Getting Started
Security zSecure Admin and Audit for RACF
Version 2.1.0

Getting Started

IBM
Before using this information and the product it supports, read the information in "Notices" on page 125.

September 2013

This edition applies to version 2, release 1, modification 0 of IBM Security zSecure Admin for RACF (product number 5655-N16) and IBM Security zSecure Audit for RACF (product number 5655-N17) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 1989, 2013.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
## Contents

### About this publication
- Intended audience
- What this publication contains
- Access to publications and terminology
- Related documentation
- Technical training
- Support information
- Statement of Good Security Practices

### Chapter 1. Overview
- CARLa auditing and reporting language
- Data sources
  - CKFREEZE data sets
  - Remote data and command routing

### Chapter 2. Basic operations
- Before you begin
- Starting the products
- Maintaining RACF profiles
- Displaying user profiles
  - Using the User selection panel
  - Filter notation
  - Date notation
  - Showing application segments
- Displaying group profiles
  - Universal groups
  - Connecting and removing users
- Reviewing data set profiles
- Listing profiles in warning mode
- Displaying discrete profiles
- Displaying the access control list (ACL)
- Access control list formats
- Access list display settings
  - Changing the access list display settings from the Setup View panel
  - Changing the access list display settings from the Setup panel
- Checking access to resources with the Access command
- Administration of access rights
- Creating digital certificates templates
- Working with certificates, key rings, filters, and tokens
- Comparing users

### Chapter 3. Administration of users and profiles
- Generating and confirming RACF commands
- Performing a mass update
- Copying a user
- Delete a user with all references
- Re-create a profile
- Merge and compare profiles
- Redundant profile management
- Displaying data structures
- Running SETROPTS reports and viewing class settings

### Chapter 4. Distributed and scoped administration functions
- Group Administration with RACF scope
- The Quick Administration panel
  - Accessing the Quick Administration panel in a stand-alone way
  - Accessing the Quick Administration panel with RA.Q
- Group administration through CKGRACF
- Single panel Helpdesk function
  - Accessing the Helpdesk function in a stand-alone way
  - Accessing the Helpdesk function with RA.H
- Helpdesk password administration functions
- Tailoring the Helpdesk

### Chapter 5. Setup functions for managing data
- Adding data
- Adding new files
- Refreshing and loading files
- Selecting the input set
- Specifying collections of input sets
- Other Setup parameters
  - INSTDATA parameter
  - View and Confirm options
  - SMTP options for email output
  - Command execution control
- Changing and verifying values
  - Line commands for common tasks

### Chapter 6. Creating and viewing a report
- Results panel
- Archiving report output
- Mailing report output

### Chapter 7. Verify functions
- Running the Verify functions
- Running the Verify functions for the first time

### Chapter 8. Auditing system integrity and security

### Chapter 9. Rule-based compliance evaluation
- Reporting
<table>
<thead>
<tr>
<th>Chapter 10. SMF data queries</th>
<th>87</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining input sets</td>
<td>88</td>
</tr>
<tr>
<td>Creating SMF reports</td>
<td>90</td>
</tr>
<tr>
<td>Auditing types of users</td>
<td>92</td>
</tr>
<tr>
<td>Change tracking</td>
<td>93</td>
</tr>
<tr>
<td>Library change detection</td>
<td>94</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 11. Resource-based reports for RACF resources</th>
<th>97</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Stack reports</td>
<td>97</td>
</tr>
<tr>
<td>UNIX file system reports</td>
<td>98</td>
</tr>
<tr>
<td>CICS region and resource reports</td>
<td>102</td>
</tr>
<tr>
<td>CICS region reports</td>
<td>102</td>
</tr>
<tr>
<td>CICS transaction reports</td>
<td>103</td>
</tr>
<tr>
<td>CICS program reports</td>
<td>104</td>
</tr>
<tr>
<td>IMS region and resource reports</td>
<td>105</td>
</tr>
<tr>
<td>IMS region reports</td>
<td>105</td>
</tr>
<tr>
<td>IMS transaction reports</td>
<td>106</td>
</tr>
<tr>
<td>IMS PSB reports</td>
<td>107</td>
</tr>
<tr>
<td>DB2 region and resource reports</td>
<td>108</td>
</tr>
<tr>
<td>Trust relations reports</td>
<td>109</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 12. CARLa commands</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browsing the SCKRCARL library</td>
<td>112</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 13. Typical administration and audit tasks</th>
<th>119</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running a member of the SCKRCARL library</td>
<td>112</td>
</tr>
<tr>
<td>Customizing the CARLa program</td>
<td>115</td>
</tr>
<tr>
<td>Creating a sample CARLa program</td>
<td>116</td>
</tr>
<tr>
<td>Running a saved CARLa program</td>
<td>116</td>
</tr>
</tbody>
</table>

| Appendix. Frequently asked questions | 121 |

<table>
<thead>
<tr>
<th>Notices</th>
<th>125</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trademarks</td>
<td>127</td>
</tr>
</tbody>
</table>

| Index   | 129 |
About this publication

IBM® Security zSecure™ Admin and Audit for RACF® (Resource Access Control Facility) automates many of the recurring administrative tasks and audit reporting for RACF systems. These products rely on the zSecure Collect program to collect and analyze data from RACF and z/OS® systems, enabling you to easily monitor user access privileges, implement scoping to limit administrator privileges, and to audit user behavior. These products also enhance the administrative and reporting functions of RACF systems, facilitating security monitoring and decentralizing system administration.

This document is intended to help you learn the basics of using IBM Security zSecure Admin and Audit for RACF. After working through this document, you should have a working understanding of these products and the ability to explore other product features.

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 systems administration and be comfortable using the Interactive System Productivity Facility (ISPF).

What this publication contains

The purpose of this document is to help you quickly become familiar with IBM Security zSecure Admin and Audit for RACF. This document is not a full reference manual and does not cover all features. The material focuses on the interactive features (using ISPF panels) and highlights the major functions of IBM Security zSecure Admin and Audit for RACF.

Except for a few introductory pages, this document is intended as a hands-on guide while you work with IBM Security zSecure Admin and Audit for RACF. The publication explains how to use IBM Security zSecure Admin and Audit for RACF to perform common administration tasks and how to audit and run reports on RACF systems.

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

- **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.

  Describes the IBM Security zSecure Audit for Top Secret product features and provides user instructions for performing standard tasks and procedures.

  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.

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.

  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.

  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](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](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](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**

---

*About this publication vii*
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


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


Related documentation

For more detailed information about the IBM Security zSecure Admin and Audit for RACF components, see the IBM Security zSecure Admin and Audit for RACF User Reference Manual (LC27-5639).

This publication is provided on the IBM Security zSecure Documentation CD (LCD7-5373) provided with IBM Security zSecure Admin and Audit for RACF. You can download the Documentation CD when you order and download the product.

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. Overview

IBM Security zSecure Admin for RACF and IBM Security zSecure Audit for RACF are two distinct but complementary products that you can use to administer and audit RACF systems.

zSecure Admin provides RACF management and administration at the system, group, and individual levels along with RACF command generation. zSecure Audit provides RACF and z/OS monitoring, Systems Management Facility (SMF) reporting, z/OS integrity checking, change tracking, and library change detection. Both products provide displaying, reporting and verifying functionality for RACF profiles and show the z/OS tables that describe the Trusted Computing Base (TCB). Figure 1 shows the functionality available in each product and shows the complementary functionality that is provided in both products.

zSecure Admin and zSecure Audit for RACF are licensed individually, but can be used together.

Figure 1. zSecure Admin and zSecure Audit product functions

The primary processing programs are large modules that can be used in batch or interactive mode. Interactive mode is most common, although batch mode can be useful for automated, periodic checks and for producing daily reports.

zSecure Admin and zSecure Audit provide an interactive user interface that is implemented in ISPF by using the panel, skeleton, and message libraries that are supplied with zSecure. ISPF is the main program that runs during an interactive session, calling the zSecure application program as needed. The interactive panels call the CKRCARLA load module as needed.

Figure 2 on page 2 illustrates the general data flow for zSecure Admin and zSecure Audit. The user works through ISPF panels, which generate commands that are...
sent to the CKRCARLA program. The program returns results that are displayed through ISPF panels.

This general design, with separate interactive and noninteractive components, has several practical advantages:
- It separates interactive interfaces from the application program. This separation gives you more flexibility in designing and using the interfaces and programs, especially when you customize the ISPF interface.
- Any functions that can be run interactively can also be run in batch mode.
- zSecure Admin and zSecure Audit for RACF can create customized reports by using the CARLa Auditing and Reporting Language (CARLa) and run these reports from the ISPF panels.
- The products can be used remotely in cases where a TSO connection is not possible or practical, in NJE networks, for example.

**CARLa auditing and reporting language**

IBM Security zSecure Audit for RACF is command-driven and uses the CARLa Auditing and Reporting Language (CARLa). The commands are explained in the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual* (LC27-5639-00).

A typical user who uses ISPF does not need to be concerned with CARLa. The commands are generated automatically and sent to the application program.
Except for these few comments, this guide does not contain information about the CARLa command language. Instead, this guide concentrates on the use of zSecure Admin and Audit through ISPF.

The command language is generally used for the following reasons:
- To generate customized reports
- To use the product in batch mode

Because the standard reports are comprehensive, you might never need customized reports, but you can create them. Batch use is attractive as part of a security monitoring function. For example, you can use a scheduled batch job to run monitoring checks and reports automatically.

A comprehensive set of sample reports is available in the CARLa library (low-level qualifier of SCKRCARL and often referred to with the default ddname CKRCARLA).

---

**Data sources**

zSecure Admin and zSecure Audit for RACF use several different types of data. Figure 3 on page 4 provides an overview of the data sources and the processing that is done by the products.
zSecure Admin and zSecure Audit for RACF typically require RACF data. This data can come from the following sources:

- The primary live RACF database
- The backup live RACF database
- Unloaded RACF data
- A copy of a RACF database or an active RACF database from another system

zSecure produces unloaded RACF data by reading the live RACF database and creating a copy in a proprietary format suitable for high-speed searches.

If you are using zSecure Audit for RACF functions, the program might require SMF data. The SMF data can come from the live SMF data sets, SMF log streams, or sequential SMF data sets produced with the IFASMFDP or IFASMFDL programs. These IBM programs unload SMF records from the live SMF data sets and SMF log streams. Sequential SMF data sets can be on disk or tape, although TSO users might not be able to mount tapes for interactive use with many installations.

zSecure Audit cannot process pseudo-SMF files that are created by the RACF REPORT WRITER or the IRRADU00 SMF unload program.
CKFREEZE data sets

zSecure Audit for RACF uses DASD data that is provided by zSecure Collect. This program runs as a batch job and reads all online Volume Table Of Contents (VTOCs), VSAM Volume Data Set (VVDSs), catalogs, selected Partitioned Data Set (PDS) directories, and calculates digital signatures at the member and data set level when requested. It writes all this data to a CKFREEZE data set.

zSecure Admin and zSecure Audit for RACF also use z/OS control block data. zSecure Collect gathers this data at the same time that it gathers DASD data. It uses APF-authorized functions to retrieve data from other address spaces and from read-protected common storage. Additionally, batch collection permits analysis of a remote system where the data was collected.

You define input sets for zSecure Admin and zSecure Audit for RACF. For example, one set might consist only of the live RACF data. Another set might use live RACF data plus a CKFREEZE file. Another set might use unloaded RACF data, a CKFREEZE data set, and several SMF data sets. You can switch between input sets while in the ISPF environment.

Remote data and command routing

zSecure Admin and zSecure Audit support the use of remote data sets as input for creating reports and displays. Using this functionality, which is known as multi-system support, you can report on and manage multiple systems from a single session. This function is also integrated with zSecure Admin support for routing RACF commands by using zSecure services or RACF Remote Sharing Facility (RRSF) services.

Using remote data for creating reports is useful for ad hoc reporting about profiles or settings. However, this access method is less suited for queries that require processing of the entire security database or the entire CKFREEZE data set. It takes longer to access large amounts of remote data than it does to access the same data locally.

To use the multi-system support, your environment must have an active zSecure Server, which runs in a separate server address space. This server performs the necessary functions for communicating with remote systems to route commands and access RACF databases, SMF input files, CKFREEZE data sets, and other defined data sets. For more detailed information, see the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*. 
Chapter 2. Basic operations

Review the following procedures to learn how to start the zSecure Admin and Audit applications and to navigate, select, input, and manage RACF data. You can read about the following tasks:

- Viewing, managing, and maintaining RACF profiles for users, groups, and data sets
- Managing access rights
- Reporting on digital certificates
- Comparing users

Before you begin

Before you begin, verify your TSO logon parameters and screen format.

Follow the procedures outlined in this section before you use zSecure Admin and zSecure Audit for RACF.

**TSO logon parameters**

Make sure that you are logged on to TSO with a large enough region size. zSecure Admin and zSecure Audit for RACF use virtual storage to reduce I/O and to improve the response time. The amount of virtual storage depends on the size of your installation and on the information you requested. A good region size value to start with is 32 MB.

**Screen format**

zSecure Admin and Audit for RACF panels are used with 24-line and larger screens. To be most effective with 24-line screens, type `PFSHOW OFF` on the command line in any ISPF panel. Press Enter to remove the program function key definition information that ISPF automatically places in the last one or two lines of the screen. Use the `PFSHOW ON` command to restore the PF key definitions.

Starting the products

**About this task**

After installing the products, you can start the zSecure Admin and Audit applications and do typical tasks.

To get started, complete the following steps:

**Procedure**

1. Type 6 on the **Option** line and press Enter to open ISPF Command Shell.
2. Enter the command `CKR` and press Enter.
   
   This command starts the combined zSecure Admin and zSecure Audit for RACF products. After you enter the command, the Main menu opens as shown in Figure 4 on page 8.
The first time you enter this panel, only the major selection options are shown.

3. If necessary, use option SE.R to reset all your settings to the default settings.

4. To select an option, type the two-character abbreviation on the command line and press Enter.

Depending on the option that is selected, the menu either expands to show more detailed options or presents the submenu for the next selection.

When you get more familiar with the product, it can be handy to know the jump command to jump directly to any other panel within that function: *X, where X is the panel identifier. For example, on any RA panel (RACF administration), you can enter the command *=G to jump to the RA.G panel (Group administration through CKGRACF).

**What to do next**

The following sections show you how to use some of the display functions to ensure that the product is working correctly. Your live RACF database is used for input. Typically, using zSecure with the live RACF database does not cause any noticeable effects on production operations.

### Maintaining RACF profiles

#### About this task

You can maintain RACF profiles by displaying an overview of the profiles and then selecting one to maintain. The profile selection panels have fields, also known as filters, to select or to exclude data. By default, everything is selected, and nothing is excluded. To see an example, complete the following steps:

**Procedure**

1. On the Main menu, type RA (RACF Administration) in the Option line and press Enter to see the options for viewing and maintaining the RACF database.

2. Type G (Group) in the Option line and press Enter without entering any parameters in the panel.

3. At the default prompt, press Enter.
Results

After completing this procedure, zSecure Admin and zSecure Audit for RACF shows everything in the RACF database relevant to the function of the panel, group profile information in this example. You can reduce the amount of data that is shown in the panel by specifying one or two selection or exclusion parameters.

Tip: You can use the **FORALL** primary command on a record-level display to specify a command to be applied to all profiles on the current display. Without a parameter, primary command **FORALL** displays a panel where a command can be entered. You can also enter the command directly on the **FORALL** command.

This example uses the live RACF database to demonstrate the speed and non-interference of zSecure Admin and Audit with the live RACF database. [“Adding data” on page 55](#) guides you through the creation of an unloaded RACF database. The unloaded database is used for the text and examples in this guide.

What to do next

zSecure Admin helps you maintain profiles at the group and user level and at the single-entry level. You can quickly find out about the structure of groups and users, and modify structures that are based on your organizational structure.

After you learn how to use the interface and manage commands, you learn about general maintenance functions, devolved maintenance, and how the help desk can shift workload by enabling password maintenance without special authority.

Displaying user profiles

Procedure

1. If you are not in the Main menu, press PF3 to return to the Main menu.
2. Type RA (RACF Administration) in the Option line and press Enter to see the options for viewing and maintaining the RACF database.
3. From the RA menu, select option U (User). Press Enter to open the User Selection panel; see [Figure 5 on page 10](#) This panel provides some of the most frequently used selections. It consists of the following parts:
   - Add new user or segment
   - Additional selection criteria
   - Output/run options
   Depending on the selection criteria or output/run options you choose by placing a / in front of one of those options, you might go to another panel to specify more selection criteria.
4. After you make a selection, press PF3 to return to the User Selection panel or press Enter to run the query.
5. In the **Userid** field, type your user ID.

**Tip:** The additional print options are available only if the **Print format** field is activated. To activate this field, type / in the **Print format** selection field.

6. Press Enter. **zSecure Admin and Audit for RACF** searches the RACF database and opens the user profile overview panel as shown in Figure 6.

The message in the upper right line of the panel provides performance information that indicates the elapsed and processor time that is used to run the query.

This overview display shows each selected user profile on a single line. If applicable, you can scroll up and down, left and right, to view more information.

Some of the field values can be edited, for example, entries in the **Name** column. Depending on your ISPF option settings and terminal type, fields that can be edited (modified) are indicated by underscores or shown in a color that is different from the color for fields that cannot be edited, for example, the **User** field. If you type a new value over a modifiable field, **zSecure Admin** generates the appropriate native RACF command to change the profile to the new value.
7. Optional: You can change the ISPF display colors in most panels by using the following procedure:
   a. Select **Options** from the menu bar.
   b. From the Options menu, select **1. Settings**
   c. Select **Colors** from the bar.
   d. Select **2. CUA attributes**.
   e. After you specify the changes, press Enter to apply them. The changes become effective the next time you run a query.

The labels in the profile display are abbreviated as shown in Table 1.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIRP</td>
<td>Flag fields that indicate whether the profile is <strong>R</strong> Revoked, <strong>I</strong> Inactive, <strong>R</strong> Restricted, or <strong>P</strong> Protected</td>
</tr>
<tr>
<td>SOA</td>
<td>Shows the settings for the following attributes: <strong>S</strong> Special, <strong>O</strong> Operations, and <strong>A</strong> Auditor</td>
</tr>
<tr>
<td>gC</td>
<td>Show <strong>g</strong>roup Authorities Present and <strong>C</strong>lass Authority Present</td>
</tr>
</tbody>
</table>
| LCX   | Indicates whether the following conditions are true:  
  • **RA**C**LI**N**K** present (**L**)  
  • User has a certificate (**C**)  
  • Password is expired (**X**) |

These field descriptions are also available on the integrated help panels available in the ISPF interface. You can access panel-level help and field-level help on most panels. Panel help and field-sensitive help are available on all security database displays at both the record level and detail level.

- For field help, position the cursor in the field of interest and press PF1.
- For panel help, position your cursor on the command line and press PF1.

**Tip:** Many of the zSecure data displays are wider than 80 characters. To scroll right or left, use the PF11 and PF10 keys.

8. To display more detailed information about a profile, complete the following steps:
   a. Move the cursor to the beginning of the displayed profile line in the line command field and press Enter.
   b. Select an entry in the panel by using either of the following methods:
      • Position the cursor on the line command field and press Enter.
      • Type the **S** command and press Enter.

Additional line commands such as **C** (copy) and **D** (delete) are also available. These commands are covered later.

**Tips:**
- If you are unsure about the available line commands on a certain profile, type a **/** and press Enter. This action opens a panel that shows all applicable line commands.
- You can use the **FORALL** primary command on a record-level display to apply a command to all profiles on the current display. Without a parameter, the **FORALL** primary command displays a panel where a command can be entered. You can also enter the command directly on the **FORALL** command.
9. To return to the User Selection panel, press PF3. Press PF3 twice if you are in
   the detail overview.

10. Now try something a little more interesting, such as entering SYS* in the
   Userid field to display all user profiles that start with SYS*. You can inspect
   the details for these users by selecting any displayed user profile line. If you
   have appropriate authority for the RACF database, you can change many of
   these fields by editing the field value in the panel. When you specify a new
   value, zSecure checks to prevent accidental changes. For the example, do not
   make any changes.

   **Note:** When you specify selection criteria in a field, you can use the generic
   characters asterisk (*) and percent sign (%).

### Using the User selection panel

#### About this task

The User Selection panel is split into the following sections:

- Use the first section to add a user or segment.
- Use the second section to specify the most commonly used RACF management
  selection criteria.
- Use the third section mostly to report on the RACF database with more
  advanced selection criteria. For example, you can report on all user profiles that
  have the SPECIAL and OPERATIONS attributes.
- Use the fourth section to customize the resulting output from your query. For
  example, you can type / in the Show differences field to compare two input
  sources.

   To do this comparison, you must select one baseline input that is set by using
   the SETUP FILES C action command and at least one regular main set by using
   the SETUP FILES S action command.

   For more detailed information, see the IBM Security zSecure Admin and Audit for

### Procedure

1. To select fields for the advanced selection criteria (third section) and output
   customization (fourth section), place a / next to the field. Press Enter.

   **Note:** Most of the fourth section of the panel can be modified only if the Print
   format field is selected by placing a / in front of it and pressing Enter. Before
   you can use the Send as email option, you must specify SMTP configuration
   parameters. Specify the parameters in the Setup output definition panel, as
   described in [“SMTP options for email output” on page 62](#). For now, continue
   without selecting the Print format option.

   zSecure displays any user profile that matches the criteria you enter in the User
   Selection panels. If nothing is specified for a particular field, that field is
   ignored during the search. Several fields accept / The / means that the option
   is selected and profiles that match the specified parameter or parameters are
   displayed (or an additional selection panel is displayed). Most fields also accept
   the S command to activate the selection option. Blank means that the option is
   ignored for selecting profiles.

   For example, typing / in the Attributes field opens the User Attributes panel
   that is illustrated in [Figure 7 on page 13](#).
2. To display all user profiles that have system-wide authority, type `/` in the Operations field of the Systemwide and group authorizations section. Then, press Enter. This operation shows all user profiles that have system-wide Operations authority.

3. In the Connect authority field, select a user that is based on the specified connect authority. Only users that have at least one group connection that satisfies the comparison operator that is applied to the connect authority are shown. Use the comparison operators that are shown in Table 2.

### Table 2. Comparison operators for Connect authority field

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;</code></td>
<td>Less than the access specified</td>
</tr>
<tr>
<td><code>&lt;=</code></td>
<td>Less than or equal to (at most) the access specified</td>
</tr>
<tr>
<td><code>&gt;</code></td>
<td>More than the access specified</td>
</tr>
<tr>
<td><code>&gt;=</code></td>
<td>More than or equal to (at least) the access specified</td>
</tr>
<tr>
<td><code>=</code></td>
<td>Exact access</td>
</tr>
<tr>
<td><code>~</code> or <code>&lt;&gt;</code></td>
<td>All but the specified access</td>
</tr>
</tbody>
</table>

**Tip:** zSecure Admin and zSecure Audit for RACF combine all the properties that you specify with AND logic unless otherwise indicated.

Besides using `/`, you can also use `xxx Y` and `N`. By specifying the AND operator and by using `Y` and `N` values in the input fields within a group, you can find users that have the attributes that are selected with `Y` that have none of the attributes that are selected with `N`.

The Revoked option in the Logon status section checks for currently revoked users.

The Password interval field checks for users who are subject to password expiration. This field is available on the panel that displays when you specify `/` in the Other fields field on the RA.U panel. After you select this field, press Enter to open the User Attributes panel to specify the attributes for selecting data. Try searching for users with a non-expiring password and SPECIAL Menu Options Info Commands Setup

---

**Figure 7. User Attributes panel**
authority, or for users with non-expiring passwords and Operations authority.
If you find any such users, other than possibly IBMUSER, you might investigate why they are defined this way.

As another example, you can type / in the Specify scope field to examine the profiles within the scope of another user ID or group. When you select this option, a panel opens for specifying the user ID or group ID.

**Filter notation**

In many panels, the input fields accept filters for selecting or excluding data. These filters are strings that can contain any of the following wildcard characters:

- `%` Match one nonblank character.
- `*` Match any number of characters within a single string but not a dot, such as a single data set name qualifier or a user name.
- `**` Match any number of qualifiers at the end of a profile name.
- `:` Search for specified characters within a name, but not for class names or data set qualifiers.

zSecure Admin and zSecure Audit for RACF use Enhanced Generic Naming (EGN) notation whether RACF is in EGN mode.

**Date notation**

Several selection fields are meant for dates. You can use various values and operators. However, all year values must be specified in four digits. Table 3 shows examples of date selection values and operators.

**Table 3. Date selection values and operator examples**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>= 04jul2004</td>
<td>July 4, 2004</td>
</tr>
<tr>
<td>&lt; 04jul2004</td>
<td>Any day before July 4, 2004</td>
</tr>
<tr>
<td>= never</td>
<td>A date was never set</td>
</tr>
<tr>
<td>= today</td>
<td>Activity happened today</td>
</tr>
<tr>
<td>= today-3</td>
<td>Three days before today</td>
</tr>
<tr>
<td>&lt; today-30</td>
<td>More than 30 days ago</td>
</tr>
<tr>
<td>&gt; 01jan2005</td>
<td>Any day after January 1, 2005</td>
</tr>
</tbody>
</table>

A date with the value DUMPDATE is the date that your RACF database was unloaded. If you are using the live RACF database, specifying the value DUMPDATE is the same as using the value TODAY.

**Note:** When you enter dates in selection fields, you must specify an operator in the small two-character input field and the date value in the larger field.

**Showing application segments**

**Procedure**

1. To show application segments for a user profile, specify the user ID for which you want to view the application segments in the User Selection panel.
2. Enter the action command SE in front of the user profile. A panel opens with a list of application segments that are defined for this user.
Tip: Instead of using the SE action command, you can type a / in front of Show segments in the Output/run options section of the User Selection panel. This action opens a User Segments panel so that you can specify which segments you want to see. If you select Segment presence together with the Show segments field in the Additional selection criteria section, a panel opens with a list of segments. You can select a segment and specify additional selection criteria that are based on segment information. For example, you can select users that are based on output settings in the TSO segment.

Displaying group profiles

About this task

This section describes the procedure to display and query group profiles.

To display group profiles, complete the following steps:

Procedure

1. Return to the Main menu by pressing End or Return.
2. From the RA menu, select option G (Group) and press Enter to open the Group Selection panel.

This panel, which is shown in Figure 8, provides some of the most frequently used selections applicable to group profiles. Like the User Selection panel, this panel has the following sections:

- **Add New Group or Segment**
- **The common selection criteria**
- **Additional selection criteria**
- **Output/run options**

Depending on the additional selection criteria or output and run options that you select with the / character, you go to another panel to specify more selection criteria. After you make your selection, press PF3 to return to the Group Selection panel.

Figure 8. Group Selection panel
3. In the **Group id** field, type your default group or a group name string; for example, type ABC* for all group profiles that start with the string ABC in the **Group id** field.

4. Press Enter to search the RACF database and display the group profile information in the Group Overview panel.

   The display, which is shown in Figure 9, looks similar to the User Selection overview except that it now shows different columns and Group profiles instead of User profiles.

   ![Figure 9. Group Overview panel](image)

### Universal groups

All RACF profiles have a maximum size. The connect information for all connected users is stored in a normal Group profile. It implies that there is a maximum number of users that can be connected to a Group profile. The maximum number is approximately 6000 users. For large RACF databases, this number might not be sufficient. This limitation is the reason for the **universal group**. When the **UNIVERSAL** attribute is assigned to a Group profile, users with a default connection (connect to the group with **USE** authority and no connect attributes) are no longer stored in the Group profile. Only users that have a connect attribute like group-**SPECIAL**, group-**OPERATIONS**, or a connect authority that exceeds **USE** are stored in the Group profile.

The advantage of the universal group is that an unlimited number of users can be connected without its reaching the maximum size of a Group profile. So in large RACF databases, it is no longer required to split a large Group. If you do want to split a large group, make a copy of the Group and connect more users to this new Group.

The disadvantage of the universal Group is that, when the Group profile is displayed, you cannot determine which users are connected to the Group without searching all User profiles to find the users that are connected to this universal Group. In zSecure Admin and zSecure Audit you can automate this search by using the Expand universal feature.
Note: Using this feature implies a full database read, and can cause the response time to be much longer.

There are two fields that are related to the **UNIVERSAL** attribute of Group profiles: **Universal Group** and **Expand universal**. If you enter a / before **Profile** fields, a panel similar to the one shown in Figure 10 opens.

![Panel](image)

**Figure 10. Group profile field selection panel**

To use the universal groups feature, take one of the following actions:

- On the panel that is shown in Figure 10, type / in the **Universal group** field. This selection searches the RACF database for universal groups only.
- Type / in the **Expand universal** field in the Group Selection panel that is shown in Figure 8 on page 15. This selection causes all connected users, instead of just users with a non-default connect, to be displayed in the detail overview.

Tip: To see how the **Expand universal** option works, list a universal group twice: first list the group with the option enabled and then list the group with the option disabled. Notice the differences in the lists of connected users.

**Connecting and removing users**

There are several ways to connect Users to a Group:

- Issue the **CO** line command (connect) in the Group or User profile overview panel.
- Use a **C** (copy) or **D** (delete) line command in the Group or User profile detail panel that precedes a line that contains connect details of a User or Group.
- Edit (type over) the current values in the lines that contain the connect information. This action generates a new connect command for the new value that you entered, and it generates a remove command for the overwritten value. If you do not want to run the **Remove** command, delete it from the command confirmation panel before you press Enter.

When the line command **CO** is used on a user or group profile, a Connect panel opens as illustrated in Figure 11 on page 18. (For Group profiles, you can add connections for up to 10 users in one operation.)
Use the panel that is shown in Figure 11 to connect the User to another Group.

In this panel, you cannot change the Userid field. When the CO command is issued for a Group profile, the Group name field cannot be modified instead.

Optionally, you can specify connect attributes in the lower half of the panel.

When you use line command C instead of CO on a User or Group profile detail panel, you can connect the same User to another Group. You can also connect another User to the same Group. It is even possible to modify both the Userid and the Group fields in the connect panel at the same time, connecting another User to another Group.

### Reviewing data set profiles

#### About this task

This section describes how to view data set profiles, enable warning mode, and view and manage the access control list.

#### Procedure

To display data set profiles, complete the following steps:

1. To return to the Main menu, press Exit (PF3) in the Group Selection panel.
2. Select Option D to open the Data set Selection panel.

You are still in the RACF subselection panel. This panel, which is shown in Figure 12 on page 19, is typically used to inquire about data set profiles and is used in much the same way as the user profile panel.
3. Specify criteria in as many fields as you like. If nothing is entered in a field, that field is not used as a selection or rejection criterion during the database search. If you press Enter without specifying any information, all existing data set profiles are displayed, which usually results in too much data.

**Dataset profile** is the most important field on the Data set Selection panel. If you know the name of the profile you are looking for, you can specify the **Exact** specification. You can also specify an **EGN mask** that covers the profile, use **Match** to match the name of a data set to the profile that covers it, or look for all matching profiles (**Any match**). For example:

a. Type SYS1.** and empty all other fields except 1 for **EGN mask**.

Remember that in EGN, the name pattern SYS1.* (with one asterisk) matches any name with a single qualifier that follows SYS1. If you specify SYS1..** (with two asterisks), this value matches any name with any number of qualifiers behind SYS1. For example, you can look for any profile that begins with SYS by using a filter like SYS*.**.

b. Press Enter.

A panel opens showing all the data set profiles that start with SYS1 in this example. This panel is like the panel that is shown in [Figure 13 on page 20](#).
Other selection criteria are available:

- Best match result
  
  a. To exit the data set overview and return to the data set Selection panel, press PF3.
  
  b. In the Dataset profile field, type SYS1.DUMP00 and select 3 for Match and press Enter.

  A panel similar to the one shown in Figure 14 opens showing the profile best matching SYS1.DUMP00.

- Any match result
  
  a. To exit the data set overview and return to the data set Selection Panel, press PF3.
  
  b. In the Dataset profile field, leave the SYS1.DUMP00 value and select 4 for Any match and press Enter.

  A panel similar to the one shown in Figure 15 on page 21 opens showing all profiles that match SYS1.DUMP00. The best-fitting profile is shown in the top line. In addition, less specific profiles are shown that might match the resource, if the top profile was deleted.
In addition to the mask and matching selection options, other selection criteria are available. These criteria can be useful when you are searching for specific types of data set profiles. For example:

a. Press PF3 to return to the data set Selection panel.

b. Type `/` in the Profile fields in the Additional selection criteria area. This action opens another panel so that you can specify more selection criteria.

Listing profiles in warning mode

**About this task**

Warning mode means that all accesses are permitted, but a warning message is issued if the access typically results in a violation. Warning mode is usually a temporary measure because it permits any action on data sets covered by the profile. To list all the profiles that are in warning mode, complete the following steps:

**Procedure**

1. Ensure that there is a `/` next to the Warning mode field and remove the selection (`) next to the No warning field. Press Enter.

   The display lists all profiles that are in warning mode. Your search can be more specific, such as `HLQ=PAYROLL` and Warn mode.

2. Press PF3 to return to the Data set Selection panel.

3. Try entering `PROD.*` or something meaningful for your installation in the Dataset profile field and `= 3 (READ)` in the UACC or ID(*) selection field. This field is in the same panel where earlier you selected the warning mode.

4. Reapply the `/` next to the No warning field in the inclusion criteria section and press Enter.

   This action produces a list of production data sets that any user can read.

5. Press PF11.

   This action shows more fields such as the **ERASE** (E) field. If a profile has the RACF ERASE ON SCRATCH (EOS) attribute, then any data set that is protected by the profile is physically erased to ensure data confidentiality when it is deleted.

6. Use the `S` line command or move the cursor to the beginning of any displayed data line to obtain the details for that particular profile.

   **Note:** Many lines in the displays can be expanded. Enter an `S` in the first field of the line or position the cursor in the first field and press Enter.

**Displaying discrete profiles**

**Procedure**

1. Return to the Data set Selection panel.

2. Erase the Dataset profile field.
3. Type a / before Profile fields in the Additional selection criteria section. Press Enter.
4. Make sure that nothing is filled in for the UACC or ID(*) field.
5. Check that there is a / in the Discrete selection field in the Data set Selection panel.
6. Remove the / from the Generic selection field. Leave all other selection criteria as they are and press Enter.
   This action produces a list of all existing discrete data set profiles.

   **Tip:** Remember that zSecure Audit for RACF uses the AND function when you specify multiple properties.

### Displaying the access control list (ACL)

#### About this task

The next steps open a list of data set profiles. Select a specific profile to obtain detailed information, like the access control list (ACL), information related to each entry in the ACL, and some of its characteristics. Select a data set profile that you know has multiple, complex usage permissions in your RACF database. You can use wildcard characters to specify the selection criteria. The following examples select data set profiles with a name pattern that matches SYS1.** as an example, but use one that is appropriate for your installation. In the data set Selection panel, complete the following steps:

#### Procedure

1. Type the profile name in the Dataset profile field.
2. Type a / next to the Enable full ACL field in the Output/run options section.
3. Press Enter to open the list of all matching profiles.
4. Select the most complex data set profile from the list.
5. Type an S line command for that line. Press Enter.

<table>
<thead>
<tr>
<th>Identification</th>
<th>SYS1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>SYS1.PROCLIB</td>
</tr>
<tr>
<td>Type</td>
<td>GENERIC</td>
</tr>
<tr>
<td>Volume serial list</td>
<td></td>
</tr>
<tr>
<td>Effective first qualifier</td>
<td>SYS1</td>
</tr>
<tr>
<td>Owner</td>
<td>SYSPROG</td>
</tr>
<tr>
<td>Installation data</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 16. Normal ACL**

In **Figure 16** you can see that in this case the ACL contains only group entries.
Access control list formats

In RACF, you can easily have multiple, inconsistent access permissions for a resource. For example, you can have read permission through a group to data set XXX. You can also belong to another group that has update permission to XXX. RACF grants the user the highest access level available in such multiple permissions. In our example, the user would have update authority.

Additionally, a specific user permit takes precedence. RACF resolves multiple access permissions to determine the operative permission. zSecure Admin and Audit can display resolved permissions, or it can display exploded permissions, showing all permissions that exist. The resolved permission is the only one that counts for granting access to a resource. An exploded list is vital in trying to determine why a user has a certain level of access to a resource. By default, zSecure Admin and Audit displays the access control list exactly as RACF would display it, but ordered by groupid or userid and including the userid, programmer name, and installation data.

To show a list of all users that are connected to these permitted groups and any user who has permission by other reasons, type ACL EXPLODE or ACL X in the command line. This command opens an exploded list (which might be more than one line per user) showing those users with access to this profile. The detailed display indicates which access control list entries provide what level of access for the users.

All users with access to the data set are displayed, along with their connect group; see [Figure 17]. Even access through system-wide and group-OPERATIONS is indicated.

<table>
<thead>
<tr>
<th>User</th>
<th>Access</th>
<th>ACL id</th>
<th>When</th>
<th>RI Name</th>
<th>DfltGrp</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMBERT</td>
<td>ALTER</td>
<td>SYSPROG</td>
<td></td>
<td>BERT JOHNSON</td>
<td>SYSPROG</td>
</tr>
<tr>
<td>CMBERT</td>
<td>READ</td>
<td>SYSPROG</td>
<td></td>
<td>BERT JOHNSON</td>
<td>SYSPROG</td>
</tr>
<tr>
<td>CRMBFT1</td>
<td>ALTER-O- oper -</td>
<td>FRANK TRATORRIA SPEC. SYSPROG</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CRMBFT1</td>
<td>ALTER</td>
<td>SYSPROG</td>
<td></td>
<td>FRANK TRATORRIA SPEC. SYSPROG</td>
<td></td>
</tr>
<tr>
<td>DEPT2</td>
<td>READ</td>
<td>SYSPROG</td>
<td></td>
<td>USR =QA OW=DEPT USR =QA CN</td>
<td></td>
</tr>
<tr>
<td>DFHSM</td>
<td>READ</td>
<td>SYSPROG</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Figure 17. Exploded ACL]

In [Figure 17] the line:

- CRMBFT1 ALTER-O - oper - FRANK TRATORRIA SPEC. SYSPROG

shows an example where access is granted because the user has OPERATIONS authority. The following line shows that the user DEPT2 is connected to group SYS1 and has READ access on the data set profile.

DEPT2 READ SYS1 USR =QA OW=DEPT USR =QA CN

A user can have multiple access rights to the same data set profile through different paths. A line is shown for each of a user’s access rights and group
connections. For example, as Figure 17 on page 23 shows, user C#MBERT is displayed in two different lines because this user is connected to group SYS1 and has READ access and this user is also connected to group SYSPROG and has ALTER access.

**Tip:** Avoid the EXPLODE option. The SORT option is best for general use.

To show only the highest level that a user has, use these ACL commands:

- **Type ACL RESOLVE (R) in the command line.**
  
  A list is displayed showing only one entry for each user, indicating exactly what access each user has. Be aware, however, that access with the system-wide and group-OPERATIONS attribute is not included in the resolved overview display.

- **Type ACL EFFECTIVE (F) in the command line.**
  
  A list is displayed showing only one entry for each user, indicating exactly what access each user has. The list, however, also includes users who have access because they possess the OPERATIONS attribute.

- **Type ACL SORT ACCESS in the command line.**
  
  A list is displayed showing the access control list by descending access level and for each access level by user ID. See Figure 18.

  **Figure 18. Effective ACL**

  The **ACL EFFECTIVE** command shows you the effective access that individual users have, including access through system and group operations. If you also want to include ownership rights through owner, qualifier, or group-SPECIAL, you can toggle it on and off by using the commands **ACL SCOPE** and **ACL NOSCOPE**. If you want to see access rights and ownership rights separately but still resolved, you can specify **ACL TRUST** instead of **ACL EFFECTIVE**.

  **Tip:** To print a display, go to the command line and type **PRT**. This command prints the current display. It includes the full report width, which can be wider than the screen of the typical user, and the higher-level information that leads to this panel. The printed output is placed in your ISPF LIST data set. When you exit ISPF, remember to print this data set. If you want to print the ISPF LIST data set without leaving ISPF, enter **LIST** in the command line and select your printing options in the displayed panel.
Access list display settings

This brief discussion of resolve and explode is an important feature for you to remember. You can change the layout of the access control list in these ways:

- Use Option 5 from the Setup panel to access the Setup View panel.
- Type SET in the Command area of an access control list display.
- Type an ACL RESOLVE, ACL EXPLODE, or ACL EFFECTIVE command in the Command area of an access control list display.

The first two methods remember the new mode for future use. The last method changes only the current display.

For more information about changing the access list display settings, see:

- “Changing the access list display settings from the Setup View panel”
- “Changing the access list display settings from the Setup panel”

Changing the access list display settings from the Setup View panel

Procedure

1. Type **SETUP VIEW** in the command line to open the Setup View panel that is shown in [Figure 19](#).

```
Menu Options Info Commands Setup
------------------------------------------------------------
Command ===> ___________________________________________
---------- zSecure Admin+Audit for RACF - Setup - View
Access list format ... 2 1. No 3. Explode 5. Effective
  2. Sort 4. Resolve
ACL/Connect sort ... 2 1. Id 2. User 3. Access
Show OS specific options / z/OS _ z/VM
  / Add user/group info to view
  (Selecting this will use some additional storage - normally on )
  / Add summary to RA displays for multiple RACF sources (normally on)
  _ Add connect date and owner to RA.U connect group section
Select view
  3 1. View only profiles you are allowed to change (administrator view)
  2. View only profiles you are allowed to change or list
  3. View all profiles (normal view)
```

2. In the **Access list format** field, specify option 5.
3. Press PF3 to ACCEPT the new value. The value is in effect the next time you do a query. From now on, you see only one line for each user. This line represents the effective access level for each user.

The resolve or explode display level that you set is in effect until you change it. The Setup View panel is one of the Setup panels. You can also access it through the Setup menus.

Changing the access list display settings from the Setup panel

Procedure

1. Return to the Main menu by using PF3.
2. Select option **SE** (Setup).
3. Select option 5 (View).

Tip: Instead of typing these commands, you can also type *SE.5 in the command line to go immediately to the Setup View panel.

4. To change the Access control list format back to SORT, type 2 in the Access list format field. The Sort format is the most appropriate format for general use.

5. Press PF3 to exit the panel.

Checking access to resources with the Access command

About this task

Note: This command is applicable only for the zSecure Admin product.

You can use the Access function RA.1 to see the data sets or resources (and RACF profile) that a specific user or group has access to. By typing a user ID, a resource class, and a data set name, general resource name, or RACF profile name, the Access function answers the question of which profile covers the resource and what the resulting access is for the user.

To use the Access function, complete the following steps:

Procedure

1. In the Id field, type the user ID or group ID.
2. Specify the resource class (data set or a general resource class name) and the data set name, resource name, or profile name in the Profile field. Press Enter.
3. Select '2. EXECUTE CKGRACF command' for command execution. Press Enter. The Access check detail panel (Figure 21) shows the access level that RACF grants to this ID and where the access is coming from.

Figure 20. Access check entry panel

Figure 21. Access check detail panel
Administration of access rights

There are several ways to administer the access control list of a data set profile:

- Issue the **PE** (permit) line command in the data set profile Overview panel.
- Use a **C** (copy), **D** (delete), **I** (insert), **R** (repeat), or **S** (modify) line command in the data set profile detail panel.
- To change a value, type over the current value in the access control list.

When you change the values, **Permit** and **Permit Delete** commands are generated to add the new value and remove the value that was overwritten.

If you do not want to run the **Permit Delete** command, remove it from the command confirmation panel before you press Enter. Press Enter again in the next panel (zSecure Admin – Confirm command) to process your **Permit** command. Do not run the RACF commands now.

Creating digital certificates templates

About this task

Use menu option **SE.9** to create digital certificate templates. Use the defined templates to generate new certificates (options RA.5.2 and RA.5.3), or to select the criteria for the display of certificates (option RA.5.1). On the definition panels, use the **F** selection fields to fix the value for a field. When you fix the value, that value cannot be changed when the template is used to generate a certificate.

Procedure

1. On the main menu, type **SE** (Setup) in the Option line and press **Enter**. The Setup menu is displayed.

   ![Setup menu](image)

   *Figure 22. Setup menu*

2. On the Setup menu, type 9 in the Option line and press **Enter**. If no templates are defined when you select this option, the Setup certificates template definition panel is displayed.
For descriptions of the fields on this panel and all subsequent panels, use the field-sensitive help function (PF1).

3. Press Enter. The following panel is displayed:

```
Menu Options Info Commands Setup
-----------------------------------------------
zSecure Suite - Setup - Certificates
Command ===> _________________________________________________________________
Name for template .... ________
Description ....... _____________________________________________
F Enter the following defaults for the new certificate:
  Certificate label prefix
  Size of new private key (Default 1024 for RSA/DSA; 192 for ECC)
  Start validity date . . . (Default is today)
  Start validity time .... (Default is 00:00:00)
  End validity date .... (yyyy-mm-dd, default 1YEAR)
  End validity time .... (Default is 23:59:59)
F Enter the following defaults for the Signing Authority:
  Digital certificate label
Optional actions . . . . 1. Connect to key ring
                         2. Export certificate
                         3. Generate certificate request
Press ENTER to continue or END to exit
```

Figure 23. Setup certificates template definition panel

For descriptions of the fields on this panel and all subsequent panels, use the field-sensitive help function (PF1).

4. Press Enter to display the next panel:

```
Menu Options Info Commands Setup
-----------------------------------------------
zSecure Suite - Setup - Certificates
Command ===> _________________________________________________________________
Name for template .... MQ
Description ....... MQ certificate template
F Enter the following defaults for the new certificate:
  Key usage ........_ Handshake _ Docsign _ Keyagree
  Select the key type to be generated:
    1. RSA(default)
    2. RSA Modulus-Exponent in PKDS
    3. DSA
    4. NIST ECC
    5. Brainpool ECC
      1. Store in PKDS with an optional PKDS label or + (types 1,2,4, and 5)
      2. Store in TKDS using existing TKDS token (types 1,4, and 5):
Press ENTER to continue or END to return to previous panel
```

Figure 24. Setup certificates template definition panel

4. Press Enter to display the next panel:
5. Press Enter. The following panel is displayed:

```
Menu Options Info Commands Setup
----------------------------------------
| zSecure Suite - Setup - Certificates |
| Command ===> _________________________________________________________________ |
| Name for template . . . . MQ |
| Description . . . . . . . . MQ certificate template |

F Enter the Subject’s X.509 Distinguished Name:
Common Name: (ex: 'John Q. Public')
Title: (ex: 'Systems Programmer')
Organizational Unit: (ex: 'S390', 'MVS')
Organization: (ex: 'IBM')
Locality: (ex: 'Poughkeepsie')
State/Province: (ex: 'New York')
Country: (ex: 'US')
```

Press ENTER to continue or END to return to previous panel

Figure 25. Setup certificates template definition panel

6. If you select option **Connect to key ring** on Figure 23 on page 28, the following panel is displayed:

```
Menu Options Info Commands Setup
----------------------------------------
| zSecure Suite - Setup - Certificates |
| Command ===> _________________________________________________________________ |
| Name for template . . . MQ |
| Description . . . MQ certificate template |

F Enter the subjectAltName extension:
Enter the IPv4 or IPv6 address
Enter the internet domain name
Enter the fully qualified email address
Enter the universal resource identifier
```

Press ENTER to continue or END to return to previous panel

Figure 26. Setup certificates template definition panel
7. After the template is defined, the following panel is displayed:

You can use the following action commands:

- **B** Allows browsing through the existing definitions.
- **C** Create a new template based on an existing template.
- **D** Shows a confirmation panel before deleting the template.
- **E** and **I** Shows the certificate definition panel.

---

**Working with certificates, key rings, filters, and tokens**

**About this task**

Digital certificates are used for authentication, verification, encryption, etc. A certificate typically contains a description of the subject, a public and/or private key, and a signature of “trusted party.”

The RACDCERT command is complex. For example, it has 25 primary options and some functions require multiple commands. Zsecure uses the standard zSecure interface: select-display-action and action via line commands and overtyping. It also provides options to directly create new objects.
Most parameters are verified before RACDCERT is run and the last specified parameters are retained for easy correction. You can use templates to specify default values; zSecure also includes two default templates:

**None**
Use empty fields.

**Previous**
Use options from last time.

Use the RA.5 (RACDCERT) menu to work with digital certificates, key rings, filters, and tokens.

### Procedure

Press PF3 until you are on the Main menu. Select RA.5 to display the RACDCERT menu.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Options</th>
<th>Info</th>
<th>Commands</th>
<th>Setup</th>
<th>Startpanel</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>zSecure Suite - RACF - RACDCERT</td>
</tr>
<tr>
<td>Option ====&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Certificates</td>
<td>Work with digital certificates</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Generate</td>
<td>Generate new certificate and a public/private key pair</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Sign</td>
<td>Generate new certificate using an existing public key</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Add</td>
<td>Add or update existing digital certificate</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Check</td>
<td>Check whether digital certificate has been added to RACF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Key rings</td>
<td>Work with key rings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Name filtering</td>
<td>Work with certificate name filters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Tokens</td>
<td>Work with tokens</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Criteria</td>
<td>Work with certificate mapping criteria</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Figure 29. RACDCERT menu*

The options on this panel are briefly explained here. For more details on the RACDCERT function, see the section on RA.5 in the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*. When you select an option, the subsequent panel is displayed. For a description of the fields on these panels, use the field-sensitive help function.

On the subsequent details displays, you can select any row to see the full detail view. You can select details by putting the cursor on the first character of the row selection field and pressing Enter, or by explicitly typing S there and pressing Enter.

**RA.5.1 Certificates - Work with digital certificates**

Use option RA.5.1 to select and perform actions on digital certificates. The following panel is displayed:
Use the Match on template option to match certificates to a template defined with SETUP (DEFAULT) CERTIFICATES. A panel is displayed in which you select a template. The selection fields on the certificate panels are pre-filled with the values of the selected template. Figure 31 shows a sample digital certificate display.

You can use several line commands:

**BI - Bind certificate to token**
Bind a RACF Certificate to an existing token.

**CO - Connect certificate to key ring**
Connect a certificate to a key ring.

**EX - Export certificate**
Write a digital certificate to a data set.

**GR - Generate certificate request**
Create a PKCS #10 Base64-encoded certificate request that is based on the specified certificate or to write the request to a data set.

**LC - RACDCERT LISTCHAIN for certificate**
issue a RACDCERT LISTCHAIN command. The command results in a listing of certificate information about a certificate that is owned by a user ID, SITE or CERTAUTH, and its issuers' certificates owned by CERTAUTH in a chain of certificates.
RK - Rekey certificate
Replicate (rekey) a digital certificate with a new public/private key pair. In general, after you rekey a certificate, issue the RO action command to supersede the old certificate with the new rekeyed certificate and retire the old private key.

RO - Rollover certificate
Supersede one certificate (source certificate) with another certificate (target certificate). In general, issue the RO action command after you issue the RK action command to supersede an old, expiring certificate with a new rekeyed certificate or to retire the private key of the expiring certificate.

UB - Unbind certificate from token
Unbind a RACF certificate from an existing token.

RA.5.2 Generate - Generate new certificate and a public/private key pair
Use this menu option to generate a new certificate and a public/private key pair. First, the template selection panel is displayed. This panel shows the templates that are defined with SETUP CERTIFICATES and these defaults:

None
Clears all fields on the GENCERT panel

Previous
Uses the values entered the last time

RA.5.3 Sign - Generate new certificate using an existing public key
Use this menu option to generate a new certificate that uses an existing public key.

RA.5.4 Add - Add or update existing digital certificate
Use this menu option to define a digital certificate by using a certificate or certificate package that is contained in the specified data set.

RA.5.5 Check - Check whether digital certificate has been added to RACF
Use this option to evaluate whether the digital certificates in the specified data set were added to the RACF database and associated with a user ID. A data set name that is enclosed in quotes must be entered. If the certificate in question is in PKCS12 format, a password is also required.

RA.5.6 Key rings - Work with key rings
Use this menu option to work with key rings. If you leave this panel empty and press Enter, all key ring records are displayed.

You can use the following line commands:

BI - Bind certificate to token
Bind a RACF Certificate to an existing token.
D - Delete token
Generate a RACDCERT DELTOKEN command.

L - List token
Generate a RACDCERT LISTTOKEN command.

UB - Unbind certificate from token
Unbind a RACF certificate from an existing token.

RA.5.8 Name filtering - Work with certificate name filters
Use this menu option to work with certificate name filter rings. Figure 33 shows a sample name filters display:

```
Command ====> _________________________________________________ Scroll====> CSR
All name mappings 12 Mar 2013 06:00
Certificate filter name (issuer and subject name separated by \c)
  \cOU=CRM.O=Consul Risk Management
  \cOU=Sysprog,OU=CRM,O=Consul Risk Management
  \OU=CICS Individual Subscribers,O=Verisign,Inc,L=Internet\c
  \OU=VeriSign Class 1 Individual Subscribers,O=Verisign,Inc,L=Internet\cOU=Sysp
******************************************************************************** Bottom of Data ****************************
```

Figure 33. Name filters overview

RA.5.9 Criteria - Work with certificate mapping criteria
Use this menu option to work with certificate mapping criteria. Figure 34 shows a sample criteria display:

```
Command ====> _________________________________________________ Scroll====> CSR
All criteria 12 Mar 2013 06:00
Criteria MapToID Owner CreateDat Lv Cl
  APPLID=CICSA CRMQA205 CRMBMR1 14Apr2000 0 DI
  APPLID=CICSB CRMQA206 CRMBMR1 14Apr2000 0 DI
******************************************************************************** Bottom of Data ****************************
```

Figure 34. Criteria overview

Comparing users

About this task

Often users ask a question such as, “Why does this function not work for me, while it does for my neighbor? I thought we were supposed to have the same access to that product?” You can use zSecure Admin and zSecure Audit for RACF for quick comparison of the access and connect status for up to four users.

To compare the access and connect status of users, complete the following steps:

**Procedure**

1. Press PF3 until you are on the Main menu.
2. From the Main menu, select option REPORTS (RA.3) from the RA panel. Select option G Compare users from the resulting panel to open the Compare users panel that is shown in Figure 35 on page 35.
On this panel, you can specify up to four users and the exact comparisons that you want to do. Up to two reports are generated: one for permits, and one for group connects.

**Example**

The Permit report is presented in three layers:
- The classes for which permits are present with the highest access of each user to any profile in that class.
- The profiles in the selected class with the highest access.
- A list with all permits for the selected users on a specific profile.

This detailed display also shows the information from the higher layers for this one specific entry, as shown in Figure 36.

**Example**

The connect report shows a matrix of all groups to which at least one of the users is connected, as shown in Figure 37.
Chapter 3. Administration of users and profiles

Note: This section is applicable only for the zSecure Admin product.

Using zSecure Admin, you can change RACF data in the following ways:
- You can change a value by typing over the existing value in a field on a profile display.
- You can use line commands in a profile display, like C (Copy), D (Delete), R (Re-create), L (list), and SE (Segments).
- You can use the Mass Update panels.
- You can submit foreground or background RACF commands that are automatically generated by various Report and Verify functions.
- You can use the distributed functions, described in Chapter 4, “Distributed and scoped administration functions,” on page 49.

Typing over a value, line commands, and Mass Update are controlled by the Confirmation setting in the Setup - Confirm panel. See “Generating and confirming RACF commands.” The Confirm panel enables or disables the Overtype function and determines what verification is required before you run a RACF command that changes the database. You can set the Confirmation control as you want. However, until you are familiar with routine product usage, use the setting ALL or PASSWORDS.

Generating and confirming RACF commands

Procedure

To generate and confirm RACF commands, complete the following steps:
1. Select option SE (Setup).
2. Select option 4 (Confirm) to open the Confirm panel that shows the current settings, as shown in Figure 38 on page 38.
3. Set the **Action on command** field to **2** (Execute).
4. Set the **Confirmation** field to **4** (All).
5. Set the **Command Routing** field to **3** (Local only).
6. Set **Overtype fields in panels** to `/`. This option is used in the following examples. Leave all other settings as they are, especially in the **Commands to generate** section.

   **Tip:** You can also switch modifiable fields on and off by entering the `MODIFY` command (or just `M`) in the command line of any profile display.

7. Press PF3 to accept the changed parameters.
8. Press PF3 again to return to the Main menu.

   **Tip:** You can always reach the Confirm panel by typing `SETUP CONFIRM` or `=SE.4` in the command line of any panel.

### What to do next

If you want to manage the RACF database from zSecure Admin by using your user ID, you must have the correct authority for the RACF database. If you are selective about attempted changes, the required authority is usually RACF SPECIAL, although group-SPECIAL might serve. An alternative is to use the `CKGRACF` program, which has its own security scheme, instead of SPECIAL authority. See "Group administration through CKGRACF" on page 50.

### Performing a mass update

#### Procedure

1. Select option **RA** (RACF Administration).
2. Select option **4** (MASS UPDATE) to open the Mass update panel that is shown in Figure 39 on page 39.
What to do next

Using Options 0 to 5 from the Mass update panel, you can manage profiles at the entity level, like user and group. For example, when you delete a user, you delete not only the user profile, but also all profiles that are related to the original user ID. Additionally, the PERMITS, CONNECTS, and the ALIAS in the master catalog are removed. All information is managed at one time.

The Mass Update panels provide many functions that are difficult to do with regular RACF commands. Some especially important points are highlighted.

Copying a user

About this task

You can clone an existing user by using the Copy user option (Option 0). In addition to copying the user profile, this command also copies the permits and connects of the model user. zSecure Admin also provides the option to create a user ALIAS in the master catalog.

Procedure

To copy a user, complete the following steps:

1. Select option 0 (Copy user) from the Mass Update panel to open the User Multiple copy panel, which is shown in Figure 40 on page 40.

Figure 39. Mass update panels
You can clone up to 10 users at a time, but for the evaluation, complete only the first line.

2. If you want to specify password phrases, type / in the Specify password phrases selection field.
   After you press Enter, a follow-up panel is displayed so that you can enter the password phrases for the user IDs. If you specify password phrases, you cannot use the protected option.

3. Specify the model user: Type your user ID, the new user ID, the name, and a password. Press Enter.
   Tip: You can use * in the password column to make the new user protected.

4. Press Enter in the next panel.
   This panel provides the option to do the following functions for the new user:
   • Omit or add more group connections.
   • Copy user data.
   • Revoke the new user or users.
   • Create one or more catalog aliases.
   • Copy one or more data sets and general resource profiles.
   • Copy one or more members of RACF variables (RACFVARS) for the new user.

   Any command necessary to create the user from the model profile is generated. After a few moments, a PDF edit panel is displayed with a complete set of RACF commands. You can scroll by using PF8 and PF7 to go forward and backward and make changes if applicable.

5. Press PF3 to quit the editor.
6. Press PF3 to skip the Result panel.
   The Result panel is described in Chapter 6, “Creating and viewing a report,” on page 69.

7. Press PF3 until you are back on the Mass Update panel.
Results

If the commands are run, the new user is defined exactly as the model user. You can also keep the generated commands in a data set for delayed execution.

Delete a user with all references

You can completely remove a user with option RA.4.4 (Delete user), which is a tedious operation if done with regular RACF commands. Completely removing a user removes the user ID from all access control lists and owner and notify fields, in addition to removing the profile. If you allocated a CKFREEZE file, this operation also deletes the catalog alias and existing data sets for the user if you select the required options. See Figure 55 on page 57.

Re-create a profile

You can re-create profiles with options RA.4.6 through RA.4.9 based on data in the unloaded RACF data set or a backup copy of the RACF database itself. This action can be used to repair profiles that are damaged by errors or deleted by mistake.

Merge and compare profiles

There are several other interesting features for merging RACF databases or comparing RACF databases. Merging is done by making an unloaded copy of one RACF database and by using it to change and add profiles in another RACF database. For confirming or editing, all RACF commands to be used for merging the RACF profiles are listed. This command list is a comparison of the relevant profiles in the RACF and unloaded data set. A complete merge is more complex than described here and is fully documented in the IBM Security zSecure Admin and Audit for RACF: User Reference Manual.

Redundant profile management

It is a good practice to regularly take a close look at the data set profiles that are defined in your RACF database. To determine which data set profiles are, or might be, obsolete, you can use the RA.3.3 function. This function opens the Reports - REDUNDANT panel that is shown in Figure 41.
In the panel that is shown in Figure 41 on page 41 you can specify which data set profiles or High Level Qualifier (HLQ) you want to include in the report. If these fields are left blank, all data set profiles are automatically processed. You can also specify whether you want to include the names of all data sets that are covered by the data set profiles in the report.

The Report Redundant function compares data set profile security definitions such as UACC, access control list, audit settings, and erase on scratch setting, to those of the next less specific generic data set profile.

When the security settings are not different, the profile is reported as -redundant-. This value indicates that when this more specific data set profile is deleted, the protection of the data sets is automatically taken over by the less specific generic data set profile (indicated as -candidate-) without causing any changes in the security definitions for the corresponding data sets.

The output of the report on redundancy is an overview of all data set profiles with an indicator in the column that is headed by First reason. The first reason column can contain any of the following values:

- **redundant**-
  With the current security definitions, this profile is not required and can be removed. Protection of the data sets covered by the redundant profile is automatically taken over by a less specific data set profile (marked with -candidate-) that is displayed in the same report somewhere above the profile that is reported as a -redundant- profile.

<table>
<thead>
<tr>
<th>Complex</th>
<th>Timestamp</th>
<th>Profiles Non-redundant</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEMO</td>
<td>8 Apr 2005</td>
<td>445</td>
</tr>
<tr>
<td>Qual</td>
<td>445</td>
<td>364</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Volume</th>
<th>Profile name</th>
<th>First reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>GENERIC</td>
<td>SYSA.D.CCW*.**</td>
<td>- candidate -</td>
<td></td>
</tr>
<tr>
<td>GENERIC</td>
<td>SYSA.D.CCW*.**</td>
<td>Extra group</td>
<td></td>
</tr>
<tr>
<td>GENERIC</td>
<td>SYSA.D.CCW*.**</td>
<td>User privileged</td>
<td></td>
</tr>
<tr>
<td>GENERIC</td>
<td>SYSA.D.CCW300.+.BASELIST</td>
<td>- redundant -</td>
<td></td>
</tr>
<tr>
<td>GENERIC</td>
<td>SYSA.D.CCW300.**</td>
<td>- candidate -</td>
<td></td>
</tr>
<tr>
<td>GENERIC</td>
<td>SYSA.D.CCW300.**</td>
<td>Access</td>
<td></td>
</tr>
<tr>
<td>GENERIC</td>
<td>SYSA.D.CCW301.**</td>
<td>Access</td>
<td></td>
</tr>
<tr>
<td>GENERIC</td>
<td>SYSA.D.CCW302.**</td>
<td>Extra group</td>
<td></td>
</tr>
<tr>
<td>GENERIC</td>
<td>SYSA.D.CCW303.**</td>
<td>Access</td>
<td></td>
</tr>
<tr>
<td>GENERIC</td>
<td>SYSA.D.CCW305.**</td>
<td>Access</td>
<td></td>
</tr>
<tr>
<td>GENERIC</td>
<td>SYSA.D.CCW310.**</td>
<td>Access</td>
<td></td>
</tr>
<tr>
<td>GENERIC</td>
<td>SYSA.D.CCW311.**</td>
<td>Access</td>
<td></td>
</tr>
<tr>
<td>GENERIC</td>
<td>SYSA.D.CCW312.**</td>
<td>Extra group</td>
<td></td>
</tr>
</tbody>
</table>

Figure 42. Report redundant details panel

In Figure 42 the following line shows an example of a profile that can take over protection of data sets when the profile marked as -redundant- is deleted.

- GENERIC SYSA.D.CCW*.** - candidate -

The following line shows an example of a profile that can be deleted because the security settings are similar to those of the candidate profile that automatically takes over protection.

- GENERIC SYSA.D.CCW300.+.BASELIST - redundant -

The output of the report on redundancy is an overview of all data set profiles with an indicator in the column that is headed by First reason. The first reason column can contain any of the following values:

- **redundant**-
-candidate-
This profile takes over the protection of data sets that are currently protected by a more specific generic data set profile, when the latter is deleted.

reason
This field provides a textual description to indicate why this profile differs significantly from the less specific generic data set profile and therefore is not considered redundant. Sample reason values are: Extra group, User privileged, and Access. When multiple differences exist, only the first reason is reported.

The report on redundancy can help you determine which data set profiles are now obsolete in the current RACF database.

Optionally, you can generate RACF commands to delete the profiles that are reported as -redundant-. Be aware, however, that you might not want to delete all profiles marked -redundant-. It is possible that a mistake was made at the time this data set profile was defined; that is, you or another RACF administrator forgot to activate erase on scratch or change the audit setting as intended.

Tip: The redundancy analysis can be useful to indicate any mistakes that you made during data set profile definition.

Displaying data structures

About this task

Another useful report when managing your RACF database is the Group tree report. In native RACF, the only way to display the RACF database structure is by processing the Group tree report by using the DSMON utility. For each requested group, this report lists all of its subgroups, all of the subgroups of subgroups, and so on. In addition, the report lists the owner of each group listed in the report, if the owner is not the superior group. Only users that have the AUDITOR attribute can use the DSMON utility. However, the AUDITOR attribute is not required to process the Group tree report.

In zSecure Admin, there is a standard function for processing a Group tree report. The group tree visualizes the group tree structure, similarly to how a browser displays the contents of your hard disk or network drive.

Procedure

To process the Group tree report, complete the following steps:
1. Select option RA (RACF Administration).
2. Select option 3.8 (Group tree) to open the Reports Group tree panel shown in Figure 43 on page 44.
You display only a particular branch of the RACF group tree by entering a group name (or filter) in the Start at field. This option is available only when running with an unloaded data source. If all fields are left blank, the entire group tree for your RACF database is displayed.

a. Optional: You can indicate that you want to include the Installation data in the group tree report by entering a / in front of Installation data. The Installation data is generally used to store the group description.

b. To include detailed information about subgroups and connected users in a detail level panel, type a / in front of the Users/Subgroups field.

3. Press Enter to open the Group tree report panel, which shows all groups in your current RACF database. See Figure 44. In the Group tree report panel shown in Figure 44, the X in the X column indicates a scope break for group special users. This break is indicated because owner is not equal to the superior group.
4. If you requested Installation data, press PF11 to review the information.
5. Press PF8 a few times to look at more parts of the group tree structure.
6. If detailed information was included in the report and you want to view it, enter the S line command in front of a group. This action opens the Group tree report detail panel shown in Figure 45.

Running SETROPTS reports and viewing class settings

About this task

You can administer the current system-wide RACF options or the Class Descriptor Table (CDT) in zSecure Admin with the RA.S and AU.S functions. This section provides information about the RA.S function. Details on the AU.S version of the SETROPTS and RACFCLAS reports are included in Chapter 8, “Auditing system integrity and security,” on page 79. See Figure 71 on page 80 and Figure 73 on page 81 for more information.

Procedure

To run SETROPTS reports and view class settings, complete the following steps:
1. Select option RA (RACF Administration).
2. Select option S (Settings) to open the SETROPTS and class settings panel that is shown in Figure 46.
   As shown in Figure 46, the SETROPTS and RACFCLAS reports are automatically generated.
3. In the SETROPTS selection field, type the S command to open the SETROPTS report that is shown in Figure 47 on page 46.
You can use this report to investigate the RACF system-wide settings. You can use PF7 and PF8 for scrolling the report up and down.

**Note:** This report is available only in zSecure Admin.

Additionally, you can administer most of the **SETROPTS** options from this panel by typing over the current value with the value for the **SETROPTS** setting you want to change. This action automatically generates the appropriate **SETROPTS** command to apply the change.

4. Press PF3 to return to the SETROPTS and Class Settings Panel.

5. To view the class settings report, complete the following steps:
   a. Enter the S command in the RACFCLAS report selection field to open the RACF class settings panel that is shown in [Figure 48](#).

b. To view the full detail settings of the involved resource class, enter the S line command in the Class selection field.

---

**Figure 47. RACF settings SETROPTS report**

**Figure 48. RACF settings RACFCLAS report**
c. Optional: You can enter the R line command to refresh the involved resource class or type over the existing value in the **Active** column. You can type: **Y**, **A**, or **Active** to activate a resource class that is inactive. Type **N** or blanks to deactivate a resource class that is active.

**Note:** This function is available only in zSecure Admin.
Chapter 4. Distributed and scoped administration functions

This section describes the distributed administration functions, which are only a selected subset of the administrative functions available. This section also provides information about the group auditor view.

Group Administration with RACF scope

Note: This function is available only in Security zSecure Admin.

To limit function to a group administrator’s natural RACF scope, the program must be run in restricted mode. You can achieve this requirement by using any of the following methods:

Method 1
Create an XFACILIT profile CKR.READALL with UACC(NONE) and give only central administrators READ permits.

This method is the easiest and most suited for an evaluation.

Method 2
Access the RACF database either through Program Access to Data Sets (PADS), or through the zSecure server (possibly in self-connect mode).

These methods are safest, but require quite some setup. For a description of setup of both methods, see the IBM Security zSecure Admin and Audit for RACF: Installation and Deployment Guide.

Method 3
Use a SIMULATE RESTRICT command in SETUP PREAMBLE.

This method works only to test your own scope.

Method 4
Issue the command SETUP VIEW and select 1 or 2 under Select view:
1. View only profiles you are authorized to change (administrator view).
2. View only profiles you are authorized to change or list.

This method provides an additional scope restriction. However, this scope restriction is not called restricted mode, but administrator view.

Like method 3, this method works only to test your own scope. It prevents you from displaying profiles that you have only READ access to. It also ignores system-wide privileges, so it is even more restrictive than the natural RACF scope.

The Quick Administration panel

Note: This function is available only in zSecure Admin.

You can access the Quick Admin function by using one of the following two methods:
• "Accessing the Quick Administration panel in a stand-alone way” on page 50
• "Accessing the Quick Administration panel with RA.Q” on page 50
Accessing the Quick Administration panel in a stand-alone way

Procedure

1. Select option X (Exit) from the Main menu.
2. Type `CKR,STARTTRX(MENU(RA.Q))` in the command line under ISPF Option 6 to start the Quick Admin application. See Figure 49.

Accessing the Quick Administration panel with RA.Q

Procedure

1. On the Main menu, select RA.Q to open the Quick Admin panel that is shown in Figure 49.
2. Use the Quick Admin panel to access the most frequently used functions that are required by a central or decentralized user administrators, hiding the details.

   The Quick Admin panel relies on the system or group-SPECIAL attribute of the administrator. The options in the panel can be hidden by `CKR.OPTION.RA.Q` profiles, but otherwise the menu works as shown.

```
Menu Options Info Commands Setup StartPanel
-----------------------------------------------
Command ===> _________________________________________________________________

1 Password    Set new password for user
2 Resume      Make sure user can work
3 Display     List user definition
4 Modify      Change user definition
5 Connect     Add group to a user
6 Add user    Create new userid from scratch
7 Add user copy Create new userid like existing model
8 Phrase      Set new password phrase for user

Figure 49. Quick Admin
```

Group administration through CKGRACF

Note: This function is available only in zSecure Admin.

zSecure Admin provides the CKGRACF program as the base for distributed RACF control; that is, Helpdesk and Group Admin. The CKGRACF program is designed to provide the following functions:

- Access to commonly used Helpdesk functions such as password reset through menus.
- Access to commonly used Group Admin functions such as permits and connects through menus.
- Access to these functions *without* granting group-SPECIAL authority.
- Granular controls over user authorization to use CKGRACF functions.

CKGRACF differs from the main CKRCARLA program in that it does most of its tasks through APF-authorized interfaces, whereas the main program generates normal RACF commands whenever possible. Because APF-authorization is required, the user of the main CKRCARLA program must have sufficient administrative RACF authority to run the generated RACF commands. These commands are generated
when you type over a parameter, or use line commands to change profiles. The main zSecure Admin ISPF panels sometimes call the CKRCARLA program to make RACF changes when no standard RACF command can be generated to make the required change. Updating user data fields is the best example of this scenario.

The CKGRACF user does not require any special RACF authority such as the SPECIAL or group-SPECIAL attribute. The CKGRACF program adopts whatever authority it needs for a task by using APF interfaces. Therefore, you must control who can use the CKGRACF program by putting each CKGRACF user or group of users in the access control lists of several XFACILIT class profiles. By creating these profiles and PERMITing selected users, you can control who can use specific functions through CKGRACF.

This section addresses two categories of CKGRACF users:
- Help desk users who issue commands such as password reset and resume.
- Decentralized administrators who issue permits or connects.

The Helpdesk functions are done from a separate panel, while the group administrator’s functions are available through the typical zSecure Admin panels. You can tailor the menus by adding RACF profiles in the XFACILIT class. Each profile represents a function. Access is granted by using the usual access rules. By default all options are shown, but after you implement a tailored menu, only the granted functions are shown to the zSecure Admin user.

For your evaluation, give yourself full authority for all CKGRACF functions and then explore the functions. Setting up the XFACILIT class controls for a realistic group of distributed administrators is a one-time job, but it can be tedious. It involves the following process:
1. Defining exactly which RACF groups are associated with which administrators.
2. Defining which CKGRACF functions are to be given to which administrators.
3. Creating the necessary RDEFINE and PERMIT commands to create this environment.

Because of the amount of time that is required to define the class controls, complete your initial product evaluation without attempting to establish granular controls.

To give yourself full CKGRACF authority, you or someone with RACF SPECIAL authority must issue the following RACF command:

\[ \text{permit ckg.** class(xfacilit) acc(update) id(yourid)} \]

**Single panel Helpdesk function**

**Note:** This function is available only in zSecure Admin.

You can access the Helpdesk function by using one of the following two methods:
- “Accessing the Helpdesk function in a stand-alone way”
- “Accessing the Helpdesk function with RA.H” on page 52

**Accessing the Helpdesk function in a stand-alone way**

**Procedure**
1. Select option X (Exit) from the Main menu.
2. Type **CKR,STARTTRX(MENU(RA.H))** in the command line under ISPF Option 6 to start the Helpdesk functions. See Figure 50 on page 52.
Accessing the Helpdesk function with RA.H

Procedure

1. Select RA.H from the Main menu to open the Helpdesk panel that is shown in Figure 50.

Use this panel to do the most frequently used functions that are required by a central or decentralized helpdesk employee.

2. To see how the Helpdesk function works, complete the following steps:
   a. Type a user ID in the Userid field.
   b. Press Enter to open the Helpdesk panel that displays the selected information about the user ID as shown in Figure 50.
   c. To see the user details, select 1 in the Helpdesk panel.

Now that you checked the status of the user ID, you can make changes, such as setting a new password (option 2).

In the initial configuration, you see the CKGRACF command before it is run. To suppress this confirmation prompt for individual administrators, type setup confirm in the command line. Or, to suppress the prompt for all administrators, type setup default and select option 4. On the next panel, change the Confirmation setting.

**Helpdesk password administration functions**

**Note:** This function is available only in zSecure Admin.

Perhaps the most important CKGRACF functions for the Helpdesk are enabling, setting, revoking, and resuming passwords. The following table lists the available functions and describes how they work.

<table>
<thead>
<tr>
<th>Helpdesk function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set a new password (option 2)</td>
<td>Set a new password and enter it twice. zSecure Admin and zSecure Audit for RACF do not use RACF to update the user profile. CKGRACF authority is used instead. The user is also resumed.</td>
</tr>
</tbody>
</table>
Table 4. Helpdesk password-related functions (continued)

<table>
<thead>
<tr>
<th>Helpdesk function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable a default password (option 3)</td>
<td>The password is set to the default password for the user. A central administrator must have previously set the personal default password for the user. The Helpdesk administrator does not see the password. The user is also resumed.</td>
</tr>
<tr>
<td>Enable the previous password (option 4)</td>
<td>The previous password is enabled again. In this case, the administrator does not see the password. The previous password is automatically marked as expired; the user can use it only one more time for the next logon. The user is also resumed.</td>
</tr>
<tr>
<td>Set default (option 8)</td>
<td>Define a default password for a user ID.</td>
</tr>
</tbody>
</table>

The concept of a default password (Option 3) is new to RACF. The intention is that a simple (and low-quality) password is defined for each user. Each user selects a word or number that can be remembered indefinitely. Only the central RACF administrator sees this word when it is established by using `CKGRACF`. Other administrators do not see it when it is called. If a normal password for the user becomes unavailable for some reason, any Helpdesk administrator can enable the default password for the user. The user is expected to create a new normal password as soon as possible. This approach is better than using system-wide reset passwords, such as `SYS1`, `SECRET`, `PSWPSW`.

**Tailoring the Helpdesk**

You can tailor the Helpdesk panel for the installation in either of the following ways:

- Through `XFACILIT` profiles that start with `CKR.OPTION.RA.H`, you can selectively enable and disable options in the Helpdesk.
- Using `SETUP NLS`, you can modify the text and options in the panel.

Some functions are user management functions and should be available to a limited number of people. Examples of these functions are setting the default password or a new password, or setting authority levels. You can define `CKR.OPTION` profiles in the `XFACILIT` class to restrict the use of management functions. Thus, the installation can specify which options are shown in the Helpdesk panel for each user and selectively delegate responsibilities in the organization.

If the access control list of the corresponding profile grants a user access, the user is allowed to do the function. Otherwise, the line command is not shown in the action list and its use is prohibited. [Figure 51 on page 54] shows an example of a tailored Helpdesk panel that does not contain the options 2, 6 and 8. It does not contain these options because the user lacks the required access in the applicable `CKR.OPTION.RA.H` profiles.
Menu Options Info Commands Setup Startpanel

Option ===> ________________________________________________

1  List  List RACF profile information
3  Default Set the password to the user's default value
4  Previous Set the password to the previous value
5  Resume Resume a userid after too many password attempts
7  Enable  Allow user to logon after a Disable

Userid . . . . . . _______ (type userid and press Enter)

Reason . . . . . . _________________________________________________________

Figure 51. Tailored Helpdesk panel
Chapter 5. Setup functions for managing data

The Setup functions control which data is used by zSecure Admin and zSecure Audit for RACF. You can switch data sources while you use them. Other Setup functions set global switches and parameters. You can see some of these functions with the Resolve and Explode options.

Adding data

About this task

So far, you used only your live RACF data to display various profiles. You can create and use the following data sources:

- An unloaded RACF database.
- A CKFREEZE data set that contains extracted information from all your DASD and from various internal z/OS tables.

To begin this process, complete the following steps:

Procedure

1. Return to the Main menu. Use PF3 as necessary.
2. Select option SE (Setup) to open the Setup panel that is shown in Figure 52.
3. If you are on a 24-line display, press PF8 and PF7 to scroll up and down in the panel.

Tip: Before you continue, you can select Options 0 through 5 (one at a time) in the Setup panel to obtain a general overview of the various setup options.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Run Specify run options</td>
</tr>
<tr>
<td>1</td>
<td>Input files Select and maintain sets of input data sets</td>
</tr>
<tr>
<td>2</td>
<td>New files Allocate new data sets for UNLOAD and CKFREEZE</td>
</tr>
<tr>
<td>3</td>
<td>Preamble Carla commands run before every query</td>
</tr>
<tr>
<td>4</td>
<td>Confirm Specify command generation options</td>
</tr>
<tr>
<td>5</td>
<td>View Specify view options</td>
</tr>
<tr>
<td>6</td>
<td>Instdata Customize installation data appearance</td>
</tr>
<tr>
<td>7</td>
<td>Output Specify output options</td>
</tr>
<tr>
<td>8</td>
<td>Command files Select and maintain command library</td>
</tr>
<tr>
<td>U</td>
<td>User defined User defined input sources</td>
</tr>
<tr>
<td>C</td>
<td>Change Track Maintain Change Tracking parameters</td>
</tr>
<tr>
<td>N</td>
<td>NLS National language support</td>
</tr>
<tr>
<td>T</td>
<td>Trace Set trace flags and CARLa listing for diagnostic purposes</td>
</tr>
<tr>
<td>D</td>
<td>Default Set system defaults</td>
</tr>
<tr>
<td>R</td>
<td>Reset Reset to system defaults</td>
</tr>
<tr>
<td>I</td>
<td>Installation Specify installation defined names</td>
</tr>
</tbody>
</table>

Figure 52. Setup
Adding new files

Procedure

1. From the initial Setup panel, which is shown in Figure 52 on page 55, select Option 2 (New files) to open the New files panel that is shown in Figure 53.

2. Type a data set name in the Unload line. An input set can contain multiple coherent files. When you enter the data set names, use quotation marks if necessary. That is, if you do not want the data set names to have your user ID as the high-level qualifier. It does not matter whether these data sets exist yet. However, if they do exist, they must be cataloged.

3. Type a data set name in the CKFREEZE line. Use quotation marks if necessary.

4. Type a short, unique description of the files in the Description line. For example, UNLOAD and CKFREEZE data sets created on 8 Apr 2005.

   **Tip:** It is a good practice to use the input file Description field to indicate what type of data sets are part of this set. In the future, this practice can prevent opening the set in browse or edit mode to examine which data sets are included.

5. Press Enter.

   If one or both of the data set names that you specified do not exist, the allocation entry panel that is shown in Figure 54 on page 57 opens to allocate and catalog the new data sets.
6. Type the appropriate allocation parameters, but do not change the DCB attributes, and press Enter.

If both named data sets are new, you see the allocation panel a second time. Running these panels allocates and catalogs your new data sets by using dynamic allocation. The first time that you create an unloaded RACF copy and a CKFREEZE data set, you must specify ample disk space. For RACF unloads, allow as much space as used by your live RACF database. For CKFREEZE files, allow at least 2 MB for each online volume, plus space for catalog and HSM information, as well as 2MB per online DASD volume, 2MB per GB HFS/ZFS space, and 1 MB per 5000 IMS or CICS transactions or programs. For more details on space requirements for CKFREEZE data sets, see IBM Security zSecure Admin and Audit for RACF: User Reference Manual.

Do not alter the DCB parameters. Until you are familiar with the disk space required, specify a large secondary allocation quantity (such as 100 MB).

Tip: After you create your first unloaded RACF copy and CKFREEZE data sets, use ISPF to examine them to determine how much disk space was used. You can use this information to estimate future usage.

After you allocate the files, the panel that is shown in Figure 55 opens.

---

**Figure 54. Typical allocation panel**

**Figure 55. Initial view of an input file set under z/OS**
Refreshing and loading files

About this task

The data sets listed constitute one input set. An input set can contain multiple CKFREEZE data sets, multiple SMF files, and multiple HTTP log files. However, an input set can contain only one RACF unload, or one or more RACF data sets from one split database.

To refresh and load files, complete the following steps:

Procedure

1. In the Input file panel (Figure 55 on page 57), type REFRESH in the command line. Press Enter to open the Job submission panel.
2. In the Job submission panel, type a valid job card in the Job statement information section.
3. Use the Edit JCL Option (2) to open the normal ISPF editor to customize the JOB statement and make any other necessary changes to the job. For example, you might need a JOBLIB or STEPLIB statement to access zSecure Admin and zSecure Audit for RACF. If you copied zSecure Collect for z/OS (CKFCOLL) to an authorized library in the LNKLST, you do not need a JOBLIB or STEPLIB statement for it. Assign a job class with a large or unlimited region size.
4. Submit the job.

What to do next

Wait until the job runs. If there is a long queue of jobs that are waiting to run, you can exit from zSecure Admin and Audit while the job completes. The job itself takes only a few minutes to run, unless you have a large configuration. You can add a NOTIFY=yourid in the job card. If the job fails, the problem is usually that there is not enough storage. A region size of 64 MB is typically sufficient to run zSecure Collect for z/OS.

After the job is completed, continue with the next procedure.

Selecting the input set

Procedure

1. To open the Input file panel, type SE.1 (Option 1 on the Setup panel) in the Command line.

   The Input file panel looks like the input set you created, with the description you entered for the input files. An example is shown in Figure 56 on page 59.
In Figure 56, the input file sets marked as selected indicate that zSecure Admin and zSecure Audit for RACF are now using these input sets for the input data. The other input sets are Active primary RACF database, Active backup RACF database, Active backup RACF database, and live SMF data sets. They are always present. You can switch to any input set that is defined in this display. For example, you can switch between the unloaded files you created and the live RACF databases by going to this panel and selecting the appropriate input set.

2. Use one of the available line commands:

   S – Select an input set for processing
   When you select an input set, the data sets it contains are selected for processing. After the data sets are located, the set is marked as selected. This option is also selected by specifying A (Add or Addition of a set). The selected set is an addition to sets already selected. You can change input selections many times during a session, although this change is not typical usage.

   C – Select a set as Compare base.
   Set a predefined set of input files as the Compare base set. Only one set can be selected as the Compare base set.

   M – Select a set as Merge source
   Set a predefined set of input files as the Merge source set.

   U – Remove an input set from selection
   Remove the selection from Active backup RACF data base and live SMF data sets that is selected. The set is not selected any more and is not used in future queries.

### Specifying collections of input sets

#### About this task

With SETUP Collections, you can specify which collection of input sets the program uses. When collections are used, sets of input files that were previously selected through SETUP FILES are no longer used. Subsequent selection of a set of input files through SETUP FILES results in unselecting the collection.

#### Procedure

1. On the main menu, type SE (Setup) in the Option line and press Enter. The Setup menu is displayed:
2. On the Setup menu, type B in the Option line and press Enter. If no collections are defined, the Setup collections definition panel is displayed.

If one or more collections have been defined, the following panel is displayed:

Use the collection display to select collections of sets of input files for processing and to add or delete collections. You can use the following line commands:

- **S** Select a collection. The input sets that are contained in the collection are selected for processing. After the data sets are found in the system, the collection is marked as selected. Sets that are selected through SETUP FILES are cleared. Only one collection can be selected at the same time.

- **U** Clear a collection. The collection is not selected any more. It is not used in future queries.
E  Edit the collection content. On the resulting display, you can select or clear input sets for the collection.

R  Repeat a collection. The contents of the collection you choose are copied into a new collection.

I  Insert a new collection.

D  Delete a collection. The collection is removed from the administration of the dialog. The input sets in the collection are not deleted from the system.

3. To edit a collection, type the E action command in front of the collection and press Enter. The following panel is displayed:

---

**Figure 60. Setup collections sets display**

Use the sets display to add sets of input files to a collection for processing. Sets can be added, edited, and deleted with SETUP FILES. You can use the following line commands:

**B** Browse the contents of a set of input files. By browsing the set, you can check the definitions for the set. When you exit the detail panels, the set is not selected.

**C** Set a set of input files as Compare base.

**M** Set a set of input files as Merge source.

**S** Select a set of input files to be added to the collection. By selecting the set, the data sets it contains are selected for processing. After the data sets are found in the system, the set is marked as selected. This option is also selected by specifying A. A selected set is added to other sets that are already selected.

**U** Clear a set of input files to remove them from the collection. The set is not selected any more and is not used in future queries.

**What to do next**

zSecure Admin offers facilities to maintain the RACF database. The examples show how easy it is to use the zSecure ISPF interface and to control the RACF or **CKGRACF** commands that the product generates in response to the commands issued from the interface.
Other Setup parameters

The Setup panel sets a number of allocation and formatting characteristics for zSecure Admin and zSecure Audit. Inspect these settings and make any necessary changes. The default settings are appropriate for most users. The most used Setup options are Confirm and View.

INSTDATA parameter

Use the INSTDATA parameter to define the layout of the installation data field so that it can be displayed in business-oriented terms in the standard panels.

View and Confirm options

Information about the View options is available in “Access list display settings” on page 25. The following sections describe the remaining settings of the View options and the Confirm options.

The ACL/Connect sort selection defines the access control list and connects sort order. It does the following types of sorts:

- By ID (user or group in the access control list) if you select option 1.
- By user ID (after exploding) if you select option 2.
- By descending access level (Alter-None) or connect authority (Join-Use) if you select option 3.

These sort options make scanning the ACL and connect easy and help you to find what you are looking for quickly.

You can use the Show OS specific options selection to switch between z/OS and z/VM® specific options or tag both to see all options.

When you select the Add summary to RA displays for multiple complexes option, an extra summary section is added to the display panels for options RA.U, RA.G, RA.D, and RA.R. The summary information shows profile differences when multiple complexes are selected. This setting is not saved in your ISPF profile. This option is enabled by default.

Use the Add connect date and owner to RA.U connect group section option to add the connect date and connect owner to the RA.U connect group section.

The Add user/group info to view parameter specifies whether to display information about users and groups (including connect groups) on ACLs. This setting provides complete information. However, it causes zSecure Admin and zSecure Audit for RACF to use much more virtual storage, which requires a larger TSO region.

In the selection field for a parameter, type a / to set a switch-on, or blank to set off the switch.

SMTP options for email output

The Output panel (Option 7 on the Setup panel) contains the SMTP options. You must specify SMTP options to send an email with reports through the Send as e-mail panel options or the M (E-mail report) action command in the Results panel. Ask your system programmer for the correct settings.
In the Setup Output panel that is shown in Figure 61, the SMTP node field specifies the job entry subsystem (JES) destination to which emails are routed for final processing. If the SMTP server is running on your local system, this field can be left blank or you can specify local.

The SMTP sysout field specifies the JES output class to be used for the SMTP output processing of emails.

The SMTP writer field specifies a name for use in SMTP selecting an email SYSOUT data set. The external writer name is equal to the SMTP or CSSMTP address space name. Usually this name is SMTP or CSSMTP.

Defining these SMTP options is required when you use email as the output source.

### Command execution control

The Confirm panel (Option 4 of the Setup panel) is important.

**Note:** For more information about the Confirm panel, see "Generating and confirming RACF commands" on page 37.

The first two parameters apply to zSecure Admin and refer to line commands (such as D (for delete) or C (for copy or clone) and field Overtype when you display various profiles. These line commands generate RACF commands. You can control the steps and execution of commands by selecting the values that you want in the Confirm panel. Type a / before a profile, and then press Enter to see the available commands.

Table 5 shows the Action on command option settings and descriptions.

<table>
<thead>
<tr>
<th>Action on command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Queue</td>
<td>RACF change commands (automatically generated when you use a line command) are written to the CKRCMD file.</td>
</tr>
<tr>
<td>2. Execute</td>
<td>The automatically generated RACF commands are immediately run, after confirmation, in RACF.</td>
</tr>
</tbody>
</table>
### Table 5. Action on command option settings and descriptions (continued)

<table>
<thead>
<tr>
<th>Action on command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Not allowed</td>
<td>No update line commands (like C and D) are permitted in the profile detail panel. Any line commands that are issued are denied.</td>
</tr>
</tbody>
</table>

**Execute display commands (for option 1 only)**

<table>
<thead>
<tr>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This option is valid only if you specify option 1 (Queue) for the <strong>Action on command</strong> field.</td>
<td></td>
</tr>
<tr>
<td>If you specify this option, list commands like LISTUSER, PING, TRACERTE, and RLIST are run even though <strong>Action on command</strong> is set to Queue. This option applies only to the commands generated by the program as list commands. If you change or add commands yourself, it does not apply. For example, FORALL treats all sorts of commands as ordinary commands even if you typed in LISTUSER.</td>
<td></td>
</tr>
</tbody>
</table>

The **confirmation** setting indicates the disposition of the RACF commands that are generated by zSecure Admin. Table 6 shows the **confirmation** option settings and descriptions.

### Table 6. Confirmation settings and descriptions

<table>
<thead>
<tr>
<th>Confirmation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. None</td>
<td>No RACF change commands must be confirmed. None disables the verification prompt; use it only when you understand how to use zSecure Admin.</td>
</tr>
<tr>
<td>2. Deletes</td>
<td>Only Delete commands must be confirmed.</td>
</tr>
<tr>
<td>3. Passwords</td>
<td>Commands containing a readable RACF password are not confirmed. All other commands must be confirmed.</td>
</tr>
<tr>
<td>4. All</td>
<td>The user must confirm all change commands.</td>
</tr>
</tbody>
</table>

**Tip:** Regardless of the preceding settings, you cannot use the facilities that described here to alter the RACF database without having the required authority. An example of such authority is group-SPECIAL, to change the RACF profiles.

The **Command routing** option determines how generated commands are processed. Table 7 describes the available command routing options.

### Table 7. Command routing settings and descriptions

<table>
<thead>
<tr>
<th>Command routing</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Ask</td>
<td>Ask is the maximum prompting level. For all commands or command files, the user is prompted for command routing information. This setting applies to commands generated for the local system and commands that are generated from data sources that are known to be from other systems.</td>
</tr>
</tbody>
</table>
Table 7. Command routing settings and descriptions (continued)

<table>
<thead>
<tr>
<th>Command routing</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Normal</td>
<td>Normal is the default prompting level for command routing. Both internally generated commands and bulk commands that are always queued are run without prompting for command routing options. Confirmation prompting and command queuing are done based on the settings for the user. If the RACF data source applies to the local system, commands are routed to the local system. The user can specify any of the following remote options for a local data source RRSFNODE, ZSECNODE, JESNODE. These remote indicators are ignored for a local data source. If the commands are not for the local system, they are routed to one of the following systems in order of preference: 1. The ZSECNODE or the ZSECYSYS as specified on the RACF data source that is used for this profile. 2. The RRSFNODE node that is associated with the RACF data source used for this profile. The command uses the AT keyword and specifies either the associated user ID if the terminal user has an association with a user ID on the target RRSFNODE, or the current user ID. 3. The NJE node that is specified for the RACF data source. If a specific routing mechanism is selected and fails, there is no automatic fallback to another routing mechanism.</td>
</tr>
<tr>
<td>3. Local only</td>
<td>Independent of the input source, this option routes the command to the local system. If the local system is part of an RRSF autocommand environment, RRSF processing might route this command to other RRSF nodes.</td>
</tr>
</tbody>
</table>

You can modify many fields while you display profiles if you are running zSecure Admin with the Overtype fields in panels option in the Command generation section of the panel. Based on the modifications, zSecure Admin and zSecure Audit for RACF automatically generate the RACF commands necessary to make the changes you want. These change commands are also subject to the action on command and confirmation settings that described previously. The ability to modify fields is one of the most important usability features. It provides an easy way to make minor changes in existing RACF profiles.

All zSecure Admin and zSecure Audit for RACF setup parameters are saved in your personal ISPF profile data set. Therefore, each user can have different setup parameters. If you access zSecure Admin and zSecure Audit for RACF by using multiple user IDs, you might have different setup parameters for each user ID.

### Changing and verifying values

#### About this task

This example uses the RA.U function that you are already familiar with to illustrate the ability to change values by using the Overtype function and verify options.

To demonstrate these options, complete the following steps:
Procedure
1. Go to the Main menu. (Press PF3 as necessary.)
2. From the Main menu, select option RA (RACF Administration).
3. Select option U (User).
4. Type a value for **Userid** or type a value for **Default group** (SYS1, for example) to obtain a display with multiple profiles.
   You can type over a value in any underlined field. For example, to change the password interval for one of the profiles, type a new value in the **PwInt** column.

   **Tip:** If no fields are underlined, type **SET** in the command line and press Enter. Verify that the **Overtype fields in panels** option is selected (/ in front of the option).

If this method does not work, complete the following steps:
- Type **SETUP** in the **Command** field to go to the Setup panel.
- In the Setup panel, select **Options** from the bar. Press Enter, and then select **1. Settings**.
- Select **Colors** from the bar, and then select **2. CUA attributes**.
- For all entry field rows, change the Highlight column to the value **USCORE**.
- Reissue the query.
   If you still do not see underlines, you probably have a terminal type (or you are emulating a terminal type) without extended Data Stream support.
5. Press Enter.
   zSecure Admin generates the appropriate RACF command to change the password interval of the involved user and prompts you to verify the command before execution.
   Remember to scroll left and right by using the standard ISPF function keys and to issue an **S** (Select) line command for more details.
6. Press PF3 to reject (not run) the RACF command or press Enter to submit the RACF command.
   If you elected to submit the command, zSecure Admin for RACF submits the command as though you entered the command in the TSO command line. You must have appropriate authority (for example, SPECIAL or ownership) before RACF accepts the command. If you do not have appropriate authority, you receive a RACF violation error message.
   You can type over the value in the installation data field in a profile, changing only the characters you want to change. Alternatively, you can issue the **MI** (manage user ID information) line command to edit the whole field. You can also work with user-defined fields in the installation data.

**Line commands for common tasks**
When you display a profile, you can issue line commands by typing a letter in the first character position of the displayed profile line and pressing Enter.

The most common functions are as follows:

<table>
<thead>
<tr>
<th>Letter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>for copy</td>
</tr>
<tr>
<td>D</td>
<td>for delete</td>
</tr>
<tr>
<td>L</td>
<td>for list</td>
</tr>
</tbody>
</table>
When you issue a line command, zSecure Admin and zSecure Audit for RACF generate the appropriate RACF commands to do the requested function. A common technique is to use the **Copy** line command to reproduce a profile. Then, type over the values in the fields that you want to be different in the new profile later.

The **L** line command runs a RACF list command in the primary RACF database for the profile you issue the **L** for. You can also use this command in a detail display.

**Note:** The **L** line command always reports from the primary RACF database.

To view a list of the line commands available in a profile overview display, type the **/** line command. For the **RA.U** function, you must scroll down (PF8) to see all of the application line commands.
Chapter 6. Creating and viewing a report

About this task

This task introduces the basic steps for generating a report and viewing the results. In this example, you generate a report to examine the scope of a specified user ID.

Procedure

1. From the IBM Security zSecure Admin and Audit for RACF Main menu, complete the following steps:
   a. Select option RA (RACF Administration).
   b. Select option 3 (Reports). On the next panel, you can select one of the predefined reports.
   c. Select option 4 (Permit/Scope).

2. On the Report panel, create a report that shows you the scope of the specified user:
   a. Type a user ID. For this exercise, it does not matter whose user ID you enter.
   b. Specify 3 (type of authorization is Scope – Access or administrative authority by any means).
   c. Type / in front of Output in print format in the Specify output options section of the screen and press Enter.
   d. Press Enter in the next panel. On this panel, you can exclude some of the ways that the entered Group or User can have access to certain resources. During this evaluation, however, do not exclude any of the options. Explore all the methods by which a Group or User can have access to a resource.

Results

zSecure Admin and Audit for RACF searches the RACF data. The report results are displayed on an overview panel that lists the classes and scope of access for the specified user ID. The Figure 62 on page 70 shows detailed information about the selected class.
After you examine the report, press PF3 to produce the Results panel. All reports generate the Results panel, see Figure 63 on page 71.

Tip: If you want to produce a scope report that shows only the access a user has through their user ID and group connects, select option 2 - Direct permit or Connect (Id or Connect Group on access list).

Results panel

The Results panel is presented after many queries or functions. Familiarize yourself with its operation. You can use the panel to review results in several different ways and save useful material from the functions. Useful material can include RACF commands that are generated by zSecure Admin and zSecure Audit for RACF while it processes the last functions.

Reports overwrite the same files every time. That is, the files like SYSPRINT, REPORT, and CKRCMD are rewritten every time that the primary modules are called. Save any important results with W line command on the Results panel before you start another query or function.
The names of some of the files on the display are highlighted to indicate that the last operation generated data in these files. When applicable, you can browse, edit, save, run, or submit any of these files with one of commands that are at the top of the Results panel.

**Tip:** You can use the `RESULTS` primary command in the command line of most panels to obtain the current Results panel.

To print DISPLAY results, use the `PRT` command.

### Archiving report output

**About this task**

This task shows the basic steps for generating an archive data set. The archive data set can be a sequential or a partitioned data set.

If you specify a data set name that does not exist, zSecure Admin and Audit prompts you for allocation parameters.

**Procedure**

1. In the Results panel, enter a `W` in front of the `REPORT` keyword. A panel opens where you can specify the data set name of an archive data set.
2. Specify the parameters that are required to create a sequential or a partitioned data set:
   a. For a sequential data set, you can write over the content by selecting disposition Overwrite, or append to the end of the current content by selecting disposition Append.
   b. For a partitioned data set, you can specify a member name and the dispositions Overwrite or Append, or choose disposition of Generate and leave the member name blank. Generate assigns a unique member name to each report, so you are not required to choose a member name.

3. Press Enter to create the data set.
4. Press PF3 to exit from the Results panel.

   The Results panel exists after any search. However, it is automatically displayed only if files other than SYSPRINT contain output.

   **Tip:** The next function that you run overwrites these result data sets. If you want to save any of the data sets, do it before you run the next search.

---

**Mailing report output**

**About this task**

The Mail option is valid only if you specified SMTP configuration options in Setup Output definition panel (SE.7). See “SMTP options for email output” on page 62. Do not attempt to send an email if the SMTP routing parameters are not defined.

**Procedure**

1. In the Results panel, enter an M in front of the REPORT keyword. The Figure 65 opens.

```
Menu Options Info Commands Setup
------------------------------------------
Command ===> ________________________________

Specify e-mail data
From    .... &jobname at &system <mbox@domain>_______________________________
Mail to . . . . ________________________________________________
CC       . . . . ________________________________________________
BCC      . . . . ________________________________________________
Reply to . . ________________________________________________
Output format 1  1. Normal (MIME/HTML)
                 2. Plain text (formatting may be lost)
Font size . . ________________________________________________
Subject . . ________________________________________________
Additional data (e.g. signature)

______________________________________________________________________________
______________________________________________________________________________
______________________________________________________________________________
______________________________________________________________________________
______________________________________________________________________________
______________________________________________________________________________

Figure 65. Email specification panel
```

2. Specify the recipient of the email and any additional formatting or notation.
3. Press Enter to send the email.
Chapter 7. Verify functions

The Verify functions help you to analyze RACF and z/OS integrity and security data. For example, many of the functions compare RACF data with what actually exists on your disks (as read by zSecure Collect for z/OS). In addition, most functions automatically generate RACF commands to correct problems found during analysis. These commands are not automatically run; they are only presented for your review or use.

The first time that you use Verify functions, you might receive more output than you expect, especially if you have a large installation that is relaxed in DASD and RACF cleanup policies. There is a default limit of 50 messages per disk volume, but optionally you can override this limit through a lower-level panel. Product messages are concise and exact, but might take a little study to absorb. Also, do not assume that your installation must correct all the anomalies reported by all of the various Verify functions. Your installation, for example, might not agree with the security policies implicit in some reports. Use the information as appropriate, but do not accept it blindly.

After a Verify function completes, the results are presented with the Results panel. Generally, if RACF commands were generated, these commands are displayed first. Sometimes, the SYSPRINT output is presented directly after the completion of the Verify function.

The SYSPRINT file contains more information about the problems that are found during analysis that is done by a Verify function, such as, concise descriptions of the anomalies and problems that are found during the analysis. When you enter the command `find 'verify '` in the command line, you go directly to the `MESSAGESVERIFY` section of the SYSPRINT file. A space between the characters and the delimiting single quotation marks are required.

- "Running the Verify functions"
- "Running the Verify functions for the first time" on page 75

Running the Verify functions

About this task

This topic describes how to run the Verify functions and provides a brief description of each function. Read the overview of the Verify functions in Chapter 7, “Verify functions” before you run them.

If you are running the Verify functions for the first time, follow the procedure in “Running the Verify functions for the first time” on page 75 for a sample walkthrough.

To display and select a Verify function, complete these steps:

Procedure

1. Select option AU (Audit) from the Main menu.
2. Select option V (Verify) to open the Verify selection panel that is shown in Figure 66 on page 74.
You can select one or more of the Verify functions for execution, although it
would be unusual to select more than three at a time. Before you try any of the
Verify functions, review the function descriptions in Table 8 and Table 9 on
page 75.

Table 8. Verify functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>Reports on any IDs (Users or Groups) used in RACF access control lists, or ownership fields, that are not currently defined as valid IDs. If these invalid IDs are defined and made valid again with a new user, this new user instantly inherits all the authorities of the former owner of that user ID. This exposure can be severe. A more severe exposure is that anyone with group-SPECIAL or JOIN authority can create a group with the same name as the ID in the access control list and obtain the authority of the ID.</td>
</tr>
<tr>
<td>User Permit</td>
<td>Reports on any resource profile that contains a user ID in the access control list, while that user is also connected to one or more groups that are also in the same access control list. The access levels of both the user ID and the group or groups are compared. If the access for that specific user ID is equal to the highest access of any connected group, the user ID entry is redundant and is eligible for removal.</td>
</tr>
<tr>
<td>Connect</td>
<td>Verifies that connect information in user and group profiles is consistent.</td>
</tr>
<tr>
<td>PADS</td>
<td>Verifies that every program on a RACF conditional access control list has a corresponding Program profile. PADS administration is often complicated, and several Verify functions address it.</td>
</tr>
<tr>
<td>Group tree</td>
<td>Detects loops in your group definitions. These loops usually happen when either RACF administration is not centralized or administrators change frequently. RACF prevents loops from occurring by checking whether an ALU or ALG command causes a loop.</td>
</tr>
<tr>
<td>Password</td>
<td>Checks every user password in the RACF database with several trivial values. The Password function cannot be performed on an Unload file, because the passwords are not unloaded.</td>
</tr>
</tbody>
</table>

The Verify functions described in Table 9 on page 75 require a CKFREEZE data set.
Table 9. Verify functions that require a CKFREEZE data set

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect all</td>
<td>Lists all disk data sets that are not protected by a generic or discrete RACF profile. If your installation is using a RACF PROTECT ALL environment, try this function. If you are not in a PROTECT ALL environment, be prepared for a large amount of output.</td>
</tr>
<tr>
<td>On Volume</td>
<td>Verifies that each discrete RACF profile has a corresponding data set on DASD. Often old discrete profiles remain in RACF long after the data set is deleted.</td>
</tr>
<tr>
<td>Not empty</td>
<td>Identifies obsolete generic profiles. This function verifies that generic data set profiles that protect subsets of more general generic profiles have existing data sets being protected by the generic profile. Take care when using this function. Profiles meant to protect future or periodic allocations might be empty (no data sets exist under the profile) at the time the Verify check is made.</td>
</tr>
<tr>
<td>All not empty</td>
<td>This function is a more general case of the Not empty check. It verifies that all generic profiles are being used to protect real data sets. It can be used to find unneeded generic profiles. RACF and z/OS have no mechanism for automatically removing generic profiles, and large numbers of obsolete profiles can accumulate over time.</td>
</tr>
<tr>
<td>Indicated</td>
<td>Verifies that all RACF data sets with RACF indicator bit set in the DSCB or catalog have a corresponding discrete profile.</td>
</tr>
<tr>
<td>Program</td>
<td>Verifies that each data set listed as a member in a Program profile does exist.</td>
</tr>
<tr>
<td>Pgm exists</td>
<td>Verifies that each Program profile covers at least one load module in a data set, as specified by the profile. If modules are moved from one library to another, there is no automatic update of RACF Program profiles and the modules are no longer protected. The Program and Pgm exists functions help you to maintain a clean PADS environment.</td>
</tr>
<tr>
<td>Started task</td>
<td>Checks the consistency of the started procedure table (ICHRIN03) with various RACF user, group, and STARTED class profile definitions and with procedure members defined for JES2 and MSTR.</td>
</tr>
<tr>
<td>TSO all RACF</td>
<td>Checks the users that are defined in the SY51.UADS data set with the user definitions in RACF and reports any UADS ID$ that can log on bypassing the control of RACF.</td>
</tr>
<tr>
<td>Sensitive</td>
<td>Checks the protection of z/OS sensitive data sets against a baseline policy. If the protection is insufficient, it generates a RACF command to fix the situation either by adding a correct profile or by fixing or improving the offending profile.</td>
</tr>
</tbody>
</table>

Some of the Verify functions are more important than others. If you are not in a PROTECT ALL environment, the Permit and Protect All functions might be the most important.

Running the Verify functions for the first time

Procedure

1. Type / in the INDICATED line in the Verify panel and press Enter. The CKRCMD command file that is shown in Figure 67 on page 76 automatically opens.
In this example, the installation contains two data sets that are RACF-indicated while the corresponding discrete data set profile is missing from the RACF database. If necessary, use the ISPF functions PF7, PF8, PF10, and PF11 to scroll the panel so that you can view all the data.

As you can see, the generated commands can be run to fix the inconsistencies that are found by the Verify Indicated function.

1. Press PF3 to open the Results panel.
2. Select the SYSPRINT file if you want to view the details of the Verify function.
3. Type `find 'verify '` command on the command line to jump to the messages section of the SYSPRINT file instead of scrolling down several panels. Alternatively, you can scroll to the bottom of the file and, if applicable, scroll back up one or two pages. 

4. Type `find 'verify '` command on the command line to jump to the messages section of the SYSPRINT file instead of scrolling down several panels. Alternatively, you can scroll to the bottom of the file and, if applicable, scroll back up one or two pages. 

5. To return to the Verify Selection panel, press PF3 twice.
6. Type `/` in the Permit line.
7. Remove the `/` from the Indicated line. Step through the next panels until zSecure Admin and zSecure Audit for RACF runs the function.

Unless you maintain a clean database, zSecure Admin and Audit for RACF probably finds invalid user IDs in the database. If there are many of these user IDs, you can print the report and study it offline. Invalid user IDs can present complex problems that are not suitable for on-the-fly repairs.

**Tip:** When RACF commands are generated by one of the Verify functions, the solution suggested by zSecure Admin and Audit for RACF might not be
appropriate or might require adjustment to your environment. Always look at
the commands closely. If necessary, look in the SYSPRINT file for more
information before you run them.
Chapter 8. Auditing system integrity and security

About this task

You can use the **AU.S** function to view the current SETROPTS settings. A range of z/OS integrity and security checks is available under the **AU.S** option in the primary menu. For example, you can view the current SETROPTS settings by using this function.

Procedure

To use the **AU.S** function, complete the following steps:

1. Select option **AU** (Audit) from the Main menu.
2. Select option **S** (Status) to open the Audit Status panel.

   You can use this panel to select one to five report categories. First, explore the **RACF control** (RACF oriented tables) category.

   ![Figure 69. Audit Status](image)

3. Select the category **RACF control** and type / before **Select specific reports from selected categories**. Press Enter.

   **Note:** The Audit policy can be set. The C1, C2, and B1 policies are security standards that are described by the US Department of Defense in a document that is known as the *Orange book*. The default policy is a standard that is a practical and achievable security level that is applicable to most companies. The policy defines what is classified as an exposure.

4. Select the report **SETROPTS** to generate a report of the current RACF system options of this installation and the report **RACFCLAS** to report in the class descriptor table and number of profiles.

5. Press Enter to generate the requested reports.

   The panel that is shown in [Figure 70 on page 80](image) opens so that you can select and view the reports.
6. Select the **SETROPTS** report. Then, press Enter to open the SETROPTS setting panel that is shown in Figure 71.

   The current SETROPTS (**SET RACF** options) are listed in this report. You can use PF8 to scroll down to see the other SETROPTS parameters that are currently active, such as system-wide audit settings and password rules.

7. Press PF3 to return to the report overview.

8. Select **SETROPAU** to open the report that is shown in Figure 72.

   This report lists the audit concerns related to the current SETROPTS settings. Audit concerns give an indication of possible security exposures in the current installation.

   zSecure Audit for RACF ranks the severity of problems found. These problems are in the **Pri** field, and are numbers 0 - 255. Be aware, however, that
understanding the reason for those rankings requires some knowledge of z/OS internals and some judgment of the context of the total system. Table 10 provides a rough categorization of the audit concern priorities.

Table 10. Audit concern priority categories

<table>
<thead>
<tr>
<th>Priority</th>
<th>Type</th>
<th>Explanation and action required</th>
</tr>
</thead>
<tbody>
<tr>
<td>40-255</td>
<td>Exposure</td>
<td>A serious potential security exposure and concern for an auditor. Requires an immediate action.</td>
</tr>
<tr>
<td>20-39</td>
<td>Concern</td>
<td>A serious security threat. Requires an action, but it is less urgent.</td>
</tr>
<tr>
<td>11-19</td>
<td>Housekeeping</td>
<td>Minor problem or authority that must be audited, reviewed, and approved or denied. RACF housekeeping can remove many of these concerns.</td>
</tr>
<tr>
<td>1-10</td>
<td>Watch</td>
<td>Read it, and resolve it as time permits.</td>
</tr>
<tr>
<td>0</td>
<td>OK</td>
<td>No audit concern.</td>
</tr>
</tbody>
</table>

By default, the Audit concerns are sorted by descending priority. The details of the audit concerns can be displayed by entering an S or I in front of the concern you want to view. To view the Audit concerns, complete the following steps:

a. Press PF3 again to return to the report overview.

b. Select report RACFCLAS and press Enter to open the Audit Status RACFCLAS report that is shown in Figure 73.

This report displays the contents of the RACF Class Descriptor Table. You find a record for all classes that are defined to RACF.

Figure 73. Audit status RACFCLAS report

In this report, the classes are sorted by descending audit concern priority. However, you can sort this overview by any column that you want. The result of entering the sort pos command is that this overview is reordered according to posit number, while the result of the sort class command is that the classes are sorted alphabetically by class name.
Tip: The help panels provide background information and explanations.
Chapter 9. Rule-based compliance evaluation

AU.R is the user interface of the zSecure Audit Compliance Testing Framework. The framework was introduced to help automate the compliance checking of newer external standards as well as site standards, and to save time for other security tasks. Standards can be customized.

To use rule-based compliance evaluation, you must ensure that the CKACUST data set was created with the proper members to define which users or groups are compliant for which tasks. See the Installation and Deployment Guide for information on creating the CKACUST data set. A sample compliant user member is shown here:

```
EDIT CRMASCH.MY.CKACUST(SYSPAUDT) - 01.00 Columns 00001 00072
Command ===>
****** ******************************************** Top of Data ********************************************
 000001 * Systems Programmers or Systems Administrators *
 000002 SYSPROG
 000003 SYSPROG
****** ******************************************** Bottom of Data ********************************************
```

Figure 74. Sample compliant user member

By default, the CKACUST data set is used that is specified in the zSecure configuration that is used to start the product. You can also specify a CKACUST data set in CO.1, which overrides the default. Note that data set concatenation is used, so only members with actual overrides need to be created. If no CKACUST data set is present in the zSecure configuration, you can use SCKRSAMP member CKAZCUST to create an "empty" set of members. To prevent error messages, a complete set of members is required.

CARLa DEFTYPES are used to look up IDs in the CKACUST members that specify the compliant populations.

Standards are, in effect, sets of predefined compliance rules. The standards as defined to zSecure Audit for automated checking are usually part of a wider standard. The wider standard also includes organizational rules for which checking cannot be automated.

Standards are defined with the CARLa statement STANDARD. If you want to add site rules, you need advanced knowledge of the CARLa command language. The built-in standard checks are provided in separate members in the SCKRCARL library for each individual rule set (=external standard rule). These members have these naming conventions:

- CKAG* members are RACF STIG rules.
- C2AG* members are ACF2 STIG rules.
- CKAO* members are GSD331 rules.
About this task

You can report on multiple standards and complexes at the same time. If you are analyzing large systems, the amount of concurrent analyses might be limited by the amount of memory available to your TSO userid (REGION session parameter).

Procedure

1. On the Main menu, type AU.R (Audit - Rule-based compliance evaluation) in the Option line and press Enter. The Audit Compliance menu is displayed:

   ![Audit Compliance Menu]

2. Select the standard you want to verify against in the Compliance evaluation section.

   The STIG and GSD selections refer to predefined subsets for these standards:
   - **GSD**: IBM standard often employed in outsourcing (GSD331)

   The Other standard member selection can be used for a site standard, or an older version of STIG and GSD.

   The Test a single rule selection is provided to assist in testing when developing a site standard. The specified member is included from a concatenation of CKRCARLA libraries. The concatenation order is shown here:
   - a. CKRCARLA library selected with CO.1
   - b. CKRCARLA library specified with UPREFIX, if applicable
   - c. CKRCARLA library specified with WPREFIX, if applicable
   - d. CKRCARLA library shipped with the product

   You can use the display format to zoom in across the following levels:
   - a. Security complex level, showing the standards tested for each security database and systems related to that database
   - b. Rule set level, showing the number of non-compliant objects per rule set
   - c. Object level
   - d. Individual test result overview level
   - e. Detail level
The following figure shows an example of output for the rule set level:

<table>
<thead>
<tr>
<th>Command</th>
<th>Standard compliance test results</th>
<th>Line 1 of 47</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scroll</td>
<td>Standard compliance test results</td>
<td>Line 1 of 47</td>
</tr>
<tr>
<td></td>
<td></td>
<td>14 Jun 2011 07:13</td>
</tr>
<tr>
<td>Complex</td>
<td>Ver Standards NonComp Unknown Exm Sup</td>
<td></td>
</tr>
<tr>
<td>ADCDPL</td>
<td>2 2 2 1</td>
<td></td>
</tr>
<tr>
<td>Standard</td>
<td>Rule sets NonComp Unknown Exm Sup Version</td>
<td></td>
</tr>
<tr>
<td>RACF_STIG</td>
<td>47 25 5 2 6.14</td>
<td></td>
</tr>
<tr>
<td>Rule set</td>
<td>Rule set Objects NonComp Unknown Exm Sup Description</td>
<td></td>
</tr>
<tr>
<td>ACP00170</td>
<td>8 7 Allocate access to SYS1.U</td>
<td></td>
</tr>
<tr>
<td>IFTP0060</td>
<td>1 1 1 SMF recording options for</td>
<td></td>
</tr>
<tr>
<td>IFTP0090</td>
<td>1 1 1 The TFTP Server program i</td>
<td></td>
</tr>
<tr>
<td>ITNT0060</td>
<td>1 1 1 SMF recording options for</td>
<td></td>
</tr>
<tr>
<td>RACF0244</td>
<td>1 FACILITY resource class i</td>
<td></td>
</tr>
<tr>
<td>RACF0246</td>
<td>1 The OPERCMDS resource cla</td>
<td></td>
</tr>
<tr>
<td>RACF0248</td>
<td>1 1 MCS consoles are not acti</td>
<td></td>
</tr>
<tr>
<td>RACF0250</td>
<td>1 The Automatic Data Set Pr</td>
<td></td>
</tr>
<tr>
<td>RACF0260</td>
<td>178 178 All active classes must b</td>
<td></td>
</tr>
<tr>
<td>RACF0270</td>
<td>2 1 The CLASSACT SETROPTS mus</td>
<td></td>
</tr>
<tr>
<td>RACF0280</td>
<td>1 The CMDVIOL SETROPTS valu</td>
<td></td>
</tr>
<tr>
<td>RACF0290</td>
<td>1 The EG N SETROPTS value sp</td>
<td></td>
</tr>
<tr>
<td>RACF0310</td>
<td>178 35 12 The GENOMD SETROPTS valu</td>
<td></td>
</tr>
<tr>
<td>RACF0320</td>
<td>178 35 12 The GENERIC SETROPTS valu</td>
<td></td>
</tr>
<tr>
<td>RACF0330</td>
<td>1 The TERMINAL SETROPTS valu</td>
<td></td>
</tr>
<tr>
<td>RACF0350</td>
<td>1 The GRPLIST SETROPTS valu</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 10. SMF data queries

Note: The SMF Query function is available only in the zSecure Audit product.

The SMF displays can work with the live SMF data sets, SMF log streams, or with sequential SMF data. SMF data is produced by the IBM IFASMFDP or IFASMFDL programs. While you are getting familiar and experimenting with zSecure Audit for RACF, work with sequential SMF data rather than the live SMF files. Using static, sequential data provides more consistent results when you try something with slightly different parameters.

You must consider what SMF data you use with zSecure Audit. The amount of SMF data that is collected by z/OS varies greatly among different installations. In some cases, you can place a week of data in a reasonable DASD allocation (30 MB, for example). In other cases, that allocation might hold only an hour of SMF data collection. For simple experimentation with zSecure Audit for RACF, a set of SMF data in the 10-30 MB range is reasonable. If you must apply filtering to reduce the size of the data set, make sure that the record types shown in Table 11 are not filtered out.

Table 11. SMF Record types to not filter out of the SMF data

<table>
<thead>
<tr>
<th>Record type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>INPUT or RDBACK data set Activity</td>
</tr>
<tr>
<td>15</td>
<td>OUTPUT, UPDATE, INOUT, or OUTIN data set Activity</td>
</tr>
<tr>
<td>17</td>
<td>Scratch data set Status</td>
</tr>
<tr>
<td>18</td>
<td>Rename data set Status</td>
</tr>
<tr>
<td>30</td>
<td>Common Address Space Work</td>
</tr>
<tr>
<td>60</td>
<td>VSAM Volume data set Updated</td>
</tr>
<tr>
<td>61</td>
<td>ICF Define Activity</td>
</tr>
<tr>
<td>62</td>
<td>VSAM Component or Cluster Opened</td>
</tr>
<tr>
<td>63</td>
<td>VSAM Catalog Entry Defined</td>
</tr>
<tr>
<td>64</td>
<td>VSAM Component or Cluster Status</td>
</tr>
<tr>
<td>65</td>
<td>ICF Delete Activity</td>
</tr>
<tr>
<td>66</td>
<td>ICF Alter Activity</td>
</tr>
<tr>
<td>67</td>
<td>VSAM Catalog Entry Delete</td>
</tr>
<tr>
<td>68</td>
<td>VSAM Catalog Entry Renamed</td>
</tr>
<tr>
<td>69</td>
<td>VSAM Data Space, Defined, Extended, or Deleted</td>
</tr>
<tr>
<td>80</td>
<td>RACF Processing</td>
</tr>
<tr>
<td>81</td>
<td>RACF Initialization</td>
</tr>
<tr>
<td>83</td>
<td>RACF Processing Record for Auditing data sets</td>
</tr>
<tr>
<td>90</td>
<td>System Status</td>
</tr>
<tr>
<td>92</td>
<td>UNIX Hierarchical file system</td>
</tr>
<tr>
<td>102</td>
<td>DB2® Performance and Audit</td>
</tr>
<tr>
<td>109</td>
<td>Firewall</td>
</tr>
<tr>
<td>118</td>
<td>TCP/IP Telnet and FTP</td>
</tr>
</tbody>
</table>
Table 11. SMF Record types to not filter out of the SMF data (continued)

<table>
<thead>
<tr>
<th>Record type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>119</td>
<td>TCP UDP and IP</td>
</tr>
<tr>
<td>120</td>
<td>WebSphere® Application Server</td>
</tr>
</tbody>
</table>

You can also run the zSecure Audit for RACF SMF analysis on a full SMF file with all record types present. zSecure Audit for RACF supports approximately 100 different SMF record types.

Defining input sets

About this task

When you opt to process SMF data, the data sets must be defined to zSecure Audit for RACF. Before you can process SMF data, you must specify the input data, using the Setup File (SE.1) option.

Procedure

1. Select option SE (Setup) from the Main menu and press Enter.
2. Select 1 (Input Files) and press Enter to open the Setup Input panel. For information about this panel, see “Selecting the input set” on page 58.
3. Move the cursor to the input field (left-most position) on a line.
4. Type the letter I and press Enter to insert a new input set. The Setup Input panel opens but without data.
5. Type a title such as Filtered SMF data set in the Description field below the Command line.
6. Move the cursor to the first Data set or Unix file name field. Type the name of the data set that contains SMF data. Then, press Enter.
   If the data set name ends with .SMF, the file type (SMF) is automatically entered. If it does not end with .SMF, a panel, such as Figure 75 on page 89 opens so that you can assign a type to the file you are defining.
7. Select option SMF and press Enter to create a line that references the live SMF data.


You return to the Input file panel with the new input set selected.

Tip: You can select multiple input sets at the same time. Consider defining a set for each file or couple of files. For example, define a live SMF set and a most recent unload of the RACF database and CKFREEZE data set and select both sets as input.

Results

Your input file settings look similar to the file settings in Figure 76.

To use live SMF data, you do not need to specify a data set. Type / in the Type field, and then press Enter. The panel in Figure 75 opens so that you can select option ACT.SMF.

This form is the most basic form of SMF input. In a more complex situation, you can combine live SMF plus the most recent n generations. Use Generation Data.
Creating SMF reports

About this task

You can generate an SMF report about SMF records that match your specified selection criteria.

Procedure

1. Select option **EV** (Events) in the Main menu and then press Enter.
2. Select option 2 (RACF Events) and then press Enter.

   Enter "/" to select report(s)
   _ All events Overview of all following RACF events (except IPL)
   _ Logging RACF logging of all events except RACINIT
   _ Not normal RACF access not due to normal profile access
   _ Warnings RACF access due to profiles in warning modes
   _ Violations RACF access violations
   _ Commands RACF command auditing
   _ CKGRACF zSecure Admin CKGRACF commands
   _ IPL RACF RACF initialization

   Menu Options Info Commands Setup
   _________________________________________________________________
   Option ===> zSecure Audit for RACF - Events - RACF events

   Select SMF records that fit all of the following criteria
   Use EGN masks for selection criteria
   Userid ...... IBMUSER
   Jobname ... ...
   Terminal ... ...
   Dataset name ... ...
   Profile class ... ...
   Profile key ... ...
   Level ... ... (installation defined resource level)
   From Until Intended access at least
   Time ____ : ____ 6. All access
   Date __________ : __________ 3. Update 4. Control
   Weekday ____ : ____ 5. Alter 6. All access
   Show all _ Success _ Warning _ Violation

   Menu Options Info Commands Setup
   _________________________________________________________________
   Command ===> zSecure Admin+Audit for RACF "DOWN " is not active

   Only SMF records that match your specified selection criteria are processed. Any fields in this panel that you do not use are not considered in the selection process. For this panel:
The Userid, Jobname, Terminal, Profile class, Profile key, and Data set name fields each accept one or more search strings that are separated by blanks. Wildcards, such as %, *, and ** can be used. A single asterisk with no other parameters in the Userid field selects all SMF records that can be attributed to a RACF user.

You can use the Level field to select by data set or resource level. Use the first field to specify the operator to determine a level present in the profile. Use < and <= for selection less than or equal to the level. Use > or >= for high level, = for exact level, ~= and <> for all but the specified level.

The second field is to specify a number for the data set or resource level. This level is not set or updated by IBM utilities, but it can be used by the installation.

Your user ID is not automatically prefixed to data set names.

Times are specified in 24-hour HHMM format.

Dates are specified as YYYY-MM-DD, DDMMYYYY or YYYY/DDD; for example, 2012-03-01, 01MAR2012, or 2012/301. A range of dates is separated by a colon; for example, 10APR2005:14APR2012.

Weekdays are spelled in English with the first three letters; for example, Mon for Monday.

In the Intended access at least field, you can select only access events that required, at least, the authority you specify.

After the selection panel, an exclusion panel opens. The exclusion panel looks similar to the selection panel in Figure 78 on page 90. If an SMF record passes the selection process, it can still be rejected by the exclusion parameters. You do not need to specify any exclusion parameters. As an example, select all accesses to data sets with the name SYS*. with access level at least UPDATE, but exclude access to data set SYS1.BRODCAST.

What to do next

After the selection and exclusion panels, there are panels to control the report that generated. These panels can be used to limit the number of input records. Especially if your SMF file is huge, limit the number of output records and format output for displaying or printing.

For this example, do not select any CKFREEZE data set to use with SMF reports. Make sure that there is no / before Use CKFREEZE data in the SMF process options panel. For RACF only purposes, this option is not needed and can increase the TSO region size required. You do need this option to format UNIX file system records (type 92).

The SMF search produces an overview report. One line for each SMF record and a statistical summary is displayed. You can enter an S line command for a detailed display of any of the records.

zSecure Audit for RACF processing of SMF records is fairly straightforward. Its power lies in good use of the selection and exclusion panels and the high-speed processing. Nevertheless, effective use of SMF processing requires planning on your part. You must have reasonable amounts of recent SMF data available that is easily accessible online or through HSM facilities.

zSecure Audit for RACF supplements any SMF event record with information from the RACF data source if such information is missing from the record. In this way, z/OS event records like type 14 and 15 can be attributed to a RACF user ID even
if the Jobname in the SMF record does not match the appearance of the RACF user ID.

### Auditing types of users

**Before you begin**

To audit a user event trail, you must have an input data set that contains SMF data selected first. Then, complete the following steps:

**Procedure**

1. Return to the Main menu.
2. Select option **EVU** (Event, User events) to open the User Selection panel that is shown in [Figure 79](#).
   
   This panel is the starting point for finding the audit trail of one or more specific users or finding events that are caused by some types of users.

3. In the **Advanced selection criteria** section, select **User actions**, and press Enter. You now see a selection panel with the types of actions recognized.
4. Type a `/` in **RACF/CKGRACF commands** issued and another `/` in front of **Successful**. Then, press Enter to open the RACF command overview panel that is shown in [Figure 80](#) on page 93.
   
   This panel shows the successful RACF commands that are issued in your system. You can scroll right by using PF1.
5. To see more detail than a one-line summary per record, select option **Include detail** in the **Output/run options** section of the panel that is shown in Figure 79 on page 92 and rerun the query.

6. In the RACF Event log overview panel, select a record to open the panel that is shown in Figure 81.

   Now, you can see the details; for example, the full command and fields that identify the user.

---

**Change tracking**

**Note:** This function is available only in zSecure Audit for RACF.

The **Change Tracking** function is a powerful way of ensuring that changes in sensitive RACF and SYSTEM definitions are tracked. You can list differences between the verified base and the current configuration.

There are different kinds of sensitive RACF definitions. Some examples are: system-wide SPECIAL users, OPERATIONS users, and profiles that protect sensitive data sets. SYSTEM-related sensitive definitions are, for instance, APF defined data sets such as APFLIST. You can also identify other RACF or SYSTEM definitions as sensitive in addition to those definitions already marked as sensitive.
Other system settings that can be monitored include changes to the list of APF-authorized libraries and changes to the RACF Class Descriptor table. You can track changes to most items that zSecure Audit for RACF show information about.

Tracked changes must be accepted or rejected, or deferred. You accept a change to update the verified base, or you reject a change because of an incorrect modification. If you reject a change, ensure that you also undo the modification in your configuration. Otherwise, during the next Change Tracking step, the same modification is reported again.

Library change detection

**Note:** This function is available only in zSecure Audit for RACF.

Using the **Library Change Detection** function in a realistic manner requires a certain amount of planning and time. After you review the short description that follows, you can decide whether you want to use this function during your evaluation. The function is described, in detail, in the *Library Audit* section of the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.

The **Library Change Detection** function provides a library update report. It is used to find and display changes to members that consist of load modules or source text of partitioned data sets. It contains logic to track libraries on shared DASD in a sysplex environment and in an SMS-managed environment. The basic function is built around zSecure Collect data for every member in every library that is monitored. All system libraries are included, although you can also exclude them. You also can specify other libraries to be monitored. zSecure Collect for z/OS examines each member of these libraries and computes a digital signature for the data in the member. This digital signature is recorded in the **CKFREEZE** data set produced by zSecure Collect for z/OS.

Library change detection is useful for internal auditors. Using the **Library Change Detection** function can be a powerful tool, especially for internal auditors. By comparing data from month to month or year to year, the auditor can identify every program that changed during that period. The programs can be either source code or load module. This function is not limited to system libraries. Application libraries also can be monitored.

The default **CKFREEZE** data sets, such as the ones you created when you build your current input sets, do not contain the necessary data for library management. You must submit another zSecure Collect for z/OS job to gather library member data. If you want to try this method, use the **Freeze** option (Option 0) in the panel that is shown in Figure 82 on page 95.

This option asks for your parameters so you can submit the necessary job. The best option for you to select is probably **System Libraries**, but you can specify any libraries that you want. You can elect to reuse your existing **CKFREEZE** data set. The new **CKFREEZE** data set has all the default data from your z/OS tables but not from VTOC, VVDS, catalogs, and so on. It also has the new library member data. This zSecure Collect for z/OS job takes a few minutes to run. It must open and read every member of the selected libraries.
Library change detection requires multiple generations of CKFREEZE data sets; you must define at least two in your input set. With some planning, GDGs are ideal for this purpose. zSecure Audit for RACF compares the signatures in the various CKFREEZE data sets and produces reports. Not all functions of library update analysis require two CKFREEZE data sets. Options 1, 3, 5, 6, 7, 8, and 9 can be used with just one or more CKFREEZE data sets. Other options are available as part of library monitoring. For example, zSecure Collect for z/OS can examine library members for specific text or hexadecimal strings anywhere in the member or for usage of specific SuperVisor Calls (SVCs). It is a good way to answer the frequently asked question of which program is using an SVC.

These options are described in the IBM Security zSecure Admin and Audit for RACF: User Reference Manual. During data collection for CKFREEZE, the hexadecimal searches can also be used to locate typical authorization code fragments. The option to identify duplicate members can be useful. It can detect library members in all the libraries that are scanned when the CKFREEZE data set was built with duplicate member names, or with duplicate contents regardless of the member name. There is no reasonable way to do either of these functions with standard z/OS utilities. Yet, detection of duplicate members is critical for effective software maintenance and for audit control.

To use the Library Change Detection functions, your input file setup might look similar to this example:

```
Menu Options Info Commands Setup StartPanel
-------------------------------------------------------------
zSecure Audit for RACF - Audit - Libraries
Option ==> ________________________________________________
0 Freeze Calculate new digital signatures
1 Lib all Overview of all libraries
2 Lib changes Overview of all libraries with changes
3 Status Show member status
4 Changes Identify members with changes
5 Scan Show members flagged by SCAN function
6 Duplicates Identify identical members
7 Application Members summarized by application
8 Prefix Members summarized by member prefix (component code)
9 PTF - ZAP Members touched by PTF or ZAP

Figure 82. Primary library update analysis panel
```

Library change detection requires multiple generations of CKFREEZE data sets; you must define at least two in your input set. With some planning, GDGs are ideal for this purpose. zSecure Audit for RACF compares the signatures in the various CKFREEZE data sets and produces reports. Not all functions of library update analysis require two CKFREEZE data sets. Options 1, 3, 5, 6, 7, 8, and 9 can be used with just one or more CKFREEZE data sets. Other options are available as part of library monitoring. For example, zSecure Collect for z/OS can examine library members for specific text or hexadecimal strings anywhere in the member or for usage of specific SuperVisor Calls (SVCs). It is a good way to answer the frequently asked question of which program is using an SVC.

These options are described in the IBM Security zSecure Admin and Audit for RACF: User Reference Manual. During data collection for CKFREEZE, the hexadecimal searches can also be used to locate typical authorization code fragments. The option to identify duplicate members can be useful. It can detect library members in all the libraries that are scanned when the CKFREEZE data set was built with duplicate member names, or with duplicate contents regardless of the member name. There is no reasonable way to do either of these functions with standard z/OS utilities. Yet, detection of duplicate members is critical for effective software maintenance and for audit control.

To use the Library Change Detection functions, your input file setup might look similar to this example:

```
Menu Options Info Commands
-------------------------------------------------------------
zSecure Audit for RACF - Setup - Input F Row 1 from 5
Command ==> ________________________________________________ Scroll ==> CSR_
(Un)select (U/S) set of input files or work with a set (B, E, R, I, D or F)
Description Complex
- CKFREEZE dd 4 Apr 2005 selected
- CKFREEZE dd 8 Apr 2005 selected
- Active primary RACF data base DEMO
- Active backup RACF data base DEMO
- Active backup RACF data base and live SMF data sets DEMO

Figure 83. Input set definition
```

This is a rather primitive input structure, but it can be used for evaluation. This section does not contain information about the SMF data set that is not required for the library functions. You would collect the OLD data first by using the Freeze function...
option to generate and submit the necessary job. Then, collect the NEW data a few days later. For long-term use, you would probably use generation data groups, such as 'HLQ.CKFREEZE(0)' and 'HLQ.CKFREEZE(-1)'.

An input set can contain any reasonable number of SMF and CKFREEZE data sets, and one RACF database. The RACF database can be the active RACF database, unloaded RACF data, a copy of a RACF database, or an active RACF database from another system. It can consist of any number of data sets.
Chapter 11. Resource-based reports for RACF resources

The Resource reports option (RE) is available from the Main menu. It provides access to display and reporting options for the following RACF resources:

- TCP/IP configuration and statistics
- UNIX file system information and audit reports
- CICS region, transaction, and program data
- IMS™ region, transaction, and program data
- DB2 region and resource data

For more information, see the following topics:

- "IP Stack reports" on page 98
- "UNIX file system reports" on page 98
- "CICS region and resource reports" on page 102
- "IMS region and resource reports" on page 105
- "DB2 region and resource reports" on page 108
- "Trust relations reports" on page 109

IP Stack reports

Use the RE.I option to select and display TCP/IP configuration and statistics data. This data is obtained from a CKFREEZE data set created by running zSecure Collect APF-authorized with the TCPIP=YES parameter. You can also report on SMF events that are related to IP configuration data by using the EV.I menu option.
When you select **RE.I** from the Main menu, the panel that is shown in Figure 85 is displayed.

When you select **RE.I** from the Main menu, the panel that is shown in Figure 85 is displayed.

![Figure 85. IP stack Selection panel](image)

From the IP stack Selection panel, you can limit the TCP/IP stack configuration data by entering selection criteria into one or more fields. When you specify selection criteria, only records that match all criteria are included in the output.

Filters can be used in some of the selection fields. For a description of the selection fields and to determine whether a field supports filters, use the field-sensitive help function (PF1).

You can also specify Output and run options on the Selection panel. You can use the run options to specify more selection criteria for specific types of IP configuration data. Use the output run options to specify report and print options.

When you select any of these options, the corresponding panels are displayed when you press Enter on the IP stack Selection panel.

If you do not select any Output or run options, the data is processed as soon as you press Enter on the IP Stack Selection panel. An overview panel is immediately displayed with a summary of the IP configuration records that match the selection criteria you specified.

See the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual* for more detailed information about these reports.

### UNIX file system reports

When you select option **RE.U**, the Resource - UNIX panel that is shown in Figure 86 opens.

![Figure 86. Resource UNIX menu](image)

File system - UNIX file system reports
Use this option to select and display UNIX file system records. A full CKFREEZE data set read is required, and the CKFREEZE data set must be made with the UNIX=Y parameter. If the zSecure Collect run was APF-authorized, more information is displayed.

When you select option F, the Resource - UNIX Selection panel that is shown in Figure 87 opens.

If the selection panel is left blank, all UNIX files are selected. You can limit the UNIX files that are selected by completing one or more fields to be used as selection criteria. Only records that match all criteria are selected. Filters can be used in some of the selection fields. You can select one of the Advanced selection criteria to specify filters to select and display UNIX files. When you select a criterion, a panel opens where you can specify the attributes in which you are interested.

Use the Output/Run options to customize settings to run the report and generate output. The settings that you specify are saved in your ISPF profile and become the default settings for all UNIX panels that provide the option.

For detailed information, see the IBM Security zSecure Admin and Audit for RACF: User Reference Manual and the online help.

After you process the CKFREEZE file by using the specified selection criteria, the UNIX summary panel opens to display the results as shown in Figure 88 on page 100.
Selecting any of the mount points listed in the summary panel that is shown in Figure 88 displays its list of UNIX files as shown in Figure 89.

You can perform the following actions from this panel:

- To browse the regular files, type B in the selection field for a file or directory entry.
- To call the UNIX System Services ISPF Shell for a file or directory, type I in the selection field for that file or directory.
- To start the z/OS UNIX Directory List Utility for a directory, type U in the selection field for the directory.

When you select to view a file from the panel that is shown in Figure 89, the panel that is shown in Figure 90 on page 101 opens. To view the contents of a file in this panel, type S in front of the Absolute pathname field.
For more detailed information about these reports, see the IBM Security zSecure Admin and Audit for RACF: User Reference Manual and the online help.

### Reports - running the predefined UNIX audit reports

For more detailed information about these reports, see the IBM Security zSecure Admin and Audit for RACF: User Reference Manual and the online help.
Use the **Reports** option to generate any of the predefined UNIX audit reports available in zSecure. When you select this option, a panel opens with a list of reports for selection. See Figure 91. For details about a specific report, position the cursor on the report selection field and press F1 to view the online help.

<table>
<thead>
<tr>
<th>Name</th>
<th>Summary</th>
<th>Records</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOUNT</td>
<td>0</td>
<td>0</td>
<td>Effective UNIX mount points</td>
</tr>
<tr>
<td>UNIXAPF</td>
<td>0</td>
<td>0</td>
<td>UNIX files with APF authorization</td>
</tr>
<tr>
<td>UNIXCTL</td>
<td>0</td>
<td>0</td>
<td>UNIX files that are program controlled</td>
</tr>
<tr>
<td>UNIXSUID</td>
<td>0</td>
<td>0</td>
<td>UNIX files with SETUID authorization</td>
</tr>
<tr>
<td>UNIXSGID</td>
<td>0</td>
<td>0</td>
<td>UNIX files with SETGID authorization</td>
</tr>
<tr>
<td>GLBNUNIX</td>
<td>0</td>
<td>0</td>
<td>UNIX files vulnerable to trojan horse &amp; back door at</td>
</tr>
<tr>
<td>UIDNOUNSR</td>
<td>0</td>
<td>0</td>
<td>UIDs not defined in the complex</td>
</tr>
<tr>
<td>GIDNOCRGP</td>
<td>0</td>
<td>0</td>
<td>GIDs not defined in the complex</td>
</tr>
<tr>
<td>SHROUIDS</td>
<td>1</td>
<td>196</td>
<td>OMVS UIDs shared between RACF users</td>
</tr>
<tr>
<td>OMWSNUID</td>
<td>1</td>
<td>21</td>
<td>RACF users with OMVS segment but no UID</td>
</tr>
<tr>
<td>SHROGIDS</td>
<td>1</td>
<td>42</td>
<td>OMVS GIDs shared between RACF groups</td>
</tr>
<tr>
<td>OMWSNGID</td>
<td>1</td>
<td>2</td>
<td>RACF groups with OMVS segment but no GID</td>
</tr>
</tbody>
</table>

**Figure 91. UNIX Reports listing**

**CICS region and resource reports**

Use the **RE.C** option on the Main menu to select and display CICS region, transaction, and program data. The report data is obtained from a CKFREEZE data set that is created by running zSecure Collect APF-authorized.

When you select **RE.C**, the panel that is shown in Figure 92 is displayed.

The **T** and **P** options are features that are provided by the zSecure Audit products.

**Figure 92. CICS Resource panel**

**CICS region reports**

In the CICS Resource panel in Figure 92, select the **R** option to display the CICS Regions selection panel in Figure 93 on page 103.

Use this panel to enter selection criteria in one or more fields to limit the CICS region configuration data. When you specify selection criteria, the output includes only those records that match all the selection criteria. Filters can be used in some of the selection fields. To find out whether a field supports filters, use the field-sensitive help function (PF1).

You can also select output and run options in the CICS Regions selection panel. Or, select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of the CICS region records that
match your selection criteria.

CICS transaction reports

In the CICS Resource panel in Figure 92 on page 102 select the T option to display the CICS Transactions selection panel in Figure 94 on page 104.

Use this panel to enter selection criteria in one or more fields to limit the CICS transaction data. When you specify selection criteria, only those records that match all criteria are included in the output. Filters can be used in some of the selection fields. To find out whether a field supports filters, use the field-sensitive help function (PF1).

To create a simulate report, use the report type option Simulate access for specified resource.

You can also select output and run options in the CICS Transactions selection panel. Additionally, you can select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of the CICS transaction records that match your selection criteria.
For detailed information, see the IBM Security zSecure Admin and Audit for RACF: User Reference Manual and the online help.

**CICS program reports**

In the CICS Resource panel in [Figure 92 on page 102](#), select the P menu option to display the CICS Programs selection panel in [Figure 95 on page 105](#).

Use this panel to enter selection criteria in one or more fields to limit CICS program data. When you specify selection criteria, only those records that match all criteria are included in the output. Filters can be used in some of the selection fields. To find out whether a field supports filters, use the field-sensitive help function (F1).

To create a simulate report, use the report type option **Simulate access for specified resource**.

You can also select output and run options in the CICS Programs selection panel. Additionally, you can select no options, and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of the CICS program records that match your selection criteria.
IMS region and resource reports

Use the **RE.M** option on the Main menu to select and display IMS region, transaction, and program data. The report data is obtained from a CKFREEZE data set created by running zSecure Collect APF-authorized.

When you select **RE.M**, the IMS Resource panel that is shown in Figure 96 is displayed.

The **T** and **P** options are features that are provided by the zSecure Audit products.

IMS region reports

In the IMS Resource panel in Figure 96 select the **R** menu option to display the IMS Regions selection panel in Figure 97 on page 106.

Use this panel to enter selection criteria in one or more fields to limit the IMS region configuration data. When you specify selection criteria, the output includes only those records that match all the selection criteria. Filters can be used in some of the selection fields. To find out whether a field supports filters, use the field-sensitive help function (F1).
You can also select output and run options in the IMS Regions selection panel. Additionally, you can select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of the IMS region records that match your selection criteria.

For detailed information, see the IBM Security zSecure Admin and Audit for RACF: User Reference Manual and the online help.

### IMS transaction reports

In the IMS Resource panel in Figure 96 on page 105, select the T menu option to display the IMS Transaction selection panel that is shown in Figure 98 on page 107.

Use this panel to enter selection criteria in one or more fields to limit IMS transaction data. When you specify selection criteria, only those records that match all criteria are included in the output. Filters can be used in some of the selection fields. To find out whether a field supports filters, use the field-sensitive help function (F1).

To create a simulate report, use the report type option **Simulate access for specified resource**.

You can also select output and run options on the IMS transaction selection panel. Additionally, you can select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of IMS transaction records that match your selection criteria.
For detailed information, see the IBM Security zSecure Admin and Audit for RACF: User Reference Manual and the online help.

**IMS PSB reports**

In the IMS Resource panel in Figure 96 on page 105, select the P menu option to display the IMS PSB selection panel in Figure 99 on page 108.

Use this panel to enter selection criteria in one or more fields to limit IMS program specification block data. When you specify selection criteria, only those records that match all criteria are included in the output. Filters can be used in some of the selection fields. To find out whether a field supports filters, use the field-sensitive help function (F1).

To create a simulate report, use the report type option **Simulate access for specified resource**.

You can also select output and run options on the IMS PSB selection panel. Additionally, you can select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of IMS PSB records that match your selection criteria.
For detailed information, see the IBM Security zSecure Admin and Audit for RACF: User Reference Manual and the online help.

DB2 region and resource reports

Use the RE.D option on the Main menu to select and display DB2 region, transaction, and program data.

When you select RE.D, the DB2 region and resource reports panel shown in Figure 100 is displayed.

Note: In zSecure Admin, only the Regions report is available.

When you select the option of your choice, the corresponding selection panel is displayed. For example, the DB2 regions selection panel.
Use this selection panel to enter your selection criteria in one or more fields to limit the data. When you specify selection criteria, the output includes only those records that match all the selection criteria. Filters can be used in some of the selection fields. To find out whether a field supports filters, use the field-sensitive help function (PF1).

You can also select output and run options in the DB2 regions selection panel. Additionally, you can select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of the records that match your selection criteria.

For detailed information, see the and the online help and the IBM Security zSecure Admin and Audit for RACF: User Reference Manual.

**Trust relations reports**

Use the RE.T option on the Main menu to select and display trust relations.

When you select RE.T, the Trusted panel shown in Figure 102 on page 110 is displayed.

Use the panel to enter selection criteria for trust relations and to limit record output. You can enter selection criteria in one or more fields. The output includes only those records that match all of the selection criteria. If the selection panel is left blank, all records are selected. Filters can be used in some selection fields. To find out if a field supports filters, use the field-sensitive help function (PF1).

You can also select output and run options in the trusted relations selection panel, or select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of the trust relations records that match your selection criteria.
Menu Options Info Commands Setup Startpanel

---------------------------------------------------------------------------------

Command ==> __________________________________________________________________

zSecure Suite - Trusted

Show trust relations that fit all of the following criteria:
Complex ........ ________ (complex or filter)
Trust level ........ __ __ (operator: < <= > >= = <> ^= , number 1-10)

Selection criteria
- Select/exclude users and access types
- Select resources

Output/run options
- 1. Summarize by resource 2. Summarize by user
- Show differences
- Print format Customize title Send as e-mail
- Background run

Figure 102. Trusted panel

For detailed information, see the IBM Security zSecure Admin and Audit for RACF: User Reference Manual and the online help.
Chapter 12. CARLa commands

zSecure Admin and Audit for RACF ISPF panels generate commands that are sent to the products for execution. These commands are in the CARLa Auditing and Reporting Language (CARLa), a useful tool for systems programmers. This process is not apparent to interactive users, but becomes important if you want to use product functions in batch mode. In general, the same CARLa commands can be used in either interactive mode or in batch mode. For example, you can use one of the primary options, the `CO.C` option to specify CARLa commands directly.

Tip: Instead of typing `=CO.C`, you can also type the primary command CARLA at the command prompt on a panel to specify CARLa commands.

Many CARLa samples are provided with the products. When you have time, browse them at random and run the code samples that are interesting to you. You can also look at the `CKASINDEX` index member, which contains a list and brief description of all members in the CARLa library. You can also browse the `SCKRCARL` library, which contains interactive ISPF and batch reports that you can use or tailor for your own needs. For more detailed information about CARLa and the `SCKRCARL` library, see the IBM Security zSecure Admin and Audit for RACF: User Reference Manual.

Tip: To browse the `SCKRCARL` library, you can use the following steps: "Browsing the SCKRCARL library" on page 112

In addition to the manuals, IBM offers:


• Hands-on exercises for understanding the basics of the zSecure CARLa Auditing and Reporting Language on developerWorks®; search developerWorks® for zSecure CARLa training at [http://www.ibm.com/developerworks/wikis/display/tivolidoccentral/Home](http://www.ibm.com/developerworks/wikis/display/tivolidoccentral/Home)

• For links to this forum and other resources, see the Community and Support tab in the zSecure Information Center at [http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.htm](http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.htm)

You can use CARLa to define and format custom reports. Use any fields that are known to RACF and SMF, with headings and line formats that are specified by you. Typical use involves identifying a pre-built display or report that is almost what you need. You can also use CARLa to capture and save the CARLa used to generate the Display/Report from the Results panel. You can modify it to produce exactly what you need. zSecure Admin and Audit for RACF provides a whole library of sample CARLa material, the `SCKRCARL` library. You can add new members to this library, or create your own library. Do not alter the existing members of the library because the interactive functions of the products use these members.

To run one of the members of the `SCKRCARL` library, complete the following steps: "Running a member of the SCKRCARL library" on page 112

© Copyright IBM Corp. 1989, 2013
To customize the CARLa program, complete the following steps: “Customizing the CARLa program” on page 115

To create a sample CARLa program, complete the following steps: “Creating a sample CARLa program” on page 116

To save your CARLa program for later use, you can copy it into your own private data set.

To copy your program, type the command C9999 over the line number field of the first CARLa line. Then, enter CREATE in the command area. You now use the normal ISPF Edit function to create (or replace) members in a PDS.

Whenever you want to rerun your saved CARLa program, complete the following steps: “Running a saved CARLa program” on page 116

Browsing the SCKRCARL library

About this task

You can browse the SCKRCARL library to view interactive ISPF and batch reports. Use and tailor these reports according to the needs of your organization.

Procedure

1. Issue the TSO ISRDDN command from within the product under ISPF.
2. Type F SCKRCARL to look for the active SCKRCARL library.
3. Use the B(Browse) function to open the SCKRCARL library.
   The CKA$INDEX member at the top lists the available members and their functions.

Running a member of the SCKRCARL library

About this task

In ISPF, you can view, edit, and run members from the current SCKRCARL command library. It is accessed through the DD-name CKRCARLA.

Procedure

1. Select option CO (Command) from the Main menu. Press Enter to open the panel that is shown in Figure 103 on page 113
   This panel is used to perform library commands.
2. Select option 2 (Members) and then press Enter to select a member or find the name of the member you want to execute in one of the user reference manuals. For this example, use member CKRLMTX3.

3. If you are using the Members function, find the member name (CKRLMTX3 or the member name you chose from the reference manual) in the Member list, or type the member name in the Member name field in the Commands panel.

4. From the members list, issue the E line command in front of the member you want to use (for example, CKRLMTX3). From the Commands panel, type option 3 (Edit) and press Enter.

   A panel opens showing the selected CARLa member as shown in Figure 104 on page 114.
Update the data sets that contain the software only during installation and maintenance. If you need customized members, store them in a data set of your own. Use the configuration parameters WPREFIX or UPREFIX to use these data sets.

What to do next

The selected CARLa program shows a matrix of the access that is granted on one or more profiles. It needs some customization for you to select the profiles you want to be reported on. To avoid changing the original member, the procedure in "Customizing the CARLa program" on page 115 shows you how to work with a temporary copy.
Customizing the CARLa program

Before you begin

Complete "Running a member of the SCKRCARL library" on page 112.

Procedure

1. Issue the CANCEL command to be sure that you leave the edit session without making any accidental changes to the member.
2. Enter option 4 (Run). Because the customization is not yet done, this option results in a syntax error about an incorrect LIKELIST.
3. Press PF3 to open the Results panel. Enter an E before the Command line and press Enter. You are now editing a temporary copy of the CARLa program.
4. Customize the program.
   The customization is documented in the Notes section of the header. This program was created to be included from other programs. To include the program, write a selection newlist (lines 15 - 17), and include the program directly behind it (line 18).
   You can achieve the same result by adding the selection newlist to the start of the CARLa program:
5. Copy lines 15 - 17 directly after line 23. (Remove the * to uncomment them.)
6. Change the class (c=data set) and HLQ (qual=sys1) specifications to match the profiles that you want to see.
7. Type Go or Run in the Command line to run this program. A report similar to the one shown in Figure 105 opens.

What to do next

Instead of running one of the existing samples, you can program your own CARLa program. In “Creating a sample CARLa program” on page 116, run a small CARLa program to see what CARLa programming can mean to you.
Creating a sample CARLa program

Before you begin

Read “Running a member of the SCKRCARL library” on page 112 and “Customizing the CARLa program” on page 115.

Procedure

To create a sample CARLa program, complete the following steps:

1. Select option CO (Command) from the Main menu to open the panel that is shown in Figure 103 on page 113 so that you can run library commands.
2. Select option C (Command) to open the PDF editor.
3. In the editor workspace, type the following CARLa statements, changing c#mb to some RACF group in your system that owns user IDs.

```
newlist type=racf file=ckrcmd nopage
  select class=user owner=c#mb segment=base
  list 'alu' key(8) 'owner(newowner)'
```

Figure 106. CARLa example program

This small CARLa program generates RACF commands to change the owner. All user profiles that are currently owned by c#mb are selected and the owner field is changed into newowner. The output (RACF commands) is written in the CKRCMD file and can be processed by the RUN command. See “Results panel” on page 70.

The output is similar to the output shown in Figure 107.

```
/* CKRCMD file CKR1CMD complex DEMO NJE JES2DEMO generated 27
   alu C#MBHEN owner(newowner)
   alu C#MBERG owner(newowner)
   alu C#MBJVO owner(newowner)
```

Figure 107. CARLa example program output

Running a saved CARLa program

Before you begin

Read “Creating a sample CARLa program.”

Procedure

To run your saved CARLa program, follow these steps:

1. Type 0 from the Main menu and press Enter.
2. Type 1 (Libraries) from the Commands panel and press Enter.
3. Type I (insert) line command in any detail line and press Enter to insert a line.
4. Type the name of your private library. Use quotation marks if necessary. Press Enter.
5. Select the library with the S line command and press Enter.
6. Press PF3 to return to the Commands panel.

The name of your library is displayed in the Current library field.
7. Type the member name of the CARLa program in the **Member name** field.
8. Select option 4 (Run).
Chapter 13. Typical administration and audit tasks

The following topics describe how to perform typical administration and audit tasks in Security zSecure Admin and Audit for RACF.

- “Removing a user”
- “Displaying which data sets a user can access”
- “Load library audit”
- “Print data on display panels” on page 120
- “Find profiles based on search criteria” on page 120
- “Protect All Verify function” on page 120
- “Command function” on page 120

Removing a user

About this task

If you want to remove the RACF access credentials for a user and do not know the user ID, you can use the zSecure Audit for RACF RA.U function. Enter a name search pattern to locate the user ID and determine which data sets the user can access. Then, you can select the user profile for removal.

Procedure

1. Enter RA.U in the Command line to open the RACF User panel.
2. In the Programmer Name field, type the user name or name pattern to display all user profiles that match the name somewhere in the Programmer Name field.
3. Press Enter to display the results
4. To remove the user from RACF, type D in front of the user profile and then press Enter.

Displaying which data sets a user can access

Procedure

To list all data sets that a particular user can access, use the RACF Report Permit/Scope function (option RA.3.4).

Load library audit

The Audit Library functions, option AU.L in zSecure Audit for RACF, can easily detect situations that are difficult to detect with standard z/OS or RACF tools.

These situations, in both load libraries and source libraries, include:

- Whether the load libraries are clean, especially the system and APF libraries.
- Whether a module is present multiple times, under different names and perhaps under different owner profiles.
- Whether the same module is present in more than one library.
Note: It would cause serious problems if one copy is obsolete, but is unknowingly called by some jobs due to the library search order.

**Print data on display panels**

While you are examining the output of a Display function, you might want to print the data. Use the `PRT` command. Output goes to the ISPF LIST data set. For more complex reports, use the `RESULTS` command to review all the files that are produced by the last function. You can also print from this panel.

**Find profiles based on search criteria**

The `Match` function can be exceptionally useful. This function finds all profiles that cover a specified data set or sets, or general resources. You can find this function in the following panels:

- Data set profiles: option `RA.D` data set
- General Resource profiles: option `RA.R` Resource
- RACF Report match: option `RA.3.7`

For `RA.D` and `RA.R`:

- **3 Match** treats the profile field as a resource name and selects the best profile that matches the resource name. See the `BESTMATCH` parameter in the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.
- **4 Any match** treats the profile field as a resource name and selects all profiles that can match the resource name. See the `MATCH` parameter in the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.

`RA.3.7` works like **Any match**: The profile used by RACF is in the first line. The other profiles are used if the first profile is removed. Poor planning or administration can result in several profiles with different access lists and UACC values covering a data set.

**Protect All Verify function**

You might be thinking about going to a Protect All environment. Most z/OS installations do so, although there can be much work involved. Try the Verify function of Protect All. If you use SMS, HSM, or ABR, you might exclude the volume `MIGRAT` on the submenu of the `Protect All` function. This action can greatly reduce the number of unwanted messages. Especially in a RACF environment without `PROTECT ALL`, this `Verify` function can be helpful. It outlines the work to be done in going to Protect All and provides an inventory of all data sets that do not have RACF protection.

**Command function**

Try the `Command` function, which is option `CO` on the primary panel. See [Chapter 12, “CARLa commands,” on page 111](#).
Appendix. Frequently asked questions

This section provides a list of frequently asked questions along with detailed answers.

Table 12. Frequently Asked Questions

Q: Why is the Main panel empty?
A: You need READ access to the CKR.** profile in the XFACILIT class. CKR.** profiles can allow or prohibit the use of functions.

Q: I am still not sure which functions are for zSecure Admin and which are for zSecure Audit for RACF. How can I separate them?
A: You can check the IBM Security zSecure Admin and Audit for RACF: User Reference Manual. With every function, the manual shows a check box indicating which product it supports. You can also add LIMIT FOCUS=AUDITRACF to the preamble SETUP PREAMBLE (SE.3) to limit the usable function to those functions in the zSecure Audit.

Q: How can I generate the DEFINE ALIAS as part of the COPY USER action?
A: The catalog information is from the CKFREEZE data set. So you must include a CKFREEZE data set in the set of input files that you use. To create a CKFREEZE data set, use the option SETUP NEWFILES from the panels to generate the JCL. Save this JCL and run it early every morning by using OPC/A or a similar product. The CKFREEZE data set can be large, so use SYSIN parameters to reduce its size. First, try creating a large CKFREEZE, running it with APF, and specifying no parameters.

If running zSecure Admin with this CKFREEZE setting is too slow, add parameters: VTOC=NO,CAT=MCAT,BCD=NO,MCD=NO,TMC=NO,RMM=NO,UNIX=NO. You still need the bigger CKFREEZE if you want to delete users, including their data sets.

You can also enter the line command MT (manage TSO) in front of a User profile in the RA,U option. You can then define the alias and the ISPF profile data set for an existing user. With this alternative, however, you must know the name of the catalog to which you want to add the user's alias.

Q: Can I collect information of unloaded RACF and CKFREEZE files on different systems and send this information to one system for display and analysis?
A: Yes, if all systems are licensed. This way is a typical way to use Security zSecure Admin and Audit for RACF.

Q: The output from my L line command does not match the information that is reported by zSecure Admin and zSecure Audit for RACF. What is wrong?
A: Check the input RACF data source. You are probably reporting from a RACF unload. Whereas, the L line command always shows the information from the active RACF database.

Q: How do I handle a shared JES2 spool environment with one RACF database and several z/OS images?
Table 12. Frequently Asked Questions (continued)

A: Run the RACF unload one time from any system unless you want to work with live RACF data. Run multiple zSecure Collect jobs, one on each system. You can use the `SHARED=NO` parameter with the second or more zSecure Collect for z/OS job. Using the `SHARED=NO` parameter reduces the size of the resulting `CKFREEZE` data sets. You can do this action only if your UCBs are properly defined with `SHARED` options to exactly reflect the sharing environment. Otherwise, zSecure Collect for z/OS processes everything. Create an INPUT SET that has these multiple `CKFREEZE` data sets defined.

Q: When do I use my live RACF database with zSecure Admin and zSecure Audit for RACF? When do I use unloaded data and when do I use an old database copy?

A: Use the live RACF database for simple *ad hoc* inquiries and day-to-day routine RACF administration. Use an unloaded copy of the RACF database when you intend to do extensive analysis work and you have no immediate intention of changing RACF data. When you are planning to use the re-create function, be sure to run from an old database copy because an unload database does not contain passwords. If you are working with RACF data from another system, this data is unloaded unless the RACF database for the other system is on shared DASD and is accessed directly as a normal data set. As an oversimplified statement, an *administrator* typically works with the live RACF database, while an *auditor* typically works with an unloaded copy.

Q: I produced a report that contains double lines for all reported profiles. What can cause this problem?

A: There are two possibilities that can cause this problem. If you created this overview with the panels, then the double lines might be caused by selecting two RACF data sources in the `SETUP` application. When you are using CARLa, this same problem can be caused by forgetting to specify the keyword `SEGMENT=BASE` in the `SELECT` statement.

Q: I used the `SETUP INPUT` options to define my input sets. The next time that I used zSecure Admin and zSecure Audit for RACF, my setup values were not saved. Why?

A: You might have used a different TSO user ID the second time. The setup information is saved in your ISPF profile, and each TSO user ID has its own ISPF profile data set. Also, there is a `SETUP` option to use the input files you last used. Look at the `SETUP RUN` to determine the setting of this option.

Q: Security zSecure Admin and Audit for RACF inspects many z/OS controls for various reports. When do the products obtain these controls from z/OS storage and when do you use a `CKFREEZE` data set?

A: For full checking, Security zSecure Admin and Audit for RACF uses z/OS control blocks that are copied into the `CKFREEZE` data set. While this problem is more complex than using in-storage z/OS data, it produces much more consistent results. The results are meaningful for the time at which the `CKFREEZE` data was collected. For this reason, you might sometimes want to collect `CKFREEZE` data when your system is fully loaded and most active. It also means that you can do studies on remote z/OS systems. Use a `CKFREEZE` file and RACF unloaded data that was created on the remote system.

Q: I prefer to use an unloaded RACF database for my analysis work. When I find something that must be corrected, I typically use the RACF commands that are generated by zSecure Admin and zSecure Audit for RACF. I sometimes edit them to correct the problem. However, my unloaded RACF database represents historical data. How do I know whether the same problem still exists in the live RACF database?
Table 12. Frequently Asked Questions  (continued)

A: Before you submit any significant change to RACF, switch to the live RACF database by using a different input set in the Setup panels. Repeat the display that detected the problem. If the problem still exists, then run the RACF changes.

Q: Some panels, such as the AUDIT STATUS panel, differentiate between full CKFREEZE data sets and some other type of CKFREEZE data sets. What is this?

A: Using the instructions in this evaluation guide, when you defined new input files and ran the Refresh job, you created a full CKFREEZE data set. In large or widely distributed installations, a CKFREEZE data set can be large. You might want to save multiple CKFREEZE data sets for audit and comparison purposes. There are options in zSecure Collect for z/OS to gather only part of the potential CKFREEZE data. Multiple CKFREEZE data sets are useful. For example, if you use the freeze functions to detect changes in various libraries, or if your auditors want system snapshots at certain defined times.

Q: I want to clone a user by using the RACF/MASS UPDATE/COPY USER function, but the target, which is a new user, is already defined. How is this problem handled?

A: Assuming that you want to keep some of the permissions of the existing target user, use the Copy function and type / before Generate RACF commands when the target user exists. This action leaves existing permissions of the target, provided they do not conflict with authorities of the source user. If a conflict occurs, then the final authority rests with the source or target user, depending on the exact commands (add versus alter). The target user might have some of its existing authority levels reduced because the source user had these lower levels.

Q: I get message CKR0536 when I attempt to copy to an existing user ID.

A: If your intent is to have the set of commands as a basis to start editing, then you can suppress the message by putting a / before Generate RACF commands when the target user exists. The standard way to merge user attributes is to use MERGE.

Q: I must do daily security administration. What RACF data source do I use?

A: For daily security administration, use an up-to-date RACF database. This database can be the active primary RACF database or the active backup RACF database. Changes to the active primary database are immediately replicated to the active backup RACF database. Because the active backup database is not used for access verification processing, it is a good practice to use it as the input data source. This practice does not degrade the performance of the RACF database when you run the access verification process for the other users of the system while you run reports.
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.
Index

Numerics

3270 format 7

A
Access check
detail panel 26
entry panel 26
Access command 26
access control list
commands 23
display 22
display settings 25
effective 23
group information, display 62
sort order 62
user information, display 62
Verify functions, run 73
view options 62
access rights 27
accessibility viii
ACL
See access control list
ACL commands
ACL EFFECTIVE 23
ACL EFFECTIVE (F) 23
ACL EXPLODE 25
ACL NOSCOPE 23
ACL RESOLVE 25
ACL RESOLVE (R) 23
ACL SCOPE 23
ACL SORT ACCESS 23
Add / copy connect panel 17
Add connect panel 17
address space name 62
administration functions
distributed 49
overview 49
administration tasks, typical 119
allocation parameters 56
APF
authorized functions 5
defined data sets 93
libraries, authorized 93
application segments 14
Archive output to a data set panel 71
attributes
AUDITOR 43
ERASE ON SCRATCH (EOS) 21
OPERATIONS 12
SPECIAL 12
UNIVERSAL 16
AU.R 83
AU.S function 45, 79
Audit
Library function 119
report overview 79
status panel 79
status RACFCLAS report 79

Audit (continued)
status SETROPTS report 79
audit tasks, typical 119
AUDITOR attribute 43

B
basic operations 7

C
CARLa
access matrix 115
auditing 2
Auditing and Reporting Language 1
data source 3
language, purpose of 2
reporting 2
sample reports 2
CARLa commands
batch mode 111
Command 120
overview 2, 111
samples 111
CARLa program
copy 111
create 116
customize 115
element 116
run saved 116
certificate templates, create 27
Change tracking function 93
CICS
profiles 38
program report 104
Programs panel 104
region report 102
region, transaction, and program data
report 97, 102
Regions panel 102
Resource panel 102
transaction report 103
Transctions panel 103
CKASINDX index member 111, 112
CKFREEZE
data sets 5, 55, 94, 121
data sources 3
data, add from file 56
files, collect information 121
user deleted 41
CKG scope 50
CKGRACF
authorization 37
CKRCARLa, differences from 50
commands 8, 52
functions 50
CKR command 7
CKR** profile 121
CKR.OPTION profiles 53
CKR.READALL profile 49

CKR0536 message 121
CKRCARLa
CKGRACF, differences from 50
commands sent to 1
language 2
CKRCMD files 70, 75, 116
CKRLMTX3 member 112
CO option 112
CO.C option 111
Collections, SETUP 59
Command function 120
commands
Access 26
ACL
See ACL commands
C 17
CARLa 2
See CARLa commands
CKGRACF 8, 52
CKR 7
CO 17
D 17
execution control 63
find ‘verify’ 73
find ‘verify’ 75
FORALL 8, 9
L 121
line 9
line, specifying 66
LIST 23
MT (manage TSO) 121
PE (permit) 27
PERMIT 27, 50
Permmit Delete 27
PRT 23, 70, 120
RACDCERT 30
RACF
See RACF commands
RDEFINE 50
RESULTS 70, 120
routing settings 63
S 12, 21
SE 14
SET 25
SETROPTS 45
SETUP FILES C 12
SETUP FILES S 12
SETUP VIEW 25, 49
SIMULATE RESTRICT 49
sort class 79
sort pos 79
TSO ISRDDN 112
UACC(NONE) 49
viewing 66
W 70, 71
Commands (CO) used to run library
commands panel 112
Common Address Space Work 87
Compare connects matrix panel 34
Compare permits detail panel 34
Compare users panel 34
IRRADU00 SMF 3
ISPF
  CARLa commands 2
  Command Shell 7
display colors, changing 9
  interface, using 8
  LIST data set 23, 120
  reports 111, 112
  ISPF format 7
J
  JES2 shared spool environment 121
  JOB statement 58
  JOBLIB statement 58
K
  key rings 30
L
  L command 121
  libraries
    APF 119
    auditing 119
    change detection 94
    load 119
    SCKRCARL
      See SCKRCARL library
    source 119
    systems 119
  Libraries panel 94
  Library Change Detection function 94
  LIMIT FOCUS=AUDITRACF 121
  line commands 9, 66
  load libraries, audit 119
  logon
    region size 7
    TSO parameters 7
M
  Mass update panel 38
  Mass Update panel 39
  Match function 120
  MT (manage TSO) command 121
  multisystem support
    remote data 5
    route commands to remote systems 5
N
  New files panel 56
O
  online
    publications v
    terminology v
  OPERATIONS attribute 12
operators (continued)
  dates 14
  options
    CO 112
    CO.C 111
    Confirm 62
    EVI 97
    P 104, 106, 107
    R 102
    RA.4.4 41
    RACDCERT (RA.5) 30
    RE.C 102
    RE.I 97
    RE.M 105
    RE.U 98
    REPORTS (RA.3) 34
    Resource report 97
    SE 25
    SE.9 27
    SE.B 59
    SE.R 7
    set up 55
    SETUP NEWFILES 121
    T 103
    View 62
    Output panel 62
    Overtype function 65
P
  P option 104, 107
  panel help 9
  panels 90
    Access check detail 26
    Access check entry 26
    Add / copy connect 17
    Add connect 17
    Archive output to a data set 71
    Audit status 79
    CICS Programs 104
    CICS Regions 102
    CICS Resource 102
    CICS Transactions 103
    Commands (CO) used to run library commands 112
    Compare connects matrix 34
    Compare permits detail 34
    Compare users 34
    Confirm 63
    Data set Selection 18, 21
    define data set definition 56
    DIGTCERT selection 30
    Display Selection 45
    Email specification 72
    event log record detail 92
    Events User Selection 92
    Group selection 16
    Group Selection 15
    IMS PSB 107
    IMS Regions 105
    IMS Resource 105
    IMS Transactions selection 106
    Input file selection 58
    Input set definition 94
    IP stack Selection 97
    Libraries 94
    Mass update 38
panels (continued)
  Mass Update 39
  New files 56
  Output 62
  Profiles Non-redundant 41
  Quick Administration 49, 50
  RACF class settings 45
  RACF events 90
  Reports - REDUNDANT 41
  Resource DB2 108
  Resource Trusted 109
  Resource UNIX selection 98
  Results 70
  scrolling 55
  SETROPTS settings - audit concerns 79
  SETROPTS system settings 45
  Setup 25, 55, 62, 88
  Setup output definition 62
  Setup View 25
  Single panel Helpdesk 52
  SMF selection 30
  SMF selection criteria 90
  Tailored Helpdesk 53
  Typical allocation 56
  User Attributes 12
  User multiple copy 39
  User Selection 12
  Verify selection 73
panelsScope report
  Scope report 69
  Scope report Results 69
parameters
  allocation 56
  DCB 56
  INSTDATA 62
  Setup 62
  partitioned data set 71
  Partitioned Data Set (PDS) directories 5
passwords
  default 52
  enable 52
  reset 52
  set 52
PDS
  See Partitioned Data Set
  PERMIT command 27, 50
  Permit Delete command 27
  problem-determination ix
  problems and solutions 121
  product
    manage 1
    start 7
profiles
  CICS 38
  CRK.** 121
  CRK.OPTION 53
  CRK.READALL 49
  compare 41
  data, change 37
  filters 8
  find 120
  merge 41
  PROGRAM 73
  querying 15
  RACF
    See RACF profiles
profiles (continued)
  RACF databases 9
  RACF, maintaining 8
  reports, creating from remote data 5
  search criteria 120
  user access 26
  warning mode list 21
  XFACTILIT 49, 53
  XFACTILIT class 50
Profiles Non-redundant panel 41
  profiles, data set
    access rights administration 27
    discrete 21
    display 18
    inquires 18
    list 22
    mass updates 38
    redundant 41
  profiles, group
    connected users, maximum 16
    searching 15
  profiles, user
    application segments, show 14
    cloning 39
    displaying 9
    RACF management selection criteria
      See user profile
    recreate 41
    system-wide authority 12
Program Access to data sets (PADS) 49
  PROGRAM profiles 73
Protect All environment 120
  PROTECT ALL environment 73
Protect All function 120
Protect All Verify function 120
  PRT command 70, 120
publications
  accessing online v
  list of for this product v
R
  questions, frequently asked 121
  Quick Administration panel
    option X, opening with 50
    overview 49
  RA.Q, opening with 50
  stand-alone, opening 50
RACF (continued)
  Class Descriptor Table 79
  class settings panel 45
  command generation 1
  commands, routing 5
  data from zSecure 3
  data sources 3, 63
  data, change 37
  databases 3, 5, 8
  definitions 93
  EGN mode 14
  events panel 90
  filters 8
  input data sets 88
  integrity analysis 73
  mass updates to 38
  monitoring 1
  natural scope 49
  processing 3
  profiles maintenance 8
  protection 120
  Remote Sharing Facility (RRSF) services 5
  reports on data 69
  security analysis 73
  start products 7
  unloaded files, collect information 121
  variables 39
  RACF access permissions
    exploded list 23
    multiple permissions resolution 23
    resolved list 23
    sexploed list 23
  RACF commands
    confirming 37
    database, changing 37
    generating 37
    mass updates, using 38
    values, changing and verifying 65
  RACF data sets
    file refresh 58
    file reload 58
    profile, recreate from 41
    record types 87
  RACF databases
    alterations 63
    change authority 37
    commands that change 37
    data input sets 58
    data, add from 56
    group profiles
      querying 15
      searching 15
      live, when to use 121
      maximum size 16
      profile, compare 41
      profile, merge 41
      profile, recreate from 41
      redundant profile management 41
      report for managing 43
      unloaded 14, 55
      user profiles, displaying 9
      RACF profiles
        date sets, corresponding 73
        maximum size 16
        obsolete, identifying 73
    RACF profiles
    user access to 26
    Verify functions 73
  RACF/MASS UPDATE/COPY USER function 121
  RACFCLA report 45
  RACFD2 region and resource data
    reports 97
  RACFVARS 39
  RDEFINE command 50
  RE.C option 102
  RE.I option 97
  REM option 105
  RE.U option 98
  remote systems communication 5
  REPORT file 70
  Report Permit/Scope function 119
  REPORT WRITER 3
  reports
    archiving 71
    AUR 84
    Audit report overview 79
    Audit status RACFCLA 79
    Audit status SETROPTS 79
    CARLA access matrix 115
    categories 79
    CICS program 104
    CICS region 102
    CICS region, transaction, and program
      data 97
    CICS region, transaction, and program
      data report 102
    CICS transaction 103
    Compare users 34
    custom 2, 111
    double line problem 121
    email 72
    generating 69
    Group tree 43
    IMS PSB 107
    IMS region 105
    IMS region, transaction, and program
      data 97
    IMS transaction 106
    IP stack configuration 97
    ISPF 111
    profiles 5
    RACF resources 97
    RACFCLA 45
    remote data, creating from 5
    Results panel 69, 70
    samples in CARLa library 2
    SCKRCARL library 112
    Scope report panel 69
    SETROPTS 45
    SETROPTS audit concerns 79
    settings 5
    SMF 90
    standard 2
    TCP/IP configuration and
      statistics 97
    UNIX audit 98
    UNIX file system 97, 98
    UNIX file system information and
      audit reports 98
    UNIX summary 98
  Reports - REDUNDANT panel 41
z/OS
  change tracking 1
  control block data 5
  integrity analysis 73
  integrity checking 1
  library change detection 1
  monitoring 1
  security analysis 73
zSecure Admin
  functions 1
  licenses 1
zSecure Audit
  functions
  licenses 1
zSecure Suite
  Main Menu 7

134  Getting Started