway_system rcvy_spurge rcvy_tpurge rcvy_wait rcvy_waittime resource resource_location rmt_dynamic rmt_name rmt_routable rmt_system rmt_tranprof sec_cmd sec_res stepname sysidnt system trace trace_confdata tran_alias tran_class tran_isolation tran_profile tran_shutdown tran_taskreq tran_tpname tran_xtranid transaction twasize vtam_applid
	■			racf_acl racf_class racf_profile racf_uacc

Type=CLASS: Class descriptor table

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			active audit auditconcern auditpriority case_asis class classno clastype clauth collect_datetime complex dataspc description dfltrc equalmac gen gencmd generic generic_allowed genlist genlist_allowed glb global id inrfr installation_defined jobname logopt maxlen maxlen_entity noprof numdisc numgen numprof oper operoper [org | order | classno] posit protect qual raclist raclist_allowed raclist_gbl_only raclreq rvrsmac same_pos seclabel signal stats syn1alp syn1nat syn1num syn1raw syn1spe synralp synrnat synrnum synrspe synrraw system uacc ver where xclass xgroup xmember

Type=COMPLIANCE

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	class complex domain domain_desc proftype resource rule rule_desc rule_exempt rule_set rule_set_desc standard standard_desc standard_version suppress suppress_reason system test test_base_field test_compliant test_compliant_value test_desc test_field test_field_base_value test_field_value test_newlist_type test_noncompliant test_reloper test_result volser_key

Type=CONCERN_TEXT: Concern translation properties

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	concern concern_id concern_orig newlist_type newlist_tag

Type=CONSOLE: System consoles

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	active alternate auditconcern auditpriority auth auto cmdsys cnid collect_datetime complex console_no [device_no | devnum] dom hc intids jobid key level logon luname migid monitor name pfktab [routecode | routcode] subsystem switchto system type ud unknids userid ver
	■			racf_profile

Type=CSM: Common storage

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	auditconcern auditpriority collect_datetime complex end fprot key length start start64 subpool system type

Type=DASDVOL: DASD volumes

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	attr auditconcern auditpriority box_serial box_type complex device format minidisk mounted online order org read_only shared sms_managed system unit use ver vmlink volume

Type=DB2_DATABASE: DB2 databases

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	alter_timestamp bufferspool class collect_datetime complex createdby create_timestamp create_timestamp_db2 database dbid db2id db2_acl implicit index_bufferspool owner ownertype resource stogroup stystem type
	■			racf_db2_acl

Type=DB2_JAR: DB2 Java archives

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	alter_timestamp alter_timestamp_db2 class collect_datetime complex create_timestamp create_timestamp_db2 db2id db2_acl jar_id owner ownertype path resource schema system
	■			racf_db2_acl

Type=DB2_PACKAGE: DB2 subsystems packages

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	bind_timestamp bind_timestamp_db2 class collect_datetime collection complex creator db2_acl db2id lastuse_date lastuse_date_db2 owner ownertype package package_type pdsname racf_db2_acl remarks resource system version

Type=DB2_PLAN: DB2 subsystems plans

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	bind_timestamp bind_timestamp_db2 boundby class collect_datetime complex db2_acl db2id lastuse_date lastuse_date_db2 owner ownertype plan racf_db2_acl resource system

Type=DB2_REGION: DB2 subsystems

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	asid charopt class class_admin class_buffer_pool class_collection class_database class_dsnr class_jar class_package class_plan class_schema class_sequences class_storedproc class_storgrp class_system class_table_index_view class_tablespace class_user_function class_user_type classnmt classopt collect_datetime complex db2_acl db2_level db2id group_name jobid jobname lu_name pc_lx racf_db2_acl [region_user | region_userid] resource site_name start_datetime stepname subsys_char sysparm_active sysparm_active_datetime sysparm_startup system ver zprm_access_cntl_module zprm_arcpfx1 zprm_arcpfx2 zprm_auditst zprm_auth zprm_bindnv_bindadd zprm_dbacrvw zprm_defltid zprm_extsec zprm_idauth_module zprm_irlmprc zprm_mccsid zprm_mixed zprm_rlfauth zprm_sccsid zprm_secadm1 zprm_secadm1_is_role zprm_secadm2 zprm_secadm2_is_role zprm_separate_security zprm_signon_module zprm_smfacct zprm_smfcomp zprm_smfstat zprm_sysadm zprm_sysadm2 zprm_sysopr1 zprm_sysopr2 zprm_tstamp zprm_util_temp_storclas
	■	■	■	auditconcern auditpriority

Type=DB2_ROUTINE: DB2 stored procedures

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	active class collect_datetime collection complex db2id db2_acl external_name external_security fenced origin owner ownertype packagepath remarks resource routine routinetype schema secure specificname system version wlm_environment
	■			racf_db2_acl

Type=DB2_SEQUENCE: DB2 sequence

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	alter_timestamp alter_timestamp_db2 cache class collect_datetime complex create_timestamp create_timestamp_db2 createdby cycle datatypeid db2id db2_acl increment maxassignedval maxvalue minvalue name order owner ownertype precision remarks resource restratwith schema seqtype sequenceid sourcetypeid start system
	■			racf_db2_acl

Type=DB2_STOGROUP: DB2 storage groups

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	alter_timestamp alter_timestamp_db2 catalog class collect_datetime complex create_timestamp create_timestamp_db2 createdby dataclas db2id db2_acl mgmtclas owner ownertype resource space stogroup storclas system [volser | volume]
	■			racf_db2_acl

Type=DB2_TABLE: DB2 subsystem tables

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	alter_timestamp alter_timestamp_db2 auditing class complex control createdby create_timestamp create_timestamp_db2 database db2id db2_acl dbid label location name obid owner ownertype racf_db2_acl related_schema related_table resource resource_prefix row_mls schema system tablespace table_type user_table
	■			racf_db2_acl

Type=DB2_TABLESPACE: DB2 subsystem table space

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	alter_timestamp alter_timestamp_db2 bufferpool class collect_datetime complex createdby create_timestamp create_timestamp_db2 database db2id db2_acl dbid dsname erase instance implicit log obid owner ownertype partitions psid resource space stogroup system tablespace type
	■			racf_db2_acl

Type=DEFTYPE: User defined data source

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	complex ddname recno record record_length

Type=DSN: Data set names

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
		■		acf2_rule_entry

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	alias_relate alias_relate_effective box_serial catalog catalog_alias catalog_volume collect_datetime complex dsname dsn_type in_connected_catalog in_directed_catalog in_master_catalog in_vtoc in_vvds is_migrated is_mounted qual qual_is_user real_dsname real_volume resource sensitivity system unittype via_symbolic_relate volume
	■			profile qual_is_dataset_profile qual_is_group

Type=DSNT: Data set name table

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			active attr bufno cms complex [db | seqno] [dsn | dataset] [mstr | master] [order | org] prim rds rectrk [shr | shared] [stat | stats | initstats] system volume

Type=DYNEXIT: System exits

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	abendconsec abendnum active# amode anykey auditconcern auditpriority collect_datetime complex description execkey exitname explicit fastpath inactive# rent_req singlemodule system

Type=EXIT: System exits

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	active active_effective address amode anykey appl at auditconcern auditpriority collect_datetime complex [content | contents] description execkey exitname explicit filter_jobname filter_stoken filter_type jobname key length module offset param position program result scan_instr scan_string scan_svc subpool [subsys | subsystem] system where

Type=FIELD: Field properties per newlist type

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	advertize base casesensitive compare_usage compare_usage_base compare_usage_by compare_usage_compare compliance_improvement description description_orig field field_tag format header header_orig help_panel horizontal length length_orig lookuponly maximum_length modifiable newlist_abbrev newlist_tag newlist_type repeated restrict subselect translated wrap

Type=FIELD_OVERRIDE

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	description description_orig field header header_orig language length length_orig newlist_name newlist_type occurrence order screddn srceline srcemem val val_orig

Type=ICSF_TOKEN: Token and certificate data from TKDS

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	alter_timestamp certificate_appl certificate_create_ts certificate_default certificate_id certificate_issuer certificate_label certificate_serial certificate_subject class collect_datetime complex create_timestamp manufacturer model name resource sequence serial system

Type=ID: User IDs and groups

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	class complex db2_authid defined dsn_hlq hsmcntl hsmdba id racf_ichrin03 racf_key racf_owner racf_permit racf_started revoked stc stcproc superuser tso uads verify vm_user vm_acigroup

Type=IMS_PSB: IMS program specification blocks

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	asid auditconcern auditpriority class collect_datetime complex imsid jobid jobname psbname qualified_resource resource resource_location stepname system transaction vtam_applid

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■			racf_acl racf_class racf_profile racf_uacc

Type=IMS_REGION: IMS subsystems

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	asid class_apsb class_cmd class_db class_field class_lterm class_oth class_otma class_psb class_seg class_tran collect_datetime complex ims_level imsid jobid jobname rclass region_type [region_user | region_userid] sec_ao_cmd sec_ao_icmd sec_cmd_all sec_cmd_eto sec_console_cmd sec_multi sec_odba sec_pr_cmd_all sec_pr_cmd_eto sec_pr_fuser sec_pr_multi sec_pr_password_upper sec_pr_user sec_racf_avail sec_rasexit sec_rasracf sec_re_cmd_all sec_re_cmd_eto sec_re_multi sec_re_trans sec_re_user sec_sd_cmd_all sec_sd_cmd_eto sec_sd_enh sec_sd_ftrans sec_sd_fuser sec_sd_multi sec_sd_racfterm sec_sd_trans sec_sd_user sec_tco_racf sec_trans sec_trans_active sec_user sec_user_active sec_viol_limit stepname subsys_crc svcno system ver vtam_applid
	■	■	■	auditconcern auditpriority

Type=IMS_TRANSACTION: IMS transactions

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	asid auditconcern auditpriority class collect_datetime complex imsid jobid jobname psbname qualified_resource resource resource_location stepname system tran_class transaction vtam_applid
	■			racf_acl racf_class racf_profile racf_uacc

Type=IOAPP: I/O appendages

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	address auditconcern auditpriority collect_datetime complex [content | contents] default defaulttype description id name system type where

Type=IP_AUTOLOG: TCP/IP autolog configuration

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	collect_datetime complex jobname options parmstring procname stack sysname sysplex system wait

Type=IP_INTERFACE: TCP/IP interface configuration

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	assoc_name chpid collect_datetime complex index interface intfid ip ipmask options pfxlen secclass sourcevipa_interface stack sysname sysplex system type vlan_id vmac_address

Type=IP_FTP_REGION: FTP daemon settings

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	anonymous_hfs_dir_mode anonymous_hfs_info anonymous_level anonymous_login_msg anonymous_mvs_info anonymous_password_set anonymous_surrogate anonymous_user anonymous_ftp_logging asid auto_mount auto_recall auto_tape_mount banner ciphersuite dataclass datetime_started db2 db2plan dcbdsn debug_on_site dest_node dest_user directory_mode dsn_ftp_data dsn_tcpip_data ds_wait_time dump_on_site email_addr_check env_bpx_jobname env_ krb5_server_keytab env_resolver_config extensions filetype ftp_keep_alive ftp_logging hfs_info inactive ispf_stats jes_get_by_dsn jes_interface_level jobname keyring login_msg mgmtclass migratevol mvs_info mvs_url_key passivedataconn_noredir passive_data_port_high passive_data_port_low passphrase port port_command_accept port_command_noredir port_command_nolowports port_of_entry_4_class region_userid, region_user reply_security_level rest_put secure_ctrl_conn secure_data_conn secure_ftp_required secure_implicit_zos secure_login secure_password_req secure_password_kerb_req secure_pbsz smf_type118_exit smf_type118_jes smf_type118_sql smf_type118_std smf_type118_subtype smf_type118_subtype_appe smf_type118_subtype_del smf_type118_subtype_logn smf_type118_subtype_ren smf_type118_subtype_retr smf_type118_subtype_stor smf_type119 smf_type119_jes smf_type119_sql smf_type119_subtype_appe smf_type119_subtype_dcfg smf_type119_subtype_del smf_type119_subtype_logn smf_type119_subtype_ren smf_type119_subtype_retr smf_type119_subtype_stor startdirectory_mvs storclass tlsmechanism_attls tls_port tls_rfc_level tls_timeout umask ver verify_user

Type=IP_NETACCESS: TCP/IP network access control configuration

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	collect_datetime complex inbound ip ipmask outbound pfxlen resname resource stack sysname sysplex system
	■			racf_acl racf_profile

Type=IP_PORT: TCP/IP port configuration

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	auditconcern auditpriority begin_port bind collect_datetime complex count end_port jobname options portrange protocol resname resource stack sysname sysplex system unrsv use
	■			racf_acl racf_profile

Type=IP_RESOLVER: CS Resolver configuration

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	alwayswto auditconcern auditpriority autoquiesce cache cachesize common_search collect_datetime complex datasetprefix dbcs_table_name defaultipnodes defaulttcpipdata domain domainorigin globalipnodes globaltcpipdata globaltcpipdata_spec hostname lookup maxttl nameserver nsportaddr options_ndots preferred_address preferred_mask resolvertimeout resolverudpretries resolvevia_tcp search setup_file setup_file_employed socksteststor stack sysname sysplex system tcpipjobname unresponsivethreshold

Type=IP_ROUTE: TCP/IP route configuration

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	collect_datetime complex dstip interface interface_index ipmask nexthop_ip pfxlen replaceable replaced stack sysname sysplex system

Type=IP_RULE: TCP/IP rule configuration

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	code collect_datetime complex dstip dstipmask dstpfxlen dstport log protocol routing secclass srcip srcipmask srcpfxlen srcport stack sysname sysplex system type

Type=IP_STACK: TCP/IP stack configuration

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	auditconcern auditpriority collect_datetime complex datetime_started dsnmem dynamicxcf_intfid dynamicxcf_ip dynamicxcf_ipmask dynamicxcf_ip6 dynamicxcf_pfxlen dynamicxcf_pfxlen6 dynamicxcf_secclass dynamicxcf_secclass6 dynamicxcf_sourcevipaint globalconf_iqdvlan globalconf_mlscheckterm globalconf_xcfgrpid ipconfig ipconfig_ipsecurity ipconfig6 ipconfig6_ipsecurity ipsec_dvipsec ipsec_logenable ipsec_logimplicit last_change_datetime netmon_pkttrcservice netmon_smf_ipsecurity netmon_smf_profile netmon_smfservice netmon_tcpconn_minlife netmon_tcpconnservice saconfig_osasf_port saconfig_snmp_port saconfig_snmp_pwdefault smf119_ftpclient smf119_ifstat smf119_ipsecurity smf119_portstat smf119_tcpinit smf119_tcpipstack smf119_tcpipstat smf119_tcpterm smf119_tn3270client smf119_udpterm stack sysname sysplex sysplex_group system tcp_restrictlowports tcpstacksourcevipa tcpstacksourcevipa6 udp_restrictlowports

Type=IP_TELNET_PORT: TelnetParms settings

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	allowappl_appl allowappl_disconnect allowappl_lu_group allowappl_lu_rule allowappl_lu_begin allowappl_lu_end allowappl_qsession conntype defaultappl_appl defaultappl_qinit defaultappl_defonly defautlappl_firstonly defaultappl_client_type defaultappl_clientid expresslogon inactive maxreqsess msg07 nacuserid passwordphrase port port_qual_ip port_qual_link port_index port_type restrictappl_appl restrictappl_user restrictappl_certauth restrictappl_disconnect restrictappl_lu_group restrictappl_lu_rule restrictappl_lu_begin restrictappl_lu_end restrictappl_qsession secureport_keyring_saf secureport_keyring_hfs secureport_keyring_mvs secureport_encryption secureport_clientauth secureport_sslv2 smfinit_type119 smfinit_type118 smfinit_type118_subtype smfterm_type119 smfterm_type118_subtype ssltimeout tkogenlu tkogenlu_keepontmreset tkogenlu_sameipaddr tkogenlu_sameconntype tkospeclu tkospeclu_keepontmreset tkospeclu_sameipaddr tkospeclu_sameconntype usstcp_table usstcp_scs usstcp_client_type usstcp_clientid

TYPE=IP_TELNET_REGION: TelnetGlobal block settings

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	datetime_started dsnmem jobname last_change_datetime [region_user | region_userid] secureport_crlldapserver smfprofile telnet_config tnsaconfig_enabled tnsaconfig_snmp_pwdflt tnsaconfig_snmp_agent tnsaconfig_snmp_enabled user

Type=IP_VIPA: TCP/IP VIPA configuration

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	active collect_datetime complex interface ip ipmask options pfxlen rank resname resource stack sysname sysplex system type
	■			racf_acl racf_profile

Type=JOBCLASS: JES2 job classes

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	acct auditconcern auditpriority auth blp class collect_datetime command complex hold iefujp iefuso proclib region [subsystem | subsys] swa system time type6 type26

Type=MEMBER: Library change detection

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	ac1 addition alias alias_of amode apf appl bytes change_date checksum complex crc [dataset | dsn] deletion dsorg enddate epa identify identify_id last_change last_change_userid lkeddate loadmod member new_identify new_zap number nx ol pdf pdf_chgdate pdf_chgtime pdf_creadate pdf_userid pdf_version prevdate psigned psigprob rent reus rmode scan_instr scan_string scan_svc sequential sysplex ssi startdate storsize sysplex system ttr versions volume zap zap_id

Type=MERGE: RACF database merge

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■				class code cur_profile cur_value field new_value pass profile reason src_profile src_value

Type=MOUNT: UNIX mount points

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	acl aggregatesize blocksize collect_datetime complex concern dataset dev device dsn dsname filesysname filesystype fragmentsize mode mountpoint nbs owning_complex owning_system readonly_seclabel rwshare security serial setuid sysplex_mode system trusted ver volume
	■	■	■	auditconcern auditpriority

Type=MSG: Message Processing Facility

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	auditconcern auditpriority auto collect_datetime complex exit exit_address exit_at exit_where mpflst msgid suppress system

Type=NEWLIST: Report translation properties

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	detailhelppanel helppanel language newlist_name newlist_type srceddn srceline srcemem subtitle subtitle_orig sumhelppanel title title_org toptitle toptitle_orig

Type=PC: Program calls

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	address address64 akm akm_key amode asid at auditconcern auditpriority authreq collect_datetime complex [content | contents] [description | sft_description] ek ekm ekm_key entry et_asid et_connects et_jobname et_system ex jobname key length lx lx_asid_cnt lx_conn_asid lx_conn_jobname lx_dormant lx_ownr_asid lx_ownr_jobname lx_seqnum lx_system lx_table_cnt mode_sup module offset parm_address parm_key parm_subpool parm_where parm1_address parm1_at parm1_key parm1_subpool parm1_where parm2_address parm2_at parm2_key parm2_subpool parm2_where pc pc_type pkm program scan_instr scan_string scan_svc sft_description sft_index space_switch state subpool system where

Type=PPT: Program properties table

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	`auditconcern auditpriority bypass collect_datetime complex default honor_iefusi_region key nodsi noncancel nonswap priv program systask system ver`

Type=RACF: RACF profiles

Note: Not all aliases are listed; neither are some less preferred fields.

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			`auditconcern cfdtype cffirst cfhelp cflist cfmixed cfmnval cfmxlen cfmxval cfother class complex cscnt cskey cstype csvalue custom_data db digtcert_label hexkey inrange keyfrom [ key | profile ] profile_used proflen rba rcvt_racflevel searchkey segment ver`

BASE segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**`All classes`**
■	■			`authdate ckgauth`[3] `ckgauthor ckgchgdate ckgevents`[3] `ckgexpiry ckgmulti ckgother`[3] `ckgrefresh ckgrequest ckgstatus cmdsact`[3] `cmdsexec`[3] `cmdsinact`[3] `cmdspend`[3] `creadate defdate fldcnt fldflag fldname fldvalue instdata owner uacc usr usrcnt userdata`[3] `usrdata version`

USER

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			(no)adsp any_cert[3] any_clauth[3] any_group_soa[3] any_link[3] (no)auditor auditpriority audits author category certct certlabl certname certpubk certseqn certsjdn cgauthda cgauthor cgcreadt cgdefdat cgflag1 cgflag2 cgflag3 cgflag4 cgflag5 cggrpaud cggrpct cggrpnm cginitct cgljdate cgljtime cgnotuac cgowner cgresmdt cgrevkdt cguacc clcnt clname congrpct congrpnm connect connects cngschedule dfltgrp dmapct dmaplabl dmapname entype flag1 flag2 flag3 flag4 flag5 flag6 flag7 flag8 flag9 fldcnt fldflag fldname fldvalue (no)grpacc (no)grpadsp (no)groupauditor (no)groupgrpacc (no)groupoperations (no)grouprevoke (no)groupspecial has_password has_phrase has_pphenv has_pwdenv is_grpaudit is_grpoper is_grpspec profile last_connect_date ljdate ljtime ljdate ljtime logdays logtime magstrip modelnam name nmapct nmaplabl nmapname numctgy (no)oidcard oldphr oldphrnm oldphrnm oldpwd oldpwdnm (no)operations (no)operparm passasis passdate passint passint_effective (no)password password_expired password_expire_date pgmrname phrase phrase_expired phrase_expire_date phrcnt phrdate phrgen pphenv (no)protected pwdcnt pwdenv pwdgen pwhashed raclink racmap_registry (no)restricted resumedt (no)revoke revokect revokedt revoke_inactive seclabel seclevel (no)special tucnt tudata tukey uaudit usrflg usrnm

GROUP

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			aclcnt acscnt acscnt anysupgroup author connect connect_count connects depth entype initcnt memberclass memberkey modelnam notrmuac subgrpct subgrpnm supgroup (no)termuacc treeline (no)universal unvflg useracs userid usrflg usrnm

DATASET

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			acl acl_alter[3] aclcnt acl_control[3] acl_execute[3] acl_none[3] acl_oper[3] acl_read[3] acl_update[3] acl2cnt acl2var acsaltr acscnt acscntl acsread acsupdt audit auditf auditlvl auditqf auditqs audits author category connect_count devtyp devtypx discrete dsn dstype entype (no)erase filter flag1 fully_qualified_generic gaudit gauditf gauditlvl gauditqf gauditqs gaudits generic groupdsn groupnm lchgdat level lrefdat (no)model notify numctgy pacscnt proftype progacs program qual retpd resowner retpd seclabel seclevel (no)tapedsn univacs user2acs useracs userdsn userid usrflg usrnm volcnt volser volser_key volume (non)vsam (no)warning

GENERAL

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			acl aclcnt acl2acc acl2acnt acl2cnt acl2name acl2rsvd acl2uid acl_alter[3] acl_control[3] acl_execute[3] acl_none[3] acl_oper[3] acl_read[3] acl_update[3] acsaltr acscnt acscntl acsread acsupdt appldata audit auditf auditlvl auditqf auditqs audits author category certificate_id certificate_trusted clastype classtype didct didlabl didrname diduser digtring_userid discrete entype filter_issuerdn filter_subjectdn filterct fltrlabl fltrname fltrstat fltruser gaudit gauditqf gauditqs gauditf gauditlvl gaudits generic lchgdat level logdays logtime logzone lrefdat maxfail memcnt memlst ndslink_userid notify numctgy pads proftype qual racdhdr racldsp raclhdr resflg retpd seclabel seclevel sentcnt sesskey (no)singleds slsfail slsflags tvtoc tvtoccnt tvtoccrd tvtocdsn tvtocind tvtocrds tvtocseq tvtocvol useracs userid usrflg usrnm olcnt volser (no)warning

[3]established by a **DEFINE** statement in sample member C2RXDEF1.

CDTINFO segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**CDT**
■	■			cdtmembr cdtoper cdtother cdtposit cdtprfal cdtracl cdtsigl cdtslreq cdtuacc class_equalmac class_raclist_allowed class_raclreq class_rvrsmax class_syn1alp class_syn1nat class_syn1num class_syn1spe class_synralp class_synrnat class_synrnum class_synrspe

CERTDATA segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**DIGTCERT, DIGTRING**
■	■			cert certct certdflt certend certificate_alt_domain certificate_alt_email certificate_alt_ip certificate_alt_uri certificate_issuer_full certificate_keyusage certificate_serial certificate_subject certlabl certlser certname certprvk certprvs certprvt certsjdn certstrt certusag label_in_pkds label_in_tkds ringct ringname ringseqn

CFDEF segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**CFIELD**
■	■			ffdtype cffirst cflist cfmixed cfmnval cfmxlen cfmxval cfother

CICS segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**USER**
■	■			cics_rslkey cics_tslkey opclass opclassn opident opprty rslkey rslkeyn timeout tslkey tslkeyn xrfsoff

CSDATA segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**USER, GROUP**
				cscnt cstype cskey csvalue

DCE segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**USER**
■	■			uuid dcename homecell homeuuid dceflags dpasswds dceencry

DFP segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**USER, GROUP**
■	■			**DATASET**
■	■			Resowner

DLFDATA segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**DLFCLASS**
■	■			jobnames jobnmcnt retain

EIM segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**USER, FACILITY, LDAPBIND**
■	■			domaindn kerbregistry ldapprof localreg options x509registry

ICSF segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**CSFKEYS, GCSFKEYS, XCSFKEY, GXCSFKEY**
■	■			asymusage symexportcerts csfsclct symcpacfwrap symexportable symexportkeys csfsklct

ICTX segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**LDAPBIND**
■	■			domap maptimeo mapreq usemap

KERB segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**USER + REALM**
■	■			curkey curkeyv deftktlf encrypt enctype kerbname keyfrom maxtktlf mintktlf prevkey prevkeyv salt

LANGUAGE segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**USER**
■	■			sname

NDS segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**USER**
■	■			consname ctl domains domainsn ic msgrecvr ngmfadmin ngmfvspn opclass opclassn

NETVIEW segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**USER**
■	■			consname ctl domains domainsn ic msgrecvr ngmfadmin ngmfvspn opclass opclassn

OMVS segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**USER**
■	■			assize assizemax cputime cputimemax fileproc fileprocmax home memlimit mmaparea mmapareamax procuser procusermax program shmemmax threads threadsmax uid
■	■			**GROUP**
■	■			gid

OPERPARM segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**USER**

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			operaltg operauth operauto opercmds operdom operhc operint operkey operlevl operlogc opermcnt opermfrm opermgid opermon opermscp operrout operstor operud operunkn

OVM segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**USER**
■	■			home program uid fsroot
■	■			**GROUP**
■	■			gid

PROXY segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**USER, GENERAL**
■	■			binddn bindpw bindpwky ldaphost

SESSION segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**APPCLU**
■	■			convsec maxfail sentcnt sentflct sentity sesskey slsfail slsflags sskey

SIGVER segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**PROGRAM**
■	■			failload sigaudit sigreuired

SSIGNON segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**PTKTDATA, KEYSMSTR**
■	■			Sskey

STDATA segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**STARTED**
■	■			flagpriv flagtrac flagtrus stgroup stuser

SVFMR segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**SYSMVIEW**
■	■			parmn scriptn

TME segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**GROUP, DATASET, GENERAL** rolen roles
■	■			rolen roles
■	■			**ROLE**
■	■			childn children groupn groups parent resn resource rolen roles

TSO segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**USER**
■	■			taccnt tcommand tcons tdest thclass tjclass tlproc tlsize tmclass tmsize toption tperform trba tsclass tsoslabl tudata tunit tupt

WORKATTR segment

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			**USER**
■	■			waaccnt waaddr1 waaddr2 waaddr3 waaddr4 wabldg wadept waname waroom

Type=RACF_ACCESS: Connects and permits

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■				access_count_suc access_count_unk access_count_vio
■	■			access access_firstuse access_intent_max_suc access_intent_min_vio access_lastuse access_reduced class complex generic id member_class member_key merged_access_reduced profile proftype qualified_resource raclist_merge resource resource_location volser

Type=RACF_ACCESS_ID: User IDs and groups

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■				access_count_suc access_count_unk access_count_vio
■	■			access_firstuse access_lastuse class id

Type=REPORT_AC1: Authorized module protection

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■		auth collect_datetime complex dsn hidden_linklist hidden_lpalist linklist lpalist lpa_type member module order pageby profile program program_type stamp system uacc ver volser

Type=REPORT_NONDEFAULT: RACF profiles changed from default

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			access complex id key mark order pageby proftype program qual reason resource_location stamp uacc volser

Type=REPORT_OUTOFGROUP: RACF profiles accessible outside group

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			access complex id key mark order pageby proftype program qual reason resource_location stamp uacc volser

Type=REPORT_PADS: Programs giving access to data sets

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			auth collect_datetime complex dsn hidden_linklist hidden_lpalist linklist lpalist lpa_type member module order pageby profile program program_type stamp system uacc volser

Type=REPORT_PROFILE: RACF profiles and data sets

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			access auditf auditlvl audits [class | c] complex erase id key order pageby proftype resource_location stamp uacc volser when

Type=REPORT_REDUNDANCY: RACF profile redundancy

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			access auditf auditlvl audits complex erase id key mark order owner pageby proftype program qual reason resource_location stamp uacc volser

Type=REPORT_SCOPE: RACF profiles and data sets in scope

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			access access_via_when class complex id key order pageby proftype resource_location stamp via volser when

Type=REPORT_SENSITIVE: Sensitive data sets by profile

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■		access auditconcern auditf auditlvl auditpriority audits complex erase id key mark order owner pageby proftype profile program reason resource_location senstype stamp uacc ver volser

Type=REPORT_STC: Started procedure protection

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
		■		acf2_access acf2_is_lid acf2_jobfrom acf2_lid acf2_maint acf2_musass acf2_non_cncl acf2_ppgm acf2_readall acf2_stc acf2_tape_blp acf2_unscoped_account acf2_unscoped_audit acf2_unscoped_security
■	■	■		collect_datetime complex concat dsn flags hidden isfp_date ispf_userid last_change last_change_userid order pageby procname stamp subsys system uacc userid ver volser
■	■			auditor group group_dlftgrp ichrin03 operations privileged profile protected special trusted

Type=RESOURCE

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	class collect_datetime complex racf_acl racf_auditf racf_audits racf_class racf_global_access racf_idstar_access racf_profile racf_uacc resource resource_location system

Type=ROUTER: SAF router table

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			action auditconcern auditpriority class collect_datetime complex incdt [order | org] reqstor subsys system

Type=RRNG: Database range table

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			collect_datetime complex db key keyhex [order | org] seqno system

Type=RRSFNODE: RRSF configuration information

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			address appc_luname appc_modename appc_tpname collect_datetime complex description is_local is_main local_node node_type portnum protocol system target_complex target_node target_state target_sysname target_system userid workspace_dataclas workspace_filesize workspace_mgmtclas workspace_prefix workspace_qualifier workspace_storclas workspace_volume

Type=SENSDSN: Sensitive data set names

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
		■		acf2_acl acf2_rule_entry acf2_trusted#
	■	■	■	apf apflist auditconcern auditpriority box_serial collect_datetime complex [dataset | dsn] erase linklist lnkauth lpalist mounted resource_location risk sensitivity sysplex system ver volser_or_sms volume

Type=SETROPTS: System-wide options as stored on disk

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			adsp aim_db_stage applaudit audit_group audit_user batchallracf catdsns cmdviol compatmode complex dasdvol dlogopt earlyverify egn eos eraseonscratch eraseseclevel genericowner genown grplist history inactive initstats interval kerblvl listgrp lvl1pref minchange mixedcase mlactive mlquiet mls mlstable modelgdg modelgroup modeluser njeuserid noaddcreator operaudit primary_language program protectall pwdhistory pwdinterval pwdrevoke pwdrule1 pwdrule2 pwdrule3 pwdrule4 pwdrule5 pwdrule6 pwdrule7 pwdrule8 pwdwarning racf_mlfsobj racf_mlipcobj racf_mlnames racf_seclbysystem racflevel racflvl realdsn retpd revoke rvarystatuspwset rvaryswitchpwset saudit seclabelaudit seclabelcontrol seclevelaudit seclevelerase secondary_language sessint sessioninterval setradsp systemadsp tapedsn tapevol terminal termuacc undefineduser warning whenprogram xbmallracf

Type=SETROPTS_CLASS: Class settings as stored on disk

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			active audit auditconcern auditpriority clauth complex default_class description gen gencmd generic genlist glb global logopt posit protect raclist stats

Type=SMF: SMF records

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
		■		acf2_access acf2_authority acf2_changes acf2_descriptor acf2_event acf2_eventtype acf2_major acf2_minor acf2_newp_rc2 acf2_nextkey acf2_pkis_func acf2_rc acf2_rmrc acf2_role acf2_rule_entry acf2_rule_header acf2_rulekey acf2_searchkey acf2_source acf2_submitter acf2_subtype acf2_uid
	■	■	■	box_serial catalog cics_monitor_class cics_performance_data cics_specific_appl cics_term cics_ttype class collect_datetime [compcode | completion_code] complex [compstat | completion_status] cssmtp_badspooldisp cssmtp_ckpfile cssmtp_checkpointing cssmtp_cn_esmtp cssmtp_cn_fips140 cssmtp_cn_local_ip cssmtp_cn_local_port cssmtp_cn_remote_ip cssmtp_cn_remote_port cssmtp_cn_tls_ssl_proto cssmtp_cn_tlsnc cssmtp_config_file cssmtp_console cssmtp_datetime cssmtp_dead_letter_actn cssmtp_dead_letter_dir cssmtp_domain_name cssmtp_extwrtname cssmtp_hostname cssmtp_logfile cssmtp_loglevel cssmtp_mail_admin_mbox cssmtp_mh_cmd_error cssmtp_mh_date cssmtp_mh_error_text cssmtp_mh_from cssmtp_mh_msgid cssmtp_mh_rcpt_reply cssmtp_mh_reply_to_error cssmtp_mh_subject cssmtp_mh_to cssmtp_report cssmtp_rtn_to_mail_from cssmtp_smf119 cssmtp_stack cssmtp_ts_dstip cssmtp_ts_index cssmtp_ts_name cssmtp_ts_port cssmtp_ts_secure cssmtp_ts_type cssmtp_useid cssmtp_userexit [dataset | dsname | dsn] date datetime db2_appl_userid db2_authid db2_authid_checked db2_command db2_connection db2_context db2_enduser_userid db2_object db2_object_type db2_original_operator db2_plan db2_role db2_secauthid db2_sqlid decompressed_record dstip dstport elapsed esm explanation fieldval file

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	ftp_anonym_hfs_dir_mode ftp_anonym_hfs_info ftp_anonym_level ftp_anonym_login_msg ftp_anonym_mvs_info ftp_anonym_password_set ftp_anonym_surrogate ftp_anonym_user ftp_anonym_ftp_logging ftp_asid ftp_auto_mount ftp_auto_recall ftp_auto_tape_mount ftp_banner ftp_ciphersuite ftp_dataclass ftp_datetime_started ftp_db2 ftp_db2plan ftp_dcbdsn ftp_debug_on_site ftp_dest_node ftp_dest_user ftp_directory_mode ftp_dsn_ftp_data ftp_dsn_tcpip_data ftp_ds_wait_time ftp_dump_on_site ftp_email_addr_check ftp_env_bpx_jobname ftp_krb5_server_keytab ftp_env_resolver_config ftp_extensions ftp_filetype ftp_ipv4_poe_class ftp_keep_alive ftp_logging ftp_hfs_info ftp_inactive ftp_ispf_stats ftp_jes_get_by_dsn ftp_jes_interface_level ftp_jobname ftp_keyring ftp_login_msg ftp_mgmtclass ftp_migratevol ftp_mvs_info ftp_mvs_url_key ftp_passive_noredir ftp_passive_data_port_hi ftp_passive_data_port_lo ftp_passphrase ftp_port ftp_port_cmd_accept ftp_port_cmd_noredir ftp_port_cmd_nolowports ftp_reply_security_level ftp_rest_put ftp_secure_ctrl_conn ftp_secure_data_conn ftp_secure_ftp_required ftp_secure_implicit_zos ftp_secure_login ftp_secure_pswd_req ftp_secure_pswd_kerb_req ftp_secure_pbsz ftp_smf118_exit ftp_smf118_jes ftp_smf118_sql ftp_smf118_std ftp_smf118_subtype ftp_smf118_subtype_appe ftp_smf118_subtype_del ftp_smf118_subtype_logn ftp_smf118_subtype_ren ftp_smf118_subtype_retr ftp_smf118_subtype_stor ftp_smf119 ftp_smf119_jes ftp_smf119_sql ftp_smf119_subtype_appe ftp_smf119_subtype_dcfg ftp_smf119_subtype_del ftp_smf119_subtype_logn ftp_smf119_subtype_ren ftp_smf119_subtype_retr ftp_smf119_subtype_stor ftp_startdirectory_mvs ftp_storclass ftp_tlsmechanism_attls ftp_tls_port ftp_tls_rfc_level ftp_tls_timeout ftp_umask ftp_verify_user group hostname intent

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	ip_autolog_jobname ip_autolog_options ip_autolog_parmstring ip_autolog_procname ip_autolog_wait ip_config_changes ip_datetime_started ip_dsnmem ip_dyn_xcf_sourcevipaint ip_dynamicxcf_intfid ip_dynamicxcf_ip ip_dynamicxcf_ipmask ip_dynamicxcf_ip6 ip_dynamicxcf_pfxlen ip_dynamicxcf_pfxlen6 ip_dynamicxcf_secclass ip_dynamicxcf_secclass6 ip_globalconf_iqdvlan ip_globalconf_mlschkterm ip_globalconf_xcfgrpid ip_interf_sourcevipaint ip_interf_vmac_address ip_interface_assoc_name ip_interface_chpid ip_interface_index ip_interface_interface ip_interface_intfid ip_interface_ip ip_interface_ipmask ip_interface_options ip_interface_pfxlen ip_interface_secclass ip_interface_type ip_interface_vlan_id ip_ipconfig ip_ipconfig_ipsecurity ip_ipconfig6 ip_ipconfig6_ipsecurity ip_ipsec_dvipsec ip_ipsec_logenable ip_ipsec_logimplicit ip_last_change_datetime ip_netaccess_inbound ip_netaccess_ip ip_netaccess_ipmask ip_netaccess_outbound ip_netaccess_pfxlen ip_netaccess_resname ip_netaccess_resource ip_netmon_pkttrcservice ip_netmon_smf_ipsecurity ip_netmon_smf_profile ip_netmon_smfservice ip_netmon_tcpconn_minl ip_netmon_tcpconnservice ip_port_begin_port ip_port_bind ip_port_end_port ip_port_jobname ip_port_options ip_port_port_count ip_port_port_use ip_port_portrange ip_port_protocol ip_port_resname ip_port_resource ip_port_unrsv ip_route_dstip ip_route_interface ip_route_interface_index ip_route_ipmask ip_route_nexthop_ip ip_route_pfxlen ip_route_replaceable ip_route_replaced ip_rule_code ip_rule_dstip ip_rule_dstipmask ip_rule_dstpfxlen ip_rule_dstport ip_rule_log ip_rule_protocol ip_rule_routing ip_rule_secclass ip_rule_srcip ip_rule_srcipmask ip_rule_srcpfxlen ip_rule_srcport ip_rule_type ip_saconf_snmp_pwdefault ip_saconfig_osasf_port ip_saconfig_snmp_port ip_smf119_ftpclient ip_smf119_ifstat ip_smf119_ipsecurity ip_smf119_portstat ip_smf119_tcpinit ip_smf119_tcpipstack ip_smf119_tcpipstat ip_smf119_tcpterm ip_smf119_tn3270client ip_smf119_udpterm ip_sysplex_group ip_tcp_restrictlowports ip_tcpstacksourcevipa ip_tcpstacksourcevipa6 ip_udp_restrictlowports ip_vipa_active ip_vipa_change_cancelled ip_vipa_interface ip_vipa_ip ip_vipa_ipmask ip_vipa_options ip_vipa_pfxlen ip_vipa_rank ip_vipa_resname ip_vipa_resource ip_vipa_type
	■	■	■	jobclass jobelapsed jobid jobname jobtag key_label key_label_encoding keyring_name logstr member member_alias member_oldname month [monthday | day] msgid name omcmd_allowed omcmd_name omcmd_text omcmd_type owner priority procname program r_logdata r_logrecord recno record recorddesc [recordlength | record_length] resource seclabel security_event sig_date sig_entity_dn sig_expiration sig_program_loaded sig_root_dn sig_time smfdd smfuser smfuserid smf_field smf_section specialtype srchost srcip srcport stepname subrecno subrecord subsys subsys_type subtype sysplex system systype terminal time transaction tsocmd tsocmdcnt type unittype unix_filetype unix_pathname [user | userid] [volser | volume] volser_or_sms vtamnet_is_remote vtamnetid weekday year

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■			access action appl auth_user_hostname auth_user_name auth_user_oid auth_user_regname authority certificate_issuer certificate_label certificate_serial certificate_subject [descriptor | desc] event event_datetime eventdesc eventqual ip_ipa6_interface_index ip_ipa6_interface_name ip_ipa6_IP ip_ipa6_pfxlen ip_netaccess_racf_prof ip_port_racf_profile ip_vipa_racf_profile ldap_client_secl ldap_conn_id ldap_entry_nm pkcs11_token product product_fmid program profile qual r_access r_action r_event r_intent r_mgmt_attr r_mgmt_cmd r_mgmt_type r_resource r_result r_rolecheck r_rolegrant r_user [racfauth | authority] racfcmd racfcmd_auth racfcmd_effective racfcmd_group racfcmd_keywords racfcmd_keywords_eff racfcmd_owner racfcmd_user racf_link_audit racf_link_event racf_section reason relocate rtoken rtoken_flags type unittype unix_access_allowed unix_access_filename unix_access_intent unix_access_origin unix_access_pathname unix_access_used unix_filename unix_function unix_program utoken utoken_flags utoken_poe utoken_poeclass utoken_poe_network utoken_session [utoken_sgroup | utoken_sgrp] utoken_snode [utoken_suser | utoken_susr] utoken_xnode
			■	tss_access tss_access_raw tss_descriptor tss_detail_reason tss_event tss_eventdesc tss_intent tss_intent_raw tss_rescode

Type=SMFOPT: SMF subsystems

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	active [actrec | wrtrec] address auditconcern auditpriority collect_datetime complex concern [desc | description] detail [exitcnt | exitcount] [inactrec | suprec] interval [partcnt | partcount] program rec record smfinterval subsys summary [supcnt | supcount] suprec system ver [wrtcnt | wrtcount] wrtrec

Type=SPT: RACF started procedure table

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			[attr | auth] collect_datetime complex group [order | org] privileged procname system trusted [user | userid]

Type=SUBSYS: MVS subsystems

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	ardr auditconcern auditpriority collect_datetime complex concern description fib function function_address function_amode function_at function_content function_key function_length function_module function_no
	■	■	■	function_offset function_program function_scanins function_scanstr function_subpool function_where max_functions name [org | order] pss ssct_address ssct_key ssct_subpool ssct_where ssvt_address ssvt_key ssvt_subpool ssvt_where sus2_address sus2_contents sus2_key sus2_subpool sus2_where suse_address suse_contents suse_key suse_subpool suse_where system type

Type=SVC: Supervisor calls

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	address amode appl at [auditconcern | concern] auditpriority caller_address caller_at caller_where collect_datetime complex contents curr_address curr_amode curr_apf curr_at curr_attr curr_contents curr_esr curr_key curr_length curr_lock curr_module curr_offset curr_program curr_result curr_same_as curr_scan_instr curr_scan_string curr_scan_svc curr_subpool curr_type curr_where esrno exp_apf exp_esr exp_program exp_type function index indexcount key length module offset old_apf old_attr old_esr old_lock old_type program result same_as scan_instr scan_string subpool svcno system update_count update_current update_date update_suffix where

Type=SYSTEM: System-wide options

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
		■		acf2_bkup_cpuid acf2_bkup_string acf2_bkup_time acf2_bkup_workunit acf2_blppgm acf2_eras_eraseall acf2_eras_nonvsam acf2_eras_process acf2_eras_seclevel acf2_eras_seclevl acf2_eras_vols acf2_eras_vsam acf2_linklst acf2_logpgm acf2_maint acf2_mlsopts_mlactive acf2_mlsopts_mlfsobj acf2_mlsopts_mlsecaud acf2_mlsopts_mlslblrq acf2_mlsopts_mlipcobj acf2_mlsopts_mlsecbys acf2_mlsopts_mlwrite acf2_mlsopts_mode acf2_opts_access acf2_opts_blplog acf2_opts_cmdrec acf2_opts_cputime acf2_opts_date acf2_opts_dftlid acf2_opts_dftstcid acf2_opts_icsf acf2_opts_infolist acf2_opts_jobck act2_opts_lds acf2_opts_maxvio acf2_opts_mode acf2_opts_namehide acf2_opts_notify acf2_opts_ptkresck acf2_opts_rptscope acf2_opts_stampsmf acf2_opts_stc acf2_opts_tapedsn acf2_opts_uads acf2_opts_vtamopen acf2_opts_wrndays acf2_pds acf2_ppgm acf2_pswd_clearvio acf2_pswd_hist_effective acf2_pswd_maxtry acf2_pswd_minpswd acf2_pswd_passlmt acf2_pswd_pswdalph acf2_pswd_pswdalt acf2_pswd_pswdch acf2_pswd_pswdenct acf2_pswd_pswdfrc acf2_pswd_pswdhst acf2_pswd_pswdjes acf2_pswd_pswdlc acf2_pswd_pswdlid acf2_pswd_pswdmax acf2_pswd_pswdmaxl acf2_pswd_pswdmin acf2_pswd_pswdmixd acf2_pswd_pswdname acf2_pswd_pswdnmic acf2_pswd_pswdnum acf2_pswd_pswdpair acf2_pswd_pswdplid acf2_pswd_pswdplst acf2_pswd_pswdreq acf2_pswd_pswdrsv acf2_pwsd_pwsdsim acf2_pswd_pswdsplt acf2_pswd_pswduc acf2_pswd_pswdvfy acf2_pswd_pswdvowl acf2_pswd_pswdxtr acf2_pwsd_pswnage acf2_pswd_pswxhist acf2_pswd_pswxhst# acf2_pswd_warndays acf2_pwphrase_allow acf2_pwphrase_alpha acf2_pwphrase_cmd_chg acf2_pwphrase_extract acf2_pwphrase_history acf2_pwphrase_lid acf2_pwphrase_maxdays acf2_pwphrase_maxlen acf2_pwphrase_mindays acf2_pwphrase_minlen acf2_pwphrase_minword acf2_pwphrase_numeric acf2_pwphrase_repchar acf2_pwphrase_special acf2_pwphrase_speclist acf2_pwphrase_temp_age acf2_pwphrase_warndays acf2_resvols acf2_ruleopts_$nosort acf2_ruleopts_central acf2_ruleopts_change acf2_ruleopts_compdyn acf2_ruleopts_decomp acf2_ruleopts_rulelong acf2_ruleopts_volrule acf2_secvols acf2_tso_logonck acf2_tso_pwphrase acf2_unixopts_dftgroup acf2_unixopts_dftuser safhfmod

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	ca1_batch ca1_create ca1_dse ca1_dsnb_effective ca1_forndsn ca1_func ca1_oceov ca1_pswd ca1_undef_fail ca1_ysvc ckrsite_class collectdate collect_datetime complex con_amrf con_cmddelim con_consol con_dflt_rout con_hcpy_cmdlvl con_hcpy_devnum con_hcpy_rout con_logon_auto con_logon_req con_mlim con_mon_dsname con_mon_space con_mpflst con_msg_loss con_pfktab con_rlim con_uexit conftxt cpu_model_byte cpu_model_name cpu_serial cpu_type date_offset devsup_tapeauthdsn devsup_tapeauthf1 devsup_tapeauthrc4 devsup_tapeauthrc8 [dfplevel | dfplvl] dms_secure_parmlib dmssecurvol esmlevel esmlvl esmname hsmbackupprefix hsmjobname [hsmlevel | hsmlvl] hsmmigrateprefix hsmsmfrecno hsmtapesecurity hsmtapeselvol hwname ikjtso iodf_config_date iodf_config_id iodf_config_time ipldate ipldev iplparm_alloc iplparm_apf iplparm_autor iplparm_axr iplparm_catalog iplparm_clock iplparm_clpa iplparm_cmb iplparm_cmd iplparm_con iplparm_couple iplparm_csa iplparm_cscbloc iplparm_cvio iplparm_devsup iplparm_diag iplparm_dump iplparm_duplex iplparm_effective iplparm_exit iplparm_fix iplparm_grs iplparm_grscnf iplparm_grsrnl iplparm_hvcommon iplparm_hvshare iplparm_ics iplparm_ikjtso iplparm_ilmlib iplparm_ilmmode iplparm_ios iplparm_ips iplparm_ixgcnf iplparm_lfarea iplparm_lnk iplparm_lnkauth iplparm_load iplparm_logcls iplparm_loglmt iplparm_logrec iplparm_lpa iplparm_maxcad iplparm_maxuser iplparm_mlpa [iplparm_mstrjcl | iplparm_mstjcl] [iplparm_mstrjcl_linklib | iplparm_mstjcl_linklib] iplparm_nonvio iplparm_nsyslx iplparm_omvs iplparm_operator iplparm_opi iplparm_opt iplparm_page_oper iplparm_page_sys iplparm_pagtotl iplparm_pak iplparm_parmlib_load iplparm_plexcfg iplparm_prescpu iplparm_prod iplparm_prog iplparm_rde iplparm_real iplparm_rer iplparm_rsu iplparm_rsvnonr iplparm_rsvstrt iplparm_rtls iplparm_sch iplparm_smf iplparm_sms iplparm_sqa iplparm_ssn iplparm_svc iplparm_swap iplparm_sysname iplparm_sysp iplparm_uni iplparm_val iplparm_viodsn iplparm_vrregn iplparm_zz ipltime iplvol [jes2level | jes2lvl] [jes2node | node | nodename] jobclass_auth_owner jobclass_auth_submitter jobstepcat lnkauth loadparm lpar memlimit mlactive mlalevel mpf_noentry_auto mpf_noentry_sup msglogname msgprotect mt_size mvsiocid mvslevel mvslvl netid oslvl osname osvendor [pcmode | program_mode] refrprot [rmflevel | rmflvl] securpass_smf_log securpass_smf_recno smf_flood_control smf_floodpol smf17temp [smf23interval | smfstatus] smfactive smfds_active smfds_blocks smfds_filled smfds_name smfds_size smfds_vol smfdumpabndretry smfjwt [smflastdshalt | lastdshalt] smfls_active smfls_being_cleaned smfls_buffersize smfls_connected smfls_default smfls_name smfls_summary smfls_writetod [smfmaxdorm | maxdorm] [smfnobuffshalt | nobuffshalt] smfprm smfrecording [smslevel | smslvl] sysclone syslog_active syslog_class syslog_commands syslog_limit sysname syspercent sysplex system tcpipproc tcpipvers tempdsformat_unique timezone tsoacbpw tsoconftxt [tsolevel | tsolvl] tsoreconlim tsousermax tsousers [vmlevel | vmlvl] ver vmsystem vmuserid [vtamlevel | vtamlvl] [vtamnetid | netid]
■	■			[adsp | setradsp | systemadsp] aim_db_stage aim_smf_recno applaudit audit_group audit_user batchallracf catdsns cmdviol compatmode dasdvol dlogopt dmsracfalwz dmsracfbkup dmsracfdvol dmsracfnewn dmsracfpred dmsracfproc dmsracfsupp dmsracfusid dynamic_cdt earlyverify egn eimregistry [eraseonscratch | eos] [eraseseclevel | seclevelerase] [force24 | below] genanc_jobcount genanc_jobname genanc_system_count [genericowner | genown] [grplist | listgrp] [history | pwdhistory] hsmerase hsmmultitapevol [hsmprofilebackup | hsmbackupprofile] hsmracfind inactive initstats [interval | pwdinterval] kerblvl lvl1pref minchange mixedcase mlquiet mls mlstable modelgdg modelgroup modeluser njeuserid noaddcreator nodup operaudit primary_language protectall pwdrule1 pwdrule2 pwdrule3 pwdrule4 pwdrule5 pwdrule6 pwdrule7 pwdrule8 racfact racf_autoappl racf_autodirect racf_autopwd racf_jesnode racfdblevel [racflevel | racflvl] racflocalnode racf_mlfsobj racf_mlipcobj racf_mlnames racf_pwsync racf_seclbysystem realdsn retpd [revoke | pwdrevoke] rvarystatuspwset rvaryswitchpwset saudit seclabelaudit seclabelcontrol seclevelaudit secondary_language [sessioninterval | sessint] tapedsn tapevol terminal termuacc undefineduser [warning | pwdwarning] [whenprogram | program] xbmallracf
	■	■	■	con_monitor iplparm_cee iplparm_drmode iplparm_prescpu

Type=TEMPLATE: RACF database templates

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			aim_alias alias command_parm command_parm_format complex date3 default description ebcdic_alias entity field first flag format group has_dpi has_template header help hidden id length masked maxlen maxval minval mixed other pad repeated segment size sorted stamp statistic vlf

Type=TRUSTED: Users that can bypass security

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
		■		acf2_rule acf2_rule_entry
	■	■		access auditconcern auditpriority class collect_datetime complex concern resource resource_location risk sensitivity system userid userid_complex userid_privilege via [volser | volume]
	■			racf_class racf_profile

Type=TYPE: Newlist type definitions

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	abbrev2 detailhelppanel helppanel newlist_tag newlist_type toptitle toptitle_orig

Type=UNIX: UNIX System Services File System

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	abs_pathname abs_pathname_select attr auditflags auditflags_auditor auditflags_user auditid collect_datetime complex depth dev directory_default_acl dirname extattr extended_acl external_link file_default_acl filename fs_complex fs_dsn fs_mountpoint fs_rdwr fs_security fs_serial fs_setuid fs_system [fs_volser | fs_volume] gid group home_of inode link_count link_target owner physical_attr physical_extattr rel_pathname seclabel symbolic_link symlink sysplex system type uid unix_acl unix_default_acl unix_fdefault_acl
	■	■	■	[auditconcern | concern] auditpriority

Type=VM_DEV: VM devices

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			auditconcern auditpriority collect_datetime complex device device_class device_size racf_acl racf_global_access racf_idstar_access racf_profile racf_uacc read_only real_device real_volume resource status system userid

See the IBM Security zSecure Manager for RACF z/VM documentation for a detailed list of the fields that are supported for the VM_DEV NEWLIST.

Type=VM_MDISK: Minidisks

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■			acigroup auditconcern auditpriority collect_datetime complex device device_arch device_type end full_pack glbldsk local mdisk_type mode mode_suffix mwritepw racf_acl racf_global_access racf_idstar_access racf_profile racf_uacc readpw real_device real_volume resource sensitivity size size_byte start system tdisk vdisk vmuserid volume writepw

See the IBM Security zSecure Manager for RACF z/VM documentation for a detailed list of the fields that are supported for the VM_MDISK NEWLIST.

Type=VSM: Virtual storage

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
	■	■	■	[auditconcern | concern] auditpriority collect_datetime complex end filled length start start64 system type

Type=ZSECNODE: zSecure server nodes

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■	■	■	■	cknserve_level cknserve_vrm default_complex hwname ipaddress ipname ipport last_connect last_connect_attempt lparname smfid sysclone sysname sysplex vmuserid zsec_active zsec_local zsec_preferred zsec_verified zsecnode zsecsys
■	■			rrsf_active rrsf_defined rrsf_local rrsf_main rrsf_userid rrsfnode

Chapter 5. CKGRACF command syntax

The RACF Administrator can use the CKGRACF program to set up decentralized RACF administration with fine-grained controls. The decentralized RACF administrator can use the CKGRACF command to run or request certain specific functions.

General usage hints

CKGRACF can also be called as a TSO command in a system REXX environment.

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	*profile* can be	
■				*profile*	to uppercase
■				*'profile'*	to uppercase
■				*'profile'*C	as is
■				*'profile'*D	discrete
■				*'profile'*G	generic
■				*'profile'*X	hexadecimal

Alternatively, double-quoted and back-quoted specifications can be used instead of single-quoted ones.

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	*string* can be	
■				*string*	to uppercase
■				*'string'*	to uppercase
■				*'string'*C	as is
■				*'string'*X	hexadecimal

Alternatively, double and back quoted specifications can be used instead of single-quoted ones.

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	*num* can be:	
■				*num* decimal	
■				*'num'*F	decimal
■				*'num'*B	binary
■				*'num'*X	hexadecimal

Alternatively, double and back quoted specifications can be used instead of single-quoted ones.

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	date can be:
■				{ *DDMMMYYYY* | *DD-MMM-YY* | *DD/MMM/YY* | *DDMMMYYYY* | *DD-MMM-YYYY* | *DD/MMM/YYYY* |
■				*YYYY-MM-DD* | *YYYY/MM/DD* |
■				*YYDDD* | *YYY/DDD* | TODAY }

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	REASON keyword:
■				On all commands, except **LIST** and **SHOW**, can be up to 215 characters

Alternatively, double and back quoted specifications can be used instead of single-quoted ones.

zSecure Admin CKGRACF commands

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■				**ACCESS** *id class profile* [ASIS | DISCRETE | GENERIC (*type*)] [REASON (*reason*)]
■				**ALLOC** [ERRDD=*ddname*] [LICENSE=*dsn(member)*] [OUTDD=*ddname*] [TEXTPIPE=*n*]
■				**AUTHORITY** *class profile* [DEFAULT | DUAL | LIST | SINGLE | TRIPLE (*action*)] [REASON (*reason*)]
■				**CKGAUTH** *class profile* [LIST | DEFAULT | SINGLE | DUAL | TRIPLE] [REASON (*reason*)]

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■				**CMD** [REASON (*reason*)] [*DLM-delimiter*] { [AT *date1* | AFTER *len*] [FOR *len* | LEN *len* | UNTIL *date2*] } { ASK | REQUEST | SECOND [APPROVE | HOLD | DENY] | COMPLETE [APPROVE | HOLD | DENY] | WITHDRAW } { CONNECT | PERMIT | REMOVE } { EXECUTE { ADDGROUP | ADDSD | ADDUSER | ALTDSD | ALTGROUP | ALTUSER | CONNECT | DEFINE | DELDSD | DELETE | DELGROUP | DELUSER | HELP | LISTDSD | LISTGRP | LISTUSER | PASSWORD | PERMIT | RACDCERT | RACLINK | RACMAP | RALTER | RDEFINE | RDELETE | REMOVE | RLIST | SEARCH | SETROPTS } } *parameters* The normal RACF-syntax rules apply to the RACF component in the **CMD** command.
■				**COMMENT** [REASON (*reason*)]
■				**DEBUG** [ICHEINTY] [RACFMSG] [RACHECK] [SAFRC]
■				**FIELD** USER *userid* { LIST *field* | SET *field(value)*... | ADD *field(value)*... | DELETE *field[(value)]*... | REPLACE *field x*... with {field x}... } [REASON (*reason*)] ***field* can be:** BINDPW PASSDATE TUPT BINDPWKY PASSWORD FLAG7 PHRASE FLAG8 PHRDATE INTERVAL REVOKECT LJDATE SSKEY LJTIME SESSKEY PASSASIS TCOMMAND
■				**IMBED/INCLUDE** [DDNAME=*file* | FILE=*file* | MEMBER=*name* | MARGINS=(*nn,ll*) | MARGINS(*nn,ll*)]
■				**LIST** *class profile* [ALL | RACF | SCHEDULE | QUEUE | TAG [NOTERM] [NOPAGE]]
■				**PWCONVERT** *userid* [REASON (*reason*)]

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■				**QUESTION** *profile* [REASON (*reason*)] { SET { *qid question* PASSWORD (*answer*) } ... | VERIFY { *qid* PASSWORD (*answer*) } ... | LIST [*qid*] ... | DELETE [*qid*] ... }
■				**RDELETE** *class profile* [ASIS | DISCRETE | GENERIC] [*volser*] [REASON (*reason*)] **Note:** Class can be any RACF class except CONNECT.
■				**REFRESH** *class profile* [REASON (*reason*)]
■				**SHOW** { { CKRSITE | ZAP } | MYACCESS [ID *id*] [NOTERM] }
■				**SUPPRESS** MESSAGE=(*list*)
■				**USER** *userid* [[INTERVAL(*num*) | NOINTERVAL] [PWDEFAULT [DELETE | PASSWORD(*string*) | PROMPT]] [PWRESET | PWSET [PASSWORD(*string*) | PHRASE(*value*) | PROMPT | DEFAULT | NOPASSWORD | REVIOUS | RANDOM | CURRENT] [PWNOHIST] [PWNOEXIT] [PWNORULE] [EXPIRED | NONEXPIRED]] [SCHEDULE *schedule* { ENABLE | DISABLE | WIPE } [*start-date* | (*start-date:end-date*) | (*start-date,length*)] [REASON (*reason*)]] * [RESUME]] [ASK | REQUEST | SECOND [APPROVE | HOLD | DENY] | COMPLETE [APPROVE | HOLD | DENY] WITHDRAW] [REASON (*reason*)] *schedule* is up to 8 alphanumeric characters.
■				**USRDATA** *class-profile* {ADD [REASON (*reason*)] *index* (*data*) | DELETE [REASON (*reason*)] *index*[(*data*)] | LIST [REASON (*reason*)] *index* | REPLACE [REASON (*reason*)] *index* (*old-data,new-data*) | SET [REASON (*reason*)] *index* (*data*) } ... *index* is up to 8 alphanumeric characters. *data* can also be 'data' [/ *flag*]

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Command syntax
■				**WIPE** *class profile* { ALL | AUTHORITY | DEFAULTPW | INSTALLATION | QUEUE | RESERVED | SCHEDULE | UNDEFINED } ... [REASON (*reason*)]

Authority check overview

Command	Checks **CKG.CMD.****	Checks **CKG.SCP.****	Subject to multiple-authority controls	Extra authority checks	System Special required
ACCESS	Yes				
AUTHORITY	Yes				
CKGAUTH	Yes				
CMD EX	Yes				
CMD	Yes	if CKG.RAC.SCP.**	Yes	CKG.RAC.**	
COMMENT	Yes				
FIELD	Yes				
LIST	Yes	Yes			
PWCONVERT	Yes				Yes
QUESTION	Yes	if CKG.USRDATA.SCP.**		CKG.USRDATA.**	
RDELETE	Yes				Yes
REFRESH	Yes				
SHOW CKRSITE					
SHOW MYACCESS	Yes				
USER	Yes	Yes	Yes	CKG.SCHEDULE.**	
USRDATA	Yes	if CKG.USRDATA.SCP.**		CKG.USRDATA.**	
WIPE	Yes				

CMD authority checks

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Resource name that is checked	Access required
■				CKG.CMD.ACCESS.ALL	READ
■				CKG.CMD.AUTHORITY.*class*	READ for the LIST option UPDATE for all other options

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Resource name that is checked	Access required
■				CKG.CMD.CMD.{ASK|REQ|SEC|CMP}.{*racfcmd* | DEFINE|DELETE}	READ UPDATE
■				CKG.CMD.COMMENT	READ
■				CKG.CMD.FIELD.*field*	READ for the LIST option UPDATE for all other options
■				CKG.CMD.LIST	READ
■				CKG.CMD.PWCONVERT	UPDATE
■				CKG.CMD.QUESTION	READ for the LIST and VERIFY actions UPDATE for the SET and DELETE actions
■				CKG.CMD.RDELETE	UPDATE
■				CKG.CMD.REFRESH	UPDATE
■				CKG.CMD.SHOW.MYACCESS	READ
■				CKG.CMD.USER.{ASK|REQ|SEC|CMP}.{*subcmd* | PWDSET.*option*}	UPDATE
■				CKG.CMD.USRDATA	READ for the LIST option UPDATE for all other options
■				CKG.CMD.WIPE.{ALL | AUTHORITY | DEFAULTPW | INSTALLATION | QUEUE | RESERVED | SCHEDULE | UNDEFINED}	UPDATE

SCOPE

Access levels are similar to those levels at the command checks.

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Resource name that is checked
■				**ID for user**
■				CKG.{SCP | SCPASK}.ID.*userid.owner.dlftgrp*
■				**ID for Group**
■				CKG.{SCP | SCPASK}.ID.*groupid.owner*
■				**GroupTree-scope based on owner**
■				CKG.{SCP | SCPASK}.G.*groups*
■				CKG.{SCP | SCPASK}.U.*user.groups*

RAC

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Resource name that is checked
■				CKG.RAC.{OWN|ALL|SCP}.*class*. {*segment.field*|BASE.*class*|BASE.ACCESS.*access*|BASE.AUTH.*auth*|WHEN.*class*}

access can be READ, UPD, ALT, CTRL, NONE, or EXEC.

auth can be USE, CREATE, JOIN, or CONN.

SCHEDULE

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Resource name that is checked
■				CKG.SCHEDULE.*schedulename*

USER CATALOG NAME

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Resource name that is checked	
■				CKG.UCAT.*usercatalogname*	(discrete required)

USRDATA

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Resource name that is checked
■				CKG.USRDATA.{ OWN | ALL | SCP }.*class.index*

Chapter 6. CKNSERVE command syntax

The systems programmer can set up the zSecure server to allow RACF reporting and administration of multiple systems. The main program that is running in the zSecure server is the CKNSERVE program. It facilitates communication with remote systems and access to security databases, SMF input files, CKFREEZE data sets, and other defined data sets.

Operator commands

START

MODIFY *taskname,action*

STOP

Configuration statements

The mandatory statements are **ZSECNODE** and **ZSECSYS**. The optional statement is **OPTION**.

ZSECNODE
NAME(*node-name*) [PREFERRED (*system-name*)]

ZSECSYS
ZSECSYS NAME(*system-name*) ZSECNODE(*node-name*) IPADDRESS(*ip-address*)
IPPORT(*ip-port*) RETRYINTERVAL(*retryinterval*)

OPTION
[OwnSys(*system-name*)] [SIRoutine(CKRSRVIR) | SIRoutine(*program-name*)]
[ServerToken(PRODSERV) | ServerToken(*token-name*)] [InSecure] [Debug]
[RMTMSG] [Timestamp] [MSGSUP(*message-number* [, ...]]
[*Other-diagnostic-options*]

Chapter 7. zSecure Alert command syntax

The systems programmer can set up the zSecure Alert server to monitor events in the system as reported through SMF records and Write To Operator (WTO) messages. The RACF analyst can configure the zSecure Alert server to send out selected alerts as emails, text messages, UNIX syslog messages, WTOs, and Simple Network Management Protocol (SNMP) traps in real time.

Start parameters

Start parameters(S C2POLICE,PARM.C2POLICE=FORCE)

DEBUG

FORCE

DEBUG-FORCE

Operator commands and configuration statements

Operator commands (F C2POLICE,command)

Operator commands that do not support any additional keywords
COLLECT
DISPLAY
REFRESH
RESTART
SIPL
STOP

Operator commands that support more keywords and are also configuration statements

DEBUG

```
[ ALL | NONE | SMF | NOSMF | WTO | NOWTO | MAIN | NOMAIN | BUFFER | NOBUFFER |
         IO | NOIO | EXTMON | NOEXTMON | CKRCARLAPARAMETER('parameter;') ]
```

DIAGNOSE

```
[ EXTMON ( [ ALL | CURRENT | HEADER ] ) ]
[ C2PC ( [ DUMP ( [ ACTIVE | COPY ] ) | SAVE | CLEAR ]  )
```

FILTER

```
{ ADDSMF (RECTYPE (rectype) [SUBTYPE (subtype) | NOSUBTYPE ] |
       DELSMF (RECTYPE (rectype) }
{ ADDWTO (prefix(prefix-chars))|
  DELWTO (prefix(prefix-chars)) }
```

REPORT

```
[ INTERVAL ( [ 60 | interval ] ) ]
[ AVERAGEINTERVAL ( [ 300 | averageinterval ] ) ]
[ { PREPROCESSINTERVAL | STAGE1INTERVAL } ( [ 60 | stage1interval ] ) ]
[ MEMBER ( [ C2PALERT | member-name ] ) ]
[ { PREPROCESSMEMBER | STAGE1MEMBER } ( [ C2PSTG1 | member-name ] ) ]
[ DDNAME ( [ SC2PSAMP | samp-ddname ] ) ]
[ EXTMONMEMBER ( report-memberE | member-name ) ]
```

Configuration statements

OPTION
[BUFSIZE ([1024 | *bufsize*])]
[NUMBUFS ([12 | *numbufs*])]
[COLLECTTIME ([0100 | *time-of-day*])]
[COLLECTSTCNAME ([C2PCOLL | *stc-name*])]
[EXTMON ([ACTIVE | INACTIVE] [RETAIN([24 | *hours*])]

SIMULATE
SYSTEM(*sysname*)
FORMAT(ACF2)
SMF ({ 230 | *rectype* })

Chapter 8. zSecure RACF-Offline command syntax

The RACF Administrator can use RACF-Offline to direct commands to a RACF database that is not in use. This function allows verifying intended RACF changes before actually changing any production environment.

Control commands specified with B8ROPT and B8RPARM

RACFDB
dsname [SEQUENCE(1) | SEQUENCE(*number*)] [DISP(SHR) | DISP(OLD)]

LOGDS
dsname

SMF
{ RENUMBER(NEW80(*new80*) NEW81(*new81*) NEW83(*new83*))
SUPPRESS | ID(*smf-id*) | USER(*user*) | ASIS }

END

RACF commands and supporting commands

RACF commands

Security zSecure Admin RACF-Offline supports most RACF commands in unmodified form. The **RVARY**, **SETROPTS**, and **RACLINK** commands are not supported. Also, RRSF support is explicitly disabled in Security zSecure Admin RACF-Offline. The AT or ONLYAT keywords are ignored. Automatic command direction is not performed no matter what system settings are specified with the TARGET operator command.

Supporting commands

B8RACFLG
[Open | Close | Reset | Flush | List]

B8REPLAY
Select(*ident*)

B8RVARY
[Select(*ident*) | List]

CKGRACF

See Chapter 5, "CKGRACF command syntax," on page 65.

END

EXEC | EX

ISPF
ISPF parameters and keywords

LOGON
[*userid/password* [*/new-password*] [SPECIAL | NOSPECIAL]
[OPERATIONS | NOOPERATIONS] [AUDITOR | NOAUDITOR]

PROFILE

REPORT
[Verbose | Terse]

TIME

TRACE

Chapter 9. zSecure Access Monitor command syntax

The systems programmer can set up the zSecure RACF Access Monitor function to monitor access events and collect relevant data. The RACF administrator can use the collected data to view and analyze usage of resource profiles and access specifications.

Start parameters

```
Start parameters(S C2PACMON,,,DEBUG)

    DEBUG

    FORCE

    DEBUG-FORCE
```

Operator commands

Operator commands that do not require more keywords

```
CONSOLIDATE
DISPLAY
RESTART
SIPL
STOP
```

Operator commands that support more keywords and are also configuration statements

```
DEBUG
[ ALL | NONE | MAIN | NOMAIN | BUFFER | NOBUFFER
|
         IO | NOIO | RACF | NORACF | CKRCARLAPARAMETER('parameter;')
]
```

```
REPORT
[
INTERVAL ( [ 60 | interval ] ) ]
[ ConsolidateTime ( [ 0000 | consolidatetime ] ) ]
[ Member ( [ C2PAMCOL | member-name ] ) ]
[ ConsolidateMember ( [ C2PAMCON | member-name ] ) ]
[ DDNAME ( [ SC2PSAMP | samp-ddname ] ) ]
```

Configuration statements

```
OPTION
[ BUFSIZE ( [ 1024 | bufsize ] ) ]
[ NUMBUFS ( [ 10 | numbufs] ) ]
[ NOINCLUDEOWNRESOURCE | INCLUDEOWNRESOURCE ]
```

Chapter 10. zSecure Collect command syntax

The RACF Administrator uses the zSecure Collect program (CKFCOLL) to gather information about the configuration of the z/OS system, quickly and with minimal resources. The CKRCARLA program analyzes the collected data.

Overview of defaults (dependent on APF status) and allowed features for each focus

Y Default =YES and allowed to specify =NO

. Default =NO or 0 and NOT allowed to specify another value

n Default =NO and allowed to specify =YES

v Default =0 but value specification is allowed

	ADMIN		AUDIT		TCIM/ALERT		VISUAL	
Parameter	Napf	apf	Napf	apf	Napf	apf	Napf	apf
ABR	Y	Y	Y	Y	.	.	Y	Y
ALLOC	Y	Y	Y	Y	Y	Y	Y	Y
BCD	.	Y	.	Y	.	.	.	Y
CAT	.	Y	.	Y	.	Y	.	Y
CHECK	.	.	n	n	.	.	.	.
CICS	Y	Y	Y	Y	Y	Y	Y	Y
DB2	Y	Y	Y	Y	Y	Y	Y	Y
DMS	Y	Y	Y	Y	.	.	Y	Y
IDR	.	.	n	n	.	.	.	.
IMS	Y	Y	Y	Y	Y	Y	Y	Y
INTERVAL	.	.	.	.	.	.	.	.
MCD	.	Y	.	Y	.	.	.	Y
MONITOR	.	.	.	.	.	.	.	.
OFFLINE	n	n	n	n	n	n	n	n
PATH	.	.	.	.	.	.	.	.
PDS	n	Y	n	Y	n	Y	.	.
RECALL	Y	Y	Y	Y	Y	Y	Y	Y
RMM	Y	Y	Y	Y	.	.	.	.
SCAN	.	.	Y	Y	.	.	.	.
SHARED	Y	Y	Y	Y	Y	Y	Y	Y
SIGVER	n	Y	n	Y	n	Y	.	.
SMS	Y	Y	Y	Y	Y	Y	Y	Y
STATS	.	.	.	.	.	.	.	.
SWCH	.	.	.	.	.	.	.	.
TAPE	.	.	.	.	.	.	.	.
TCPIP	.	Y	.	Y	.	Y	.	.

Parameter	ADMIN		AUDIT		TCIM/ALERT		VISUAL	
	Napf	apf	Napf	apf	Napf	apf	Napf	apf
TMC	Y	Y	Y	Y	.	.	.	.
UNIX	.	.	Y	Y	Y	Y	.	.
VMF	Y	Y	Y	Y	.	.	.	.
VTOC	Y	Y	Y	Y	Y	Y	Y	Y
VVDS	Y	Y	Y	Y	Y	Y	Y	Y

Use the column corresponding with the first part of the focus name. For example, for AUDITRACF, use the AUDIT column.

Feature selection

N Specified as NO.

a Default N, alternate data source allowed.

n Default N, Y, or other data source allowed.

Y Specified as YES

. Default Y or N depending on FOCUS/APF

Parm specified:							
IO	N	.	.	.	.	.	.
UNITIO	.	N	.	.	.	.	.
ALLOC	.	.	N	.	.	.	.
DASD	.	.	.	N	.	.	.
VTOC	.	.	.	.	N	.	.
VVDS	.	.	.	.	.	N	.
CHECK	.	.	.	.	.	.	Y
Implies:							
ABR	N	N	n	n	.	.	.
ALLOC	N	N	N	Y	Y	Y	Y
CAT	N	N	N	n	n	.	.
CHECK	N	N	.	.	.	.	Y
MCD	N	N	a	n	.	.	.
BCD	N	N	a	n	.	.	.
DMS	N	N	a	n	.	.	.
IDR	N	N	.	.	.	.	Y
PATH	N	N	.	.	.	.	.
PDS	N	N	a	n	.	.	.
RMM	N	N	a	n	.	.	.
SCAN	.	.	.	.	.	.	.
SIGVER	N	N	a	n	.	.	.
SWCH	N	N	.	.	.	.	.
TAPE	N	N	.	.	.	.	.

TCPIP	.	.	.	.	.	.	.
TMC	N	N	a	n	.	.	.
UNIX	N	N	N	.	.	.	.
VMF	N	N	n	n	.	.	.
VTOC	N	N	N	n	N	.	.
VVDS	N	N	N	n	N	N	.

Calling JCL

`CKFREEZE`

`DSNIN`

`DSNOUT`

`DSNPRT`

`SYSPRINT`

`SYSTERM`

`SYSIN`

Command syntax

The zSecure Collect program supports a number of parameters or commands to restrict the information that is collected to a subset of your I/O subsystem or to a specific purpose. Some restrictions are more limiting than others, and some restrictions can be combined to generate a subset.

- Multiple parameters can be specified, separated by commas, semicolons, or blanks. The commands are not case-sensitive.
- The parameters can be specified on the `PARM` field of the `EXEC` statement, or in the `SYSIN` file.
- If the `SYSIN` file is 80 characters-wide, only positions 1 - 72 are read.
- Commands can be continued on the next line, but not in the middle of a word.
- The line end acts as a separator just like a blank or comma. If parameters are specified more than once, the value last given is used.
- Parameters on the `EXEC` statement, or passed on a `TSO` command are processed before the parameters in the `SYSIN` file.
- All parameters are listed on the `SYSPRINT` file, prefixed with their origin (`PARM` or `SYSIN`).
- The *command order* is free, except that the `FOCUS` command must be specified before any command that is not allowed under each focus. Practically speaking, FOCUS must either be the first command or be omitted altogether.
- To indicate a comment, use `/*` at the beginning of the comment, and end the comment with `*/`.
- If not already part of such a comment, `'*'` also starts a comment, which then runs to the end of the line.

Command reference

```
ABR={ YES | NO }
ALLOC={ YES | NO }
ALLRECS
APF
ARCDSN={ dsn | dsn/vol }
AUTOMOUNT={ YES | NO }
BCD={ YES | NO }
BURSTS=nn
BURSTWAIT=nn
BURSTSIZE=nn
CAPS
CAT={ YES | NO | MCAT }
CHECK=( { DD | DDPREF } = dd )
CHECK=( { DSN | DSNPREF } = dsn [ ,DSORG = ( PO | PS | VS ) ] )
CHECK={ YES | NO }
CHECKDSN={ dsn | dsn/vol }
CHECKPWD={ 'txt' | "txt" | word }
CICS={ YES | NO }
CKFREEZE=[ 'dsn' | 'dsn(mem)' | dsn | dsn(mem) ]
DASD={ YES| NO }
DB2={ YES | NO }
DB2ADM
DB2CAT={ YES | NO }
DEBUG
DEBUGDB2
DEBUGHANGTEST=n
DEBUGHANVOLUME=volume
DMS={ YES | NO }
DMSFILES={ dsn | dsn/vol }
DMSPARMS={ dsn | dsn/vol }
DMSUNL={ dsn | dsn/vol }
ENQ=NO
ERRDD=ddname
{ EXCLUDE | EXCL | X } =selectionlist (see explanation of selectionlist
                                        after this list)
EXIT=( [ RC=rc ],[ NOCLEAR | CLEAR ] )
{ FOCUS | F } = { focus | focuslist }
FREE
FREEZEDD=ddname
HFS={ YES | NO }
HFSCLIENT={ YES | NO }
HSMBCD={ dsn | dsn/vol }
HSMMCD={ dsn | dsn/vol }
ICFCAT= { dsn | dsn/vol }
IDR={ YES | NO }
IF symbol [ = | <> ] list :
IMS={ YES | NO }
INDD=ddname
INFO
IO={ YES | NO }
IOTIMEOUT=nnn
MCD= { YES | NO }
MOD={ YES | NO }
NJE={ YES | NO }
```

```
NOBSAMBPAM
NOBYPASS
NOCLOSE
NODB2ADM
NODCBE
NODIAG
NOKEY0
NOMSG=list
NOREPORT
NOSIO
NOUID0
{ NOWARNINGRC | NOWARNRC }
NOXMDSN
NOXMEM
OFFLINE=YES
OUTDD=ddname
{ PAR | PARALLEL } = { PATH | PATHGROUP | NONE }
PATH={ YES | NO }
PDS={ YES | NO }
PDSDIR= { dsn | dsn/vol }
PDSEBUFSIZE=nn
RECALL={ YES | NO }
REPORT
RESTORE={ YES | NO }
RMM={ YES | NO }
RMMCTL={ dsn | dsn/vol }
S=selectionlist (see explanation of selectionlist after this list)
SCAN={ YES | NO }
SCANSTR=list
SCANSVC=list
{ SELECT | SEL | S }=selectionlist (see explanation of selectionlist
                                    after this list)
SERIALIZATION( [ ENQ( [ CKRDSN ],[ SYSDSN ] ) | NOENQ ]
   [ FAIL | WAIT [ MAXWAIT(minutes) ] ] [ UNIT ] [ VOLSER ] )
SHARED={ YES | NO }
SIGVER={YES | NO}
SLOWDOWN
SMS=NO
STORAGEGC
{ SUP | SUPMSG | SUPP | SUPPMSG | SUPPRESS }=list
TCPIP={ YES | NO }
TKDS={ YES | NO }
TKDSN={ dsn | dsn/vol }
TMC={ YES | NO }
TMCDSN= { dsn | dsn/vol }
UNCONNECTED
UNITIO={ YES | NO }
{ UNIX | HFS }={ YES | NO }
UNIXACL={ YES | NO }
{ UNIXCLIENT | HFSCLIENT }={ YES | NO }
VMF={ YES | NO }
VMFDSN={ dsn | dsn/vol }
VTOC={ YES | NO }
VVDS={ YES | NO | NONE }
```

```
WAIT={ YES | NO }
X=selectionlist (see explanation of selectionlist after this list)
XTIOT={ YES | NO }
```

selectionlist can be any one of the following parameters or a list that is enclosed in parentheses that are separated by commas:

```
   { C | CH | CHP | CHANNEL }=xx
{ V | VOL | VOLSER | VOLUME }=xxxxxx
{ DEV | DEVICE | U | UNIT }=xxxx
{ SG | STORGRP }=xxxxxxx
LCU=xxx
DSNHLQ=list
{ D | DSN | DSNPREF }=prefix
```

Chapter 11. zSecure Command Verifier profiles

zSecure Command Verifier adds granular controls for RACF commands. RACF Administrators can use Command Verifier to help prevent errors and block noncompliant commands before execution.

In general, if no profile is defined, zSecure Command Verifier considers this as the absence of a specific policy and defers the authorization decision to RACF. Standard RACF processing is followed, as if zSecure Command Verifier was not implemented. If a policy profile exists, the access level (by access list and UACC) is usually interpreted as follows:

No profile found	The policy rule is not implemented.
NONE	The terminal user does not meet the requirements as described by the policy rule. Most often, the command is rejected.
READ	Same as NONE. Also, in many situations, READ access is sufficient to remove an attribute, or specify an initial value.
UPDATE	The terminal user does meet all the requirements as described by the policy rule. The command continues.
CONTROL	The policy rule does not apply to this terminal user.

Note: In some cases, there are specific descriptions for some profiles. You can find these descriptions in the User Guide.

General functions

C4R.DEBUG	This profile is now deprecated. Instead, use the C4R.=MSG.CMD profile.
C4R.EXEMPT	Policies do not apply.
C4R.SUPPRESS	Policy violations are suppressed.
C4R.ERROR.CONTINUE	Policy errors do not cause command termination.
C4R.=MSG.CMD	Display RACF command before execution.
C4R.=MSG.SUPPRESSED	Controls whether message C4R899W is issued when a keyword or parameter value is suppressed.
C4R.=MSG.MANDATORY	Controls whether message C4R898W is issued when Command Verifier policies override a mandatory keyword or parameter value of a user specified keyword or parameter.
C4R.=MSG.DEFAULTS	Controls whether message C4R897W is issued when Command Verifier policies supply a default keyword or parameter value to complete the user specified command.

C4R.command.=SPECIAL	The command is running with RACF System-Special authorization.
C4R.command.=CTLSPEC	If all command keywords are controlled by a policy profile, the command is running with RACF System-Special authorization.
C4R.class.segment.=RACUID	Authority to manage own segments.
C4R.class.segment	Authority to manage segments other than your own user ID.
C4R.class.segment./SCOPE	Segment management only within (group-) special scope

Replace RACF commands

Commands and keywords that are supported by Command/Keyword Replace Function

Command	Keyword	Keyword-qualifier
ALTUSER	**RESUME**	**RESUME**
ALTUSER	**REVOKE**	**REVOKE**
ALTUSER	**RESUME**(*date*) **NORESUME**	**RESUMEDT**
ALTUSER	**REVOKE**(*date*) **NOREVOKE**	**REVOKEDT**
ADDUSER **ALTUSER**	**SPECIAL**	**SPECIAL**
ADDUSER **ALTUSER**	**OPERATIONS**	**OPERATIONS**
ADDUSER **ALTUSER**	**AUDITOR**	**AUDITOR**
PERMIT	**CLASS**(*class*)	**CLASS**(*class*)
ADDUSER **ALTUSER**	*segment* **NO***segment*	*segment.action* *action* = { Add | Alt | Del }

Profiles used for the Replace RACF Commands function

C4R.command.**=PRECMD.***keyword-qualifier*
C4R.command.**=REPLACE.***keyword-qualifier*
C4R.command.=**PSTCMD.***keyword-qualifier*

Variables supported in APPLDATA

&CLASS	The CLASS of the PROFILE
&PROFILE	The PROFILE
&PROFILE(1)	One of the multiple profiles that are used in the command. Which one is unpredictable.
&SEGMENT	The list of segments that are being managed in the command.
&SEGMENT(1)	One of the segments that are being managed in the command. Which one is unpredictable.

&RACUID	The USERID of the terminal user that is issuing the command.
&RACGPID	The current connect GROUP of the terminal user that is issuing the command
&DATE	The current date in Julian format (YY.DDD)
&TIME	The current time in 24 hour format (HH:MM:SS)
&SYSID	The SMF System Identifier of the current system
&ACLID	The list of IDs specified in the ID keyword of the PERMIT command
&ACLID(1)	One of the IDs specified in the ID keyword of the PERMIT command. Which one is unpredictable.
&ACLACC	The access level that is granted by the ACCESS keyword of the PERMIT command

Auditing policy profiles

RACF Administrators and Auditors can use zSecure Command Verifier to audit the commands as issued and monitor the effects of the implemented policies.

Command Audit Trail

C4R.*class***.=CMDAUD.=SEGMENT.***profile-identification***
C4R.*class***.=CMDAUD.=ATTR.***profile-identification***
C4R.*class***.=CMDAUD.=CONNECT.***profile-identification***
C4R.*class***.=CMDAUD.=ACL.***profile-identification***
C4R.*class***.=CMDAUD.=MEMBER.***profile-identification***
C4R.*class***.=CMDAUD.=MAINT.***profile-identification***

Profile-identification values for *class*

Class	**profile-identification**
USER	*owner.userid*
GROUP	*owner.group*
resource	*resource-profile*

Access levels for all policy profiles except for the =CMDAUD.=MAINT

No Profile Found	No Command Audit Trail data is collected or retained.
NONE	Command Audit Trail data is collected or retained.
READ	Same as NONE.
UPDATE	Same as NONE.
CONTROL	Same as NONE.

Access levels for the =CMDAUD.=MAINT policy profile

No Profile Found	Command Audit Trail data is not displayed and cannot be maintained by the C4RCATMN command.
NONE	The Audit Trail data is not shown and cannot be maintained by the C4RCATMN command.
READ	The Audit Trail data is shown as part of the RACF LIST command.
UPDATE	The Audit Trail data is shown as part of the RACF LIST command. It can also be displayed by the C4RCATMN command.
CONTROL	The terminal user is also authorized to use the C4RCATMN command to remove the Command Audit Trail data.

Policy profiles for command auditing

C4R.PREAUD.*command*
C4R.PSTAUD.*command*
C4R.ERRMSG.*command*

Administration policy profiles

The RACF administrator can use regular zSecure Command Verifier administration policies to manage the use of RACF commands, keywords, and parameter values.

SETROPTS-related profiles

Profiles that are used for verification of SETROPTS LIST authority

The entries in this table reflect the **SETROPTS** keywords that are used to set a particular option.

Keyword	Value	Profile
LIST	N/A	C4R.RACF.LIST

Profiles that are used for verification of RACF options

The entries in this table reflect the **SETROPTS** keywords that are used to set a particular option.

Keyword	Value	Profile
(NO)ADDCREATOR	N/A	C4R.RACF.OPTION.ADDCREATOR
(NO)ADSP	N/A	C4R.RACF.OPTION.ADSP
CATDSNS	*mode*	C4R.RACF.OPTION.CATDSNS.*mode* *mode* = { *FAILURES*, *WARNING* }
NOCATDSNS	N/A	C4R.RACF.OPTION.CATDSNS.FAILURES C4R.RACF.OPTION.CATDSNS.WARNING
(NO)EGN	N/A	C4R.RACF.OPTION.EGN
ERASE	*type*	C4R.RACF.OPTION.ERASE.*type* *type* = { *PROFILE*, *SECLEVEL*, *ALL* }

Keyword	Value	Profile
(NO)GENERICOWNER	N/A	C4R.RACF.OPTION.GENERICOWNER
(NO)GRPLIST	N/A	C4R.RACF.OPTION.GRPLIST
KERBLVL	*level*	C4R.RACF.OPTION.KERBLVL
PROTECTALL	*mode*	C4R.RACF.OPTION.PROTECTALL.*mode* }*mode* = { *FAILURES*, *WARNING*
NOPROTECALL	N/A	C4R.RACF.OPTION.PROTECTALL.FAILURES C4R.RACF.OPTION.PROTECTALL.WARNING
(NO)REALDSN	N/A	C4R.RACF.OPTION.REALDSN
RETPD	*period*	C4R.RACF.OPTION.RETPD
SESSIONINTERVAL NOSESSIONINTERVAL	*interval* N/A	C4R.RACF.OPTION.SESSIONINTERVAL
(NO)TAPEDSN	N/A	C4R.RACF.OPTION.TAPEDSN
TERMINAL	*access*	C4R.RACF.OPTION.TERMINAL.*access*
RVARYPW	SWITCH(*password*)	C4R.RACF.OPTION.RVARYPW.SWITCH
RVARYPW	STATUS(*password*)	C4R.RACF.OPTION.RVARYPW.STATUS

Profiles that are used for verification of RACF auditing settings

The entries in this table reflect the **SETROPTS** keywords that are used to set a particular option.

Keyword	Value	Profile
(NO)APPLAUDIT	N/A	C4R.RACF.AUDIT.APPLAUDIT
(NO)CMDVIOL	N/A	C4R.RACF.AUDIT.CMDVIOL
(NO)INITSTATS	N/A	C4R.RACF.AUDIT.INITSTATS
(NO)OPERAUDIT	N/A	C4R.RACF.AUDIT.OPERAUDIT
(NO)SAUDIT	N/A	C4R.RACF.AUDIT.SAUDIT
(NO)SECLABELAUDIT	N/A	C4R.RACF.AUDIT.SECLABELAUDIT
SECLEVELAUDIT	*seclevel*	C4R.RACF.AUDIT.SECLEVELAUDIT.*seclevel*
NOSECLEVELAUDIT	N/A	C4R.RACF.AUDIT.SECLEVELAUDIT

Profiles that are used for verification of JES-related settings

The entries in this table reflect the **SETROPTS** keywords that are used to set a particular option.

Keyword	Value	Profile
(NO)BATCHALLRACF	N/A	C4R.RACF.JES.BATCHALLRACF
(NO)EARLYVERIFY	N/A	C4R.RACF.JES.EARLYVERIFY
(NO)XBMALLRACF	N/A	C4R.RACF.JES.XBMALLRACF
NJEUSERID	*userid*	C4R.RACF.JES.NJEUSERID.*userid*
UNDEFINEDUSER	*userid*	C4R.RACF.JES.UNDEFINEDUSER.*userid*

Profiles that are used for verification of USER-related settings

The entries in this table reflect the **SETROPTS** keywords that are used to set a particular option.

Keyword	Value	Profile
(NO)INACTIVE	*days*	C4R.RACF.USER.INACTIVE
PASSWORD	HISTORY(*count*)	C4R.RACF.USER.PASSWORD.HISTORY
PASSWORD	INTERVAL*(period)*	C4R.RACF.USER.PASSWORD.INTERVAL
PASSWORD	MINCHANGE*(period)*	C4R.RACF.USER.PASSWORD.MINCHANGE
PASSWORD	(NO)MIXEDCASE	C4R.RACF.USER.PASSWORD.MIXEDCASE
PASSWORD	REVOKE(*count*)	C4R.RACF.USER.PASSWORD.REVOKE
PASSWORD	WARNING(*period*)	C4R.RACF.USER.PASSWORD.WARNING
PASSWORD	RULE*n(rule-spec)*NORULE*n* NORULES	C4R.RACF.USER.PASSWORD.RULES

Profiles that are used for verification of MLS-related settings

The entries in this table reflect the **SETROPTS** keywords that are used to set a particular option.

Keyword	Value	Profile
(NO)COMPATMODE	N/A	C4R.RACF.MLS.COMPATMODE
MLACTIVE	*mode*	C4R.RACF.MLS.MLACTIVE.*mode* *mode* = { FAILURES, WARNING }
NOMLACTIVE	N/A	C4R.RACF.MLS.MLACTIVE.FAILURES C4R.RACF.MLS.MLACTIVE.WARNING
MLS	*mode*	C4R.RACF.MLS.MLS.*mode* *mode* = { FAILURES, WARNING }
NOMLS	N/A	C4R.RACF.MLS.MLS.FAILURES C4R.RACF.MLS.MLS.WARNING
(NO)MLSTABLE	N/A	C4R.RACF.MLS.MLSTABLE
MLFSOBJ	*mode*	C4R.RACF.MLS.MLFSOBJ
MLIPCOBJ	*mode*	C4R.RACF.MLS.MLIPCOBJ
(NO)MLNAMES	N/A	C4R.RACF.MLS.MLNAMES
(N0)MLQUIET	N/A	C4R.RACF.MLS.MLQUIET
(NO)SECLABELCONTROL	N/A	C4R.RACF.MLS.SECLABELCONTROL
(NO)SECLBYSYSTEM	N/A	C4R.RACF.MLS.SECLBYSYSTEM

Profiles that are used for verification of class-specific settings

The entries in this table reflect the **SETROPTS** keywords that are used to set a particular option.

Keyword	Value	Profile
(NO)AUDIT	*class*	C4R.RACF.*class*.AUDIT
(NO)CLASSACT	*class*	C4R.RACF.*class*.CLASSACT
(NO)GENCMD	*class*	C4R.RACF.*class*.GENCMD
(NO)GENERIC	*class*	C4R.RACF.*class*.GENERIC
(NO)GENLIST	*class*	C4R.RACF.*class*.GENLIST
(NO)GLOBAL	*class*	C4R.RACF.*class*.(NO)GLOBAL
(NO)RACLIST	*class*	C4R.RACF.*class*.RACLIST
NO)STATISTICS	*class*	C4R.RACF.*class*.STATISTICS
(NO)WHEN	*class*	C4R.RACF.*class*.WHEN

Keyword	Value	Profile
LOGOPTIONS	*condition* *(class)*	C4R.RACF.*class*.LOGOPTIONS.*condition* *condition* = { ALWAYS, NEVER, SUCCESSES, FAILURES, DEFAULT }

User ID-related profiles

Profiles that are used for verification of RACF USERID

The entries in this table reflect the keywords that describe the name of new and deleted user IDs.

Keyword	Value	Profile
ADDUSER	*userid*	C4R.USER.ID.=RACUID(*n*)
ADDUSER	*userid*	C4R.USER.ID.=RACGPID(*n*)
ADDUSER	*userid*	C4R.USER.ID.*userid*
DELUSER	*userid*	C4R.USER.DELETE.*userid*

Profiles that are used for mandatory values of RACF USERID place-related command/keywords

The entries in this table reflect the keywords that describe the mandatory value of new user IDs.

Command	Keyword	Profile	APPLDATA used?
ADDUSER	*userid*	C4R.USER.=DFLTGRP.*userid*	Yes See Values accepted for the APPLDATA field (DFLTGRP): RACF USERID place-related Command/Keywords.
ADDUSER	*userid*	C4R.USER.=OWNER.*userid*	Yes See Values accepted for the APPLDATA field (OWNER): RACF USERID place-related Command/Keywords.

Profiles that are used for default values of RACF USERID place-related command/keywords

The entries in this table reflect the keywords that describe the default value of new user IDs.

Command	Keyword	Profile	APPLDATA used?
ADDUSER	*userid*	C4R.USER./DFLTGRP.*userid*	Yes See Values accepted for the APPLDATA field (DFLTGRP): RACF USERID place-related Command/Keywords.
ADDUSER	*userid*	C4R.USER./OWNER.*userid*	Yes See Values accepted for the APPLDATA field (OWNER): RACF USERID place-related Command/Keywords.

Values that are accepted for the APPLDATA field (DFLTGRP): RACF USERID place-related command/keywords

blank
This is used to indicate that RACF default processing must be used. That is, RACF uses the current group of the terminal user.

userid
This invalid entry is not caused by incorrect entry by the terminal user. Therefore, the command is allowed to continue (with the current group of the terminal user).

group
This group is inserted. If the terminal user does not have sufficient access to this group, the command is failed by RACF.

=OWNER
Reflects the OWNER as specified (or defaulted) by the OWNER keyword on the command. This value can also be an OWNER value as inserted by zSecure Command Verifier.

=MYOWNER
Reflects the OWNER of the terminal user. This value must be a group. All other situations are considered an error. This error is not caused by incorrect entry by the terminal user. Therefore, the command is allowed to continue (with the current group of the terminal user).

=USERID(*n*)
Reflects the first n characters of the new USERID itself. This value must be a GROUP. All other situations are considered an error, and the current GROUP of the terminal user is used instead.

=RACGPID
Reflects the GROUP that was used to allow definition of the USERID by =RACGPID(n). This value is only used if =RACGPID(n) was used to allow definition. In all other situations, the APPLDATA value =RACGPID is considered an error, and the current group of the terminal user is used instead.

Values that are accepted for the APPLDATA field (OWNER): RACF USERID place-related command/keywords

blank
The specified value of the new OWNER is suppressed, and replaced by the USERID of the terminal user. This value is the default value that RACF uses if no OWNER was specified.

userid
Depending on the access level to the /GROUP profile, the user ID is inserted as the owner of the new USERID.

group
The specified GROUP is used as OWNER of the new USERID

=OWNER
Reflects the OWNER as specified (or defaulted) by the OWNER keyword on the command. If this OWNER resolves to the special value =DFLTGRP(indicating the default group), the command is failed.

=MYOWNER
Reflects the OWNER of the terminal user. If this value is a GROUP, the value is

used as the OWNER of the new USERID. If this value is a USERID, further processing is dependent on the access level that the terminal user has to the /GROUP profile.

=USERID(*n*)
Reflects the first n characters of the new USERID itself. This value must be a USERID of GROUP. All other situations are considered an error, and the current GROUP of the terminal user is used instead.

=RACGPID
Reflects the GROUP that was used to allow definition of the USERID by =RACGPID(n). This value is only used if =RACGPID(n) was used to allow definition. In all other situations, the APPLDATA value =RACGPID is considered an error, and the current group of the terminal user is used instead.

Profiles that are used for verification of RACF USERID

The entries in this table reflect the keywords that the terminal user specified to describe the name and place of new or changed user IDs.

Keyword	Value	Profile
ADDUSER ALTUSER	DFLTGRP	C4R.USER.DFLTGRP.=RACUID(*n*)
ADDUSER ALTUSER	DFLTGRP	C4R.USER.DFLTGRP.=RACGPID(*n*)
ADDUSER ALTUSER	DFLTGRP	C4R.USER.DFLTGRP.=USERID(*n*)
ADDUSER ALTUSER	DFLTGRP	C4R.USER.DFLTGRP.*group.userid*
ADDUSER ALTUSER	DFLTGRP	C4R.USER.DFLTGRP./SCOPE.*group.userid*
ADDUSER ALTUSER	DFLTGRP	C4R.USER.DFLTGRP./OWNER.*group.userid*
ADDUSER ALTUSER	OWNER	C4R.USER.OWNER.=RACUID(*n*)
ADDUSER ALTUSER	OWNER	C4R.USER.OWNER.=RACGPID(*n*)
ADDUSER ALTUSER	OWNER	C4R.USER.OWNER.=USERID(*n*)
ADDUSER ALTUSER	OWNER	C4R.USER.OWNER.*owner.userid*
ADDUSER ALTUSER	OWNER	C4R.USER.OWNER./SCOPE.*owner.userid*
ADDUSER ALTUSER	OWNER	C4R.USER.OWNER./GROUP.*owner.userid*
ADDUSER ALTUSER	OWNER	C4R.USER.OWNER./DFLTGRP..*owner.userid*

Profiles that are used for RACF attributes

The entries in this table reflect the keywords that are specified on the **ADDUSER** and **ALTUSER** command.

Keyword	Value	Profile	APPLDATA used?
ADDUSER	N/A	C4R.USER.=ATTR.*owner.userid*	Yes

Keyword	Value	Profile	APPLDATA used?
ADDUSER ALTUSER	SPECIAL	C4R.USER.ATTR.SPECIAL *.owner.userid*	
ADDUSER ALTUSER	OPERATIONS	C4R.USER.ATTR.OPERATIONS.*owner.userid*	
ADDUSER ALTUSER	AUDITOR	C4R.USER.ATTR.AUDITOR.*owner.userid*	
ADDUSER ALTUSER	RESTRICTED	C4R.USER.ATTR.RESTRICTED.*owner.userid*	
ALTUSER	UAUDIT	C4R.USER.ATTR.UAUDIT.*owner.userid*	
ADDUSER ALTUSER	ADSP	C4R.USER.ATTR.ADSP.*owner.userid*	
ADDUSER ALTUSER	GRPACC	C4R.USER.ATTR.GRPACC.*owner.userid*	
ADDUSER ALTUSER	NOPASSWORD	C4R.USER.ATTR.PROTECTED.*owner.userid*	
ADDUSER ALTUSER	OIDCARD	C4R.USER.ATTR.OIDCARD.*owner.userid*	
ALTUSER	REVOKE	C4R.USER.ATTR.REVOKE.*owner.userid*	
ALTUSER	RESUME	C4R.USER.ATTR.RESUME.*owner.userid*	
ALTUSER	REVOKE(*date*) NOREVOKE	C4R.USER.ATTR.REVOKEDT.*owner.userid*	
ALTUSER	**RESUME**(*date*) NORESUME	C4R.USER.ATTR.RESUMEDT.*owner.userid*	

Values that are accepted for the APPLDATA

SPECIAL and NOSPECIAL
OPERATIONS and NOOPERATIONS
AUDITOR and NOAUDITOR
PASSWORD and NOPASSWORD
RESTRICTED and NORESTRICTED
OIDCARD and NOOIDCARD
ADSP and NOADSP
GRPACC and NOGRPACC

Profiles that are used for RACF password and password phrase

The entries in this table reflect the keywords that are specified on the **ADDUSER**, **ALTUSER** and **PASSWORD** command.

Command	Keyword	Profile	APPLDATA used?
ADDUSER **ALTUSER**	PASSWORD	C4R.USER./PASSWORD.*owner.userid*	Yes. See Values supported for APPLDATA: RACF Password and Password Phrase.
ADDUSER **ALTUSER**	PASSWORD	C4R.USER.PASSWORD.*owner.userid*	
PASSWORD	PASSWORD	C4R.USER.PASSWORD.=RACUID	
ADDUSER **ALTUSER**	PHRASE	C4R.USER.PHRASE.*owner.userid*	
PASSWORD	PHRASE	C4R.USER.PHRASE.=RACUID	
ADDUSER **ALTUSER**	PASSWORD	C4R.USER.PASSWORD=DFLTGRP	
PASSWORD	USER(*userid*)	C4R.USER.PASSWORD=DFLTGRP	

Command	Keyword	Profile	APPLDATA used?
ADDUSER **ALTUSER**	PASSWORD	C4R.USER.PASSWORD.=USERID	
PASSWORD	(NO)INTERVAL	C4R.USER.=PWINT.*owner.userid*	Yes. See Values accepted for the APPLDATA field: RACF Password and Password Phrase.
PASSWORD	(NO)INTERVAL	C4R.USER.PWINT.*owner.userid*	Yes. See Values accepted for the APPLDATA field: RACF Password and Password Phrase.
ALTUSER	(NO)EXPIRED	C4R.USER.PWEXP.*owner.userid*	

Values that are supported for APPLDATA: RACF password and password phrase

blank
This value is used to indicate that RACF default processing must be used. RACF uses the DFLTGRP of the target user, which can trigger other password policy rules (especially C4R.USER.PASSWORD.=DFLTGRP).

RANDOM
zSecure Command Verifier generates a RANDOM value for the password.

Values that are accepted for the APPLDATA field: RACF password and password phrase

blank
This value is used to indicate that the RACF SETROPTS value must be used as a default / maximum

interval
The interval must be specified bythree digits (including leading zeros).

NEVER
The password interval is set to never. This results in a password that never expires. Note that RACF requires more authorization to specify this value. If the terminal user lacks this authorization, the command is failed.

other
This is an error. The RACF **SETROPTS** value is used as maximum.

Profiles that are used for other user settings

The entries in this table reflect the keywords that are specified on the **ADDUSER** and **ALTUSER** command.

Command	Keyword	Profile	APPLDATA used?
ADDUSER **ALTUSER**	NAME	C4R.USER.NAME.*owner.userid*	
ADDUSER **ALTUSER**	(NO)DATA	C4R.USER.INSTDATA.*owner.userid*	Yes. See Values accepted for the APPLDATA field: Other User Settings.
ADDUSER **ALTUSER**	(NO)CLAUTH	C4R.USER.CLAUTH.*class.owner.userid*	
ADDUSER **ALTUSER**	(NO)SECLABEL	C4R.USER.SECLABEL.*seclabel.owner.userid*	
ADDUSER **ALTUSER**	ADD/DEL CATEGORY	C4R.USER.CATEGORY.*category.owner.userid*	
ADDUSER **ALTUSER**	(NO)SECLEVEL	C4R.USER.SECLEVEL.*seclevel.owner.userid*	

Command	Keyword	Profile	APPLDATA used?
ADDUSER **ALTUSER**	(NO)MODEL	C4R.USER.MODEL.*owner.userid*	
ADDUSER **ALTUSER**	(NO)WHEN	C4R.USER.WHEN.*owner.userid*	

Values that are accepted for the APPLDATA field: other user settings

Format-Name
The name of the format that must be used for the installation data of the user ID. The *Format-Name* is used to locate the appropriate set of format profiles.

Group-related profiles

Profiles that are used for verification of RACF GROUP

The entries in this table reflect the keywords that describe the name of new and deleted groups.

Keyword	Value	Profile
ADDGROUP	*groupname*	C4R.GROUP.ID.=RACUID(*n*)
ADDGROUP	*groupname*	C4R.GROUP.ID.=RACGPID(*n*)
ADDGROUP	*groupname*	C4R.GROUP.ID.*group*
DELGROUP	*groupname*	C4R.GROUP.DELETE.*group*
DELGROUP	*groupname*	C4R.GROUP.DELETE.=UNIVERSAL

Profiles that are used for mandatory values of RACF GROUP place-related command/keywords

The entries in this table reflect the mandatory values for keywords that describe the hierarchy of new groups

Command	Keyword	Profile	APPLDATA used?
ADDGROUP	*group*	C4R.GROUP.=SUPGRP.*group*	Yes. See Values accepted for the APPLDATA field (SUPGRP): RACF GROUP Place Related Command/Keywords.
ADDGROUP	*group*	C4R.GROUP.=OWNER.*group*	Yes. See Values accepted for the APPLDATA field (OWNER).

Profiles that are used for default values of RACF GROUP place-related command/keywords

The entries in this table reflect the default values for keywords that describe the hierarchy of new groups.

Command	Keyword	Profile	APPLDATA used?
ADDGROUP	*group*	C4R.GROUP./SUPGRP.*group*	Yes. See Values accepted for the APPLDATA field (SUPGRP): RACF GROUP Place Related Command/Keywords.

Command	Keyword	Profile	APPLDATA used?
ADDGROUP	*group*	C4R.GROUP./OWNER.*group*	Yes. See Values accepted for the APPLDATA field (OWNER).

Values that are accepted for the APPLDATA field (SUPGRP): RACF GROUP place-related command/keywords

BLANK
This is used to indicate that RACF default processing must be used. The current group of the terminal user is used.

userid
This invalid entry is not caused by incorrect entry by the terminal user. Therefore, the command is allowed to continue (with the current group of the terminal user).

group
This group is inserted. If the terminal user has insufficient access to this group, the command is failed by RACF.

=OWNER
Reflects the OWNER as specified (or defaulted) by the OWNER keyword on the command. This keyword can also be an OWNER value as inserted by zSecure Command Verifier. If the owner resolves to the special value =SUPGRP (indicating the superior group), the command is failed.

=MYOWNER
Reflects the OWNER of the terminal user. This value must be a group. All other situations are considered an error. Because these errors are not caused by incorrect entry by the terminal user, the command is allowed to continue (with the current GROUP of the terminal user).

=GROUP(*n*)
Reflects the first n characters of the new GROUP itself. This value must be a GROUP. All other situations are considered an error, and the current GROUP of the terminal user is used instead.

=RACGPID
Reflects the GROUP that was used to allow definition of the USERID by =RACGPID(n). This value is only used if =RACGPID(n) was used to allow definition. In all other situations, the APPLDATA value =RACGPID is considered an error, and the current group of the terminal user is used instead.

Values that are accepted for the APPLDATA field (OWNER)

BLANK
zSecure Command Verifier inserts the RACF default (the terminal user) as explicit value for the OWNER.

userid
The user ID found is inserted as the owner.

group
The specified GROUP used as OWNER of the new group.

=SUPGRP
Reflects the superior group (SUPGRP) as specified (or defaulted) on the command. If this value resolves to the special value =OWNER the command failed.

=MYOWNER
The OWNER of the terminal user is inserted as the value for the owner.

=GROUP(*n*)
Reflects the first n characters of the new USERID itself. This value must be a USERID of GROUP. All other situations are considered an error, and the current GROUP of the terminal user is used instead.

=RACGPID
Reflects the GROUP that was used to allow definition of the GROUP by =RACGPID(n). This value is only used if =RACGPID(n) was used to allow definition. In all other situations, the APPLDATA value =RACGPID is considered an error, and the current group of the terminal user is used instead.

Profiles that are used for verification of RACF GROUP

The entries in this table reflect the keywords that are specified by the terminal user that describe the name and place of new or changed groups.

Command	Keyword	Profile
ADDGROUP **ALTGROUP**	SUPGRP	C4R.GROUP.SUPGRP.=RACUID(*n*)
ADDGROUP **ALTGROUP**	SUPGRP	C4R.GROUP.SUPGRP.=RACGPID(*n*)
ADDGROUP **ALTGROUP**	SUPGRP	C4R.GROUP.SUPGRP.*supgrp.group*
ADDGROUP **ALTGROUP**	SUPGRP	C4R.GROUP.SUPGRP./SCOPE.*supgrp.group*
ADDGROUP **ALTGROUP**	SUPGRP	C4R.GROUP.SUPGRP./OWNER.*supgrp.group*
ADDGROUP **ALTGROUP**	OWNER	C4R.GROUP.OWNER.=RACUID(*n*)
ADDGROUP **ALTGROUP**	OWNER	C4R.GROUP.OWNER.=RACGPID(*n*)
ADDGROUP **ALTGROUP**	OWNER	C4R.GROUP.OWNER.=GROUP(*n*)
ADDGROUP **ALTGROUP**	OWNER	C4R.GROUP.OWNER.*owner.group*
ADDGROUP **ALTGROUP**	OWNER	C4R.GROUP.OWNER./SCOPE.*owner.group*
ADDGROUP **ALTGROUP**	OWNER	C4R.GROUP.OWNER./GROUP.*owner.group*
ADDGROUP **ALTGROUP**	OWNER	C4R.GROUP.OWNER./SUPGRP.*owner.group*

Profiles that are used for RACF attributes

The entries in this table reflect the keywords that are specified on the **ADDGROUP** and **ALTGROUP** command.

Command	Keyword	Profile	APPLDATA used?
ADDGROUP		C4R.GROUP.=ATTR.owner.*group*	Yes Values that are accepted for the APPLDATA are TERMUACC , NOTERMUACC, and UNIVERSAL
ADDGROUP	UNIVERSAL	C4R.GROUP.ATTR.UNIVERSAL.*owner.group*	
ADDGROUP **ALTGROUP**	(NO)TERMUACC	C4R.GROUP.ATTR.TERMUACC.*owner.group*	
ADDGROUP **ALTGROUP**	(NO)DATA	C4R.GROUP.INSTDATA.*owner.group*	
ADDGROUP **ALTGROUP**	(NO)MODEL	C4R.GROUP.MODEL.*owner.group*	

User-to-group connections

Profiles that are used to control self-authorization

The entries in this table reflect the keywords that describe the ACL entries or CONNECTs.

Keyword	Value	Profile
PERMIT	*userid*	C4R.class.ACL.=RACUID.*access.profile*
PERMIT	*group*	C4R.class.ACL.=RACGPID.*access.profile*
CONNECT	*userid*	C4R.CONNECT.ID.*group*.=RACUID
REMOVE	*userid*	C4R.REMOVE.ID.*group*.=RACUID

Profiles that are used for RACF CONNECTION-related command/keywords

The entries in this table reflect the user and group of newly defined connections.

Keyword	Value	Profile
CONNECT	GROUP(*group*)	C4R.CONNECT.ID.=USERID(*n*)
CONNECT	*userid* GROUP(*group*))	C4R.CONNECT.ID.*group.userid*
CONNECT	*userid* GROUP(*group*))	C4R.CONNECT.ID./USRSCOPE.*group.userid*
CONNECT	*userid* GROUP(*group*))	C4R.CONNECT.ID./GRPSCOPE.*group.userid*
CONNECT	*userid* GROUP(*group*))	C4R.CONNECT.ID.=DSN.*group.userid*
REMOVE	*userid* GROUP(*group*))	C4R.REMOVE.ID.*group.userid*

Profiles that are used for RACF CONNECTION-related command/keywords

The entries in this table reflect the keywords that are specified on the **ADDUSER**, **ALTUSER**, and **CONNECT** commands.

Command	Keyword	Profile	APPLDATA used?
CONNECT	OWNER	C4R.CONNECT.=OWNER.*group.userid*	Yes. See Values accepted for the APPLDATA field for RACF CONNECTION related Command/Keywords (OWNER).
CONNECT	OWNER	C4R.CONNECT./OWNER.*group.userid*	Yes. See Values accepted for the APPLDATA field for RACF CONNECTION related Command/Keywords (OWNER).
CONNECT **ADDUSER**	AUTH(*auth*)	C4R.CONNECT.=AUTH.*group.userid*	Yes. See Values accepted for the APPLDATA field for RACF CONNECTION related Command/Keywords (AUTH).
CONNECT **ADDUSER**	AUTH(*auth*)	C4R.CONNECT./AUTH.*group.userid*	Yes. See Values accepted for the APPLDATA field for RACF CONNECTION related Command/Keywords (AUTH).
CONNECT **ADDUSER**	UACC(*uacc*)	C4R.CONNECT.=UACC.*group.userid*	Yes. See Values accepted for the APPLDATA field for RACF CONNECTION related Command/Keywords (UACC).
CONNECT **ADDUSER**	UACC(*uacc*)	C4R.CONNECT./UACC.*group.userid*	Yes. See Values accepted for the APPLDATA field for RACF CONNECTION related Command/Keywords (UACC).

Values that are accepted for the APPLDATA field for RACF CONNECTION-related command/keywords (OWNER)

BLANK
This value explicitly indicates that the RACF default behavior is to be accepted. The terminal user is inserted as the owner of the user to group connection.

=GROUP
The group part of the CONNECT is to become the owner of the CONNECT profile.

=USERID
The user part of the CONNECT is to become the owner of the CONNECT profile.

value
The specified value is inserted. If the specified value is not an existing RACF USERID or GROUP, the current GROUP of the terminal is used instead.

Values that are accepted for the APPLDATA field for RACF CONNECTION-related command/keywords (AUTH)

auth
Any of the possible connect authorization levels (USE, CREATE, CONNECT, JOIN). The value is inserted as the CONNECT authorization for this USER CONNECT.

other
This is considered an error. The RACF default CONNECT authorization (USE) is used instead.

Values that are accepted for the APPLDATA field for RACF CONNECTION-related command/keywords (UACC)

auth
Any of the possible uacc values (NONE/READ/UPDATE/CONTROL/ALTER). The value is inserted as the UACC for this CONNECT / USER.

other
This is considered an error. The RACF default UACC level (NONE) is used instead.

Profiles that are used for RACF attributes and authorizations

The entries in this table reflect the keywords that are specified on the **CONNECT** command.

Keyword	Value	Profile
CONNECT	OWNER(*owner*)	C4R.CONNECT.OWNER.*owner.group.userid*
CONNECT ADDUSER ALTUSER	AUTH(*auth*)	C4R.CONNECT.AUTH.*auth.group.userid*
CONNECT ADDUSER ALTUSER	UACC(*uacc*)	C4R.CONNECT.UACC.*uacc.group.userid*
CONNECT	SPECIAL	C4R.CONNECT.ATTR.SPECIAL..*group.userid*
CONNECT	OPERATIONS	C4R.CONNECT.ATTR.OPERATIONS..*group.userid*
CONNECT	AUDITOR	C4R.CONNECT.ATTR.AUDITOR..*group.userid*
CONNECT	ADSP	C4R.CONNECT.ATTR.ADSP..*group.userid*
CONNECT	GRPACC	C4R.CONNECT.ATTR.GRPACC..*group.userid*
CONNECT	REVOKE	C4R.CONNECT.ATTR.REVOKE..*group.userid*
CONNECT	RESUME	C4R.CONNECT.ATTR.RESUME..*group.userid*
CONNECT	REVOKEDT	C4R.CONNECT.ATTR.REVOKEDT..*group.userid*
CONNECT	RESUMEDT	C4R.CONNECT.ATTR.RESUMEDT..*group.userid*

Data sets and general resource-related profiles

General policies

C4R.LISTDSD.TYPE.AUTO.*hlq.rest-of-profile*	Automatically list best fitting generic.
C4R.*class*./FROM.*hlq.rest-of-profile*	Automatic modeling on current best fit.
C4R.*class*.=FROM.*hlq.rest-of-profile*	Automatic modeling on existing profile.
C4R.*class*.FROM.*hlq.rest-of-profile*	Use of FROM keyword to model on existing profile.

Authority to manage your own data set profiles

Command	Keyword	Profile
ADDSD **DELDSD** **ALTDSD** **PERMIT**	*profile*	C4R.DATASET.ID.=RACUID.*rest-of-profile*

Authority to manage your own access

Command	Keyword	Profile
PERMIT	*userid*	C4R.*class*.ACL.=RACUID.*access.profile*
PERMIT	*group*	C4R.*class*.ACL.=RACGPID.*access.profile*
CONNECT	*userid*	C4R.CONNECT.ID.*group*.=RACUID
REMOVE	*userid*	C4R.REMOVE.ID.*group*.=RACUID

Create more specific profiles

Command	Keyword	Profile
ADDSD **RDEFINE**	*profile*	C4R.*class*.=UNDERCUT.*current-profile*

Locked resource profiles

Command	Keyword	Profile	APPLDATA used?
ADDSD **DELDSD** **ALTDSD** **PERMIT**	*profile*	C4R.DATASET.=NOCHANGE.*dsname*	Yes
RDEF **RDEL** **RALT** **PERMIT**	*profile*	C4R.*class*.=NOCHANGE.*profile*	Yes
ADDSD **DELDSD** **ALTDSD** **PERMIT**	*profile*	C4R.DATASET.=NOUPDATE.*dsname*	Yes
RDEF **RDEL** **RALT** **PERMIT**	*profile*	C4R.*class*.=NOUPDATE.*profile*	Yes

Values that are accepted for the APPLDATA field

LEVEL=*nn*
The LEVEL of the profile is used to indicate whether more controls on modification of the target resource profile are required.

Profiles that are used for verification of RACF resources

The entries in this table reflect the Keywords that describe the name of new Resources.

Command	Keyword	Profile
ADDSD **DELDSD**	*profile*	C4R.DATASET.ID.*hlq.rest-of-profile*
RDEFINE **RDELETE**	*profile*	C4R.*class*.ID.*profile*
RDEFINE **RALTER**	ADDMEM	C4R.*class*.ID.*member*
RDEFINE **RALTER**	DELMEM	C4R.*class*.ID.*member*

Profiles that are used for owner of resource profiles

The entries in this table reflect the commands and keywords that describe the mandatory or default value for the OWNER of new resource profiles.

Command	Keyword	Profile	APPLDATA used?
ADDSD	*profile*	C4R.DATASET.=OWNER.*profile*	Yes. See Values accepted for the APPLDATA field for Owner of Resource Profiles.

Command	Keyword	Profile	APPLDATA used?
ADDSD	*profile*	C4R.DATASET./OWNER.*profile*	Yes. See Values accepted for the APPLDATA field for Owner of Resource Profiles.
RDEFINE	*profile* *class*	C4R.*class*.=OWNER.*profile*	Yes. See Values accepted for the APPLDATA field for Owner of Resource Profiles.
RDEFINE	*profile* *class*	C4R.*class*./OWNER.*profile*	Yes. See Values accepted for the APPLDATA field for Owner of Resource Profiles.

Values that are accepted for the APPLDATA field for owner of resource profiles

BLANK
Any specified value of the new OWNER is suppressed, and replaced by the current GROUP of the terminal user.

=HLQ
Reflects the High Level Qualifier (HLQ) of the resource profile. This setting usually makes sense only for DATASET profiles. If the HLQ is not an existing USERID of GROUP, the current group of the terminal user is used instead.

=MYOWNER
Reflects the OWNER of the terminal user. If this owner is an existing USERID or GROUP, the value is used as the OWNER of the new resource profile. Otherwise, the current group of the terminal user is used instead.

other
The specified USERID or GROUP is used as OWNER of the new resource profile. If this owner is not an existing USERID or GROUP, the current group of the terminal user is used instead.

Profiles that are used for Owner of Resource profiles

The entries in this table reflect the commands and keywords that the Terminal User specified to describe the Owner of new or changed Resource Profiles.

Command	Keyword	Profile
ADDSD **ALTDSD**	*profile* *owner*	C4R.DATASET.OWNER.=RACUID(*n*)
ADDSD **ALTDSD**	*profile* *owner*	C4R.DATASET.OWNER.=RACGPID(*n*)
ADDSD **ALTDSD**	*profile* *owner*	C4R.DATASET.OWNER.=HLQ(*n*)
ADDSD **ALTDSD**	*profile* *owner*	C4R.DATASET.OWNER.*owner.profile*
ADDSD **ALTDSD**	*profile* *owner*	C4R.DATASET.OWNER./SCOPE.*owner.profile*
ADDSD **ALTDSD**	*profile* *owner*	C4R.DATASET.OWNER./GROUP.*owner.profile*
ADDSD **ALTDSD**	*profile* *owner*	C4R.DATASET.OWNER./HLQ.*owner.profile*
RDEFINE **RALTER**	*profile* *class* *owner*	C4R.*class*.OWNER.=RACUID(*n*)

Command	Keyword	Profile
RDEFINE **RALTER**	*profile* *class* *owner*	C4R.*class*.OWNER.=RACGPID(*n*)
RDEFINE **RALTER**	*profile* *class* *owner*	C4R.*class*.OWNER.=HLQ(*n*)
RDEFINE **RALTER**	*profile* *class* *owner*	C4R.*class*.OWNER.*owner.profile*
RDEFINE **RALTER**	*profile* *class* *owner*	C4R.*class*.OWNER./SCOPE.*owner.profile*
RDEFINE **RALTER**	*profile* *class* *owner*	C4R.*class*.OWNER./GROUP.*owner.profile*
RDEFINE **RALTER**	*profile* *class* *owner*	C4R.*class*.OWNER./HLQ.*owner.profile*

Profiles that are used for verification of RACF access

The entries in this table reflect the commands and keywords that are used to manage access.

Command	Keyword	Profile	APPLDATA used?
ADDSD **RDEFINE**	*profile*	C4R.*class*.=UACC.*profile*	Yes. Values that are accepted for the APPLDATA are NONE, EXECUTE, READ, UPDATE, CONTROL, or ALTER.
ADDSD **RDEFINE**	*profile*	C4R.*class*./UACC.*profile*	Yes. Values that are accepted for the APPLDATA are NONE, EXECUTE, READ, UPDATE, CONTROL, or ALTER.
ADDSD **RDEFINE** **ALTDSD** **RALTER**	*profile*	C4R.*class*.UACC.*uacc.profile*	
PERMIT	*userid*	C4R.*class*.ACL.=RACUID.*access.profile*	
PERMIT	*group*	C4R.*class*.ACL.=RACGPID.*access.profile*	
PERMIT	*profile* ID(*id*)	C4R.*class*.ACL.=PUBLIC.*profile*	
PERMIT	*profile* ID(*userid*) AC(*access*)	C4R.*class*.ACL.*user.access.profile*	
PERMIT	*profile* ID(*userid*) AC(*access*)	C4R.*class*.ACL.=STAR.*access.profile*	
PERMIT	*profile* FROM(*model*)	C4R.*class*.ACL.=FROM.*profile*	
PERMIT	*profile* RESET(*standard*)	C4R.*class*.ACL.=RESET.*profile*	
PERMIT	*profile* ID(*group*)	C4R.*class*.ACL.=DSN.*group.profile*	
PERMIT	*profile* ID(*userid*)	C4R.*class*.ACL./GROUP.*userid.profile*	
PERMIT	*profile* ID(*userid*)	C4R.*class*.ACL./GROUP.=HLQTYPE.USER	
PERMIT	*profile* ID(*userid*)	C4R.*class*.ACL./GROUP.=HLQTYPE.GROUP	
PERMIT	*profile* ID(*userid*)	C4R.*class*.ACL./SCOPE.*userid.profile*	

Command	Keyword	Profile	APPLDATA used?
PERMIT	*profile* FROM(*model*)	C4R.*class*.ACL.=FROM.*profile*	

Policy profiles for the conditional access list

The entries in this table reflect the policy profiles that are used to control the CLASS specified for the conditional access list.

Command	Keyword	Profile
PERMIT	*profile* WHEN(*whenclass*)	C4R.*class*.CONDACL.*whenclass.profile* Possible values for the *whenclass* are APPCPORT, CONSOLE, JESINPUT, PROGRAM, TERMINAL, SYSID, SERVAUTH, and SQLROLE.
PERMIT	*profile* RESET(*when*)	C4R.*class*.CONDACL.=RESET.*profile*

Profiles that are used for resource profile settings

The entries in this table reflect the keywords that are specified on the RACF commands.

Command	Keyword	Profile	APPLDATA used?
ADDSD	*noset* *setonly*	C4R.DATASET.RACFIND.*set-value.profile*	
ADDSD **RDEFINE**	*generic* *model* *tape* *other*	C4R.*class*.TYPE.*type-value.profile*	
ADDSD **ALTDSD** **RDEFINE** **RALTER**	NO(WARNING)	C4R.*class*.ATTR.WARNING.*profile*	
ADDSD **ALTDSD** **RDEFINE** **RALTER**	(NO)DATA	C4R.*class*.INSTDATA.*profile*	Yes. Values that are accepted for the APPLDATA field: *format* The name of the format that must be used for the installation data of the profile. The Format name is used to locate the appropriate set of format profile
ADDSD **ALTDSD** **RDEFINE** **RALTER**	(NO)NOTIFY	C4R.*class*.NOTIFY.*notify-id.profile*	
RDEFINE **RALTER**	APPLDATA	C4R.*class*.APPLDATA.*profile*	
ADDSD **ALTDSD** **RDEFINE** **RALTER**	(NO)SECLABEL	C4R.*class*.SECLABEL.*seclabel.profile*	
ADDSD **ALTDSD** **RDEFINE** **RALTER**	ADD/DEL CATEGORY	C4R.*class*.CATEGORY.*category.profile*	
ADDSD **ALTDSD** **RDEFINE** **RALTER**	(NO)SECLEVEL	C4R.*class*.SECLEVEL.*seclevel.profile*	
ADDSD **ALTDSD** **RDEFINE** **RALTER**	*level*	C4R.*class*.LEVEL.*level.profile*	

Command	Keyword	Profile	APPLDATA used?
ADDSD **ALTDSD**	RETPD	C4R.*class*.RETPD.*profile*	

Profiles that are used for resource profile settings

The entries in this table reflect the remaining resource profile attributes that can be controlled by zSecure Command Verifier.

Command	Keyword	Profile
RDEFINE **RALTER**	SINGLEDSN	C4R.*class*.ATTR.SINGLEDSN.*profile*
RDEFINE **RALTER**	TVTOC	C4R.*class*.ATTR.TVTOC.*profile*
RDEFINE **RALTER**	TIMEZONE	C4R.*class*.ATTR.TIMEZONE.*profile*
RDEFINE **RALTER**	WHEN	C4R.*class*.ATTR.WHEN.*profile*
ADDSD **ALTDSD**	NO(ERASE)	C4R.*class*.ATTR.ERASE.*profile*

Installation data format specification

Profiles that are used for INSTDATA verification

The entries in this table reflect the Class and the corresponding policy profiles.

Class	Profile	APPLDATA used?
USER	C4R.USER.INSTDATA.*owner.userid*	*Format-Name* See Values accepted for the APPLDATA field for INSTDATA verification.
GROUP	C4R.GROUP.INSTDATA.*owner.group*	*Format-Name* See Values accepted for the APPLDATA field for INSTDATA verification.
DATASET	C4R.DATASET.INSTDATA.*hlq.rest-of-profile*	*Format-Name* See Format rules used for INSTDATA verification.
class	C4R.*class*.INSTDATA.*profile*	*Format-Name* See Format rules used for INSTDATA verification.
class	C4R.*class*.INSTDATA.=FMT.*format-name*.POS(*start:end*)	*Format-Rule* See Format rules used for INSTDATA verification.
class	C4R.*.INSTDATA.=FMT.*format-name*.POS(*start:end*)	*Format-Rule* See Format rules used for INSTDATA verification.

Values that are accepted for the APPLDATA field for INSTDATA verification

format
The name of the format that must be used for the installation data of the profile. The format name is used to locate the appropriate set of format profiles.

Format rules that are used for INSTDATA verification

The entries in this table contain the format rule and a description of the rule.

NB NonBlank. The specified part of the installation data field cannot consist of all blanks.

NC NoChange. The current value of the specified part of the installation data cannot be modified.

ALPHA
Alphabetics. The specified part of the installation data field can contain only alphabetic characters or blanks.

NUM
Numerics. The specified part of the installation data field can contain only numeric characters or blanks.

ALPHANUM
Alphanumerics. The specified part of the installation data field can contain only alphabetic or numeric characters or blanks.

PICT(*picture-string***)**
Picture format. The specified part of the installation data field must match the Picture-String format.

LIST(*values***)**
List of allowed values for the specified part of the installation data field.

LISTX(*values***)**
List of not allowed values for the specified part of the installation data field.

=USERID
Any valid RACF USERID.

=GROUP
Any valid RACF GROUP.

The format rules that are used for INSTDATA verification include a possibility for a picture-string. The picture characters that can be specified in the PICT format are given in Picture characters that can be specified in the PICT format.

Picture characters that can be specified in the PICT format

The following entries describe the supported picture string characters.

Numeric character (0-9).

@ Alphabetic character (A to Z).

***** Alphanumeric character (A-Z, 0-9).

**$** Special character (@#$).

. Anything. No verification is done.

Other
Literal value. The installation data character must be identical to the `Picture-String` character.

Segment management functions

Profiles that are used for verification of UNIX ID values

The entries in this table reflect the Class, Segment, and Field and the corresponding policy profiles.

Class	Segment	Field	Profile
USER	OMVS	*UID*	C4R.USER.OMVS.UID.*uid.owner.userid*
USER	OMVS	*UID*	C4R.USER.OVM.UID.*uid.owner.userid*
GROUP	OMVS	*GID*	C4R.GROUP.OMVS.GID.*gid.owner.group*
GROUP	OMVS	*GID*	C4R.GROUP.OVM.GID.*gid.owner.group*

Profiles that are used for verification of STDATA values

The entries in this table reflect the Class, Segment, and Field and the corresponding policy profiles.

Class	Field	Profile
STARTED	PRIVILEGED	C4R.STARTED.STDATA.ATTR.PRIVILEGED.*started-profile*
STARTED	TRUSTED	C4R.STARTED.STDATA.ATTR.TRUSTED.*started-profile*
STARTED	TRACE	C4R.STARTED.STDATA.ATTR.TRACE.*started-profile*
STARTED		C4R.STARTED.STDATA.=USER.*started-profile*
STARTED		C4R.STARTED.STDATA./USER.*userid.started-profile*
STARTED	*userid*	C4R.STARTED.STDATA.USER.*started-profile*
STARTED	NOUSER	C4R.STARTED.STDATA.USER.=NONE.*started-profile*
STARTED		C4R.STARTED.STDATA.=GROUP.*started-profile*
STARTED		C4R.STARTED.STDATA./GROUP.*started-profile*
STARTED	*group*	C4R.STARTED.STDATA.*started-profile*
STARTED		C4R.STARTED.STDATA.GROUP.*started-profile*
STARTED	NOGROUP	C4R.STARTED.STDATA.GROUP.=NONE.*started-profile*

Chapter 12. zSecure Visual resources

zSecure Visual is a Windows-based interface that provides a subset of the features that are provided by zSecure Admin, enabling decentralized RACF administration. This product is generally meant for helpdesk personnel that has little or no knowledge of mainframes.

Admin	Audit for RACF	Audit for ACF2	Audit for Top Secret	Resource name that is checked	
■				C2R.CLIENT.*option*	(discrete required)
■				C2R.SERVER.ADMIN	(discrete required)

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web

sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not

been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, Acrobat, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Printed in USA

SC27-5646-00