Security zSecure Audit for ACF2
Version 2.1.0

Getting Started
Security zSecure Audit for ACF2
Version 2.1.0

Getting Started
## Contents

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

### Chapter 1. Overview
- Data sources ..................................................... 2
- Remote data ..................................................... 3
- ACF2 terminology used in this guide ........................... 3
- ACF2 scoping ................................................... 5
  - Sample scope records ....................................... 6
  - Scoping by default .......................................... 7
  - LIST command .............................................. 7
  - SELECT command .......................................... 8
- Screen navigation ............................................. 8
  - Opening the Main menu ................................... 10
  - Trying out the options .................................... 10
  - Viewing the Rules information ............................ 10
  - Viewing Audit information ................................ 10
  - Masking characters ........................................ 11
  - Date fields .................................................. 11
  - Summary of navigation characters ....................... 11

### Chapter 2. Logon ID tasks
- Accessing the Logon ID functions ............................ 13
- Displaying your Logon ID ..................................... 14
- Displaying Logon IDs using SELECT .......................... 16
- Interpreting Logon ID settings ................................ 18
- Displaying logonids using LIST .............................. 19
- Displaying Logon IDs using a mask ............................ 20
- Displaying logon IDs with matching UID string ............. 21
- Listing logon IDs with special privileges ...................... 22
  - Example: Find all logon IDs with `SECURITY` and `ACCOUNT` and not `NON-CNCL` .............................................. 24
  - Displaying all logon IDs with the same user name ............ 25

### Chapter 3. Rule analysis
- Data set rules .................................................. 27
- Resource rules ................................................ 27
- Viewing data set rules ....................................... 27
  - Viewing by rule set ....................................... 29
- Displaying data set rules using LIST ......................... 30
- Displaying data set rules using SELECT ....................... 32
- Audit concerns ................................................ 38
  - Suggestions for rule reviews ................................ 38
  - Displaying who last stored a rule ........................... 39
  - Listing rule lines for a specific data set ................... 40
  - Analyzing data set access ................................... 42
  - Listing data set rule lines specific to a uid string ....... 43
  - Displaying NEXTKEYs in data set rules .................... 45
  - Specifying additional selection criteria .................... 46
  - Data set rule structure and NEXTKEYs ..................... 48
  - Displaying rules lines in expanded NEXTKEY format ....... 49
  - Using the expanded NEXTKEYs function .................... 50
  - Reviewing the expanded NEXTKEY rule lines for each X line ...... 54
  - Viewing individual data set rule lines ..................... 56
  - Viewing a resource rule .................................... 58

### Chapter 4. Infostorage records
- Infostorage record types and attributes ..................... 61
- Viewing scope records ....................................... 62
  - Viewing an individual Scope record ....................... 64
- Viewing cross-reference records ............................ 65
  - Viewing an individual cross-reference group record .... 66

### Chapter 5. SETUP functions for data management
- Inputting data ................................................ 69
- Inputting new files .......................................... 69
- Refreshing and loading files ................................ 71
- Selecting the input set ...................................... 72
- Specifying collections of input sets ........................ 73

### Chapter 6. Security control analysis
- Audit concerns ................................................ 75
  - Selecting the Audit function ................................ 75
  - Viewing audit concerns detected by zSecure ............... 76
  - Audit for ACF2 ............................................. 76
  - Reviewing audit concerns overview by priority .......... 77
  - Audit concern overview by priority ....................... 77
  - Viewing GSO system settings ................................ 79
  - Global System Options ..................................... 82
  - GSO Maintenance record .................................... 84
  - GSO PDS record ........................................... 84
  - Auditing user concerns .................................... 85
  - Reviewing the Overview report selection .................. 86
  - User audit concerns by priority ......................... 87
  - Auditing password concerns ............................... 88
  - Listing logon IDs without a password interval .......... 89
  - Viewing information about the Logon ID ................. 90
  - Creating audit reports for resource concerns .......... 92
  - Sensitive Data report ..................................... 93
  - Authorized Programs report ................................ 93
  - Started Task Protection report ............................ 93
  - Globally Writable Files report ......................... 93
  - Sensitive Data Trustees report ............................ 93
  - Displaying the sensitive data trustees report .......... 94
  - Viewing more detail ...................................... 94
  - Selecting an entry ......................................... 96
  - Viewing similar information for rules .................... 97

© Copyright IBM Corp. 1998, 2013
<table>
<thead>
<tr>
<th>Chapter 7. Rule-based compliance evaluation</th>
<th>99</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting</td>
<td>100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 8. Resource-based reports for ACF2 resources</th>
<th>103</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP stack reports</td>
<td>103</td>
</tr>
<tr>
<td>UNIX file system reports</td>
<td>104</td>
</tr>
<tr>
<td>CICS region and resource reports</td>
<td>108</td>
</tr>
<tr>
<td>IMS region and resource reports</td>
<td>109</td>
</tr>
<tr>
<td>DB2 region and resource reports</td>
<td>110</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 9. Event reporting</th>
<th>113</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMF data sources for input sets</td>
<td>113</td>
</tr>
<tr>
<td>Specifying a data set with SMF data</td>
<td>114</td>
</tr>
<tr>
<td>Reviewing violation events</td>
<td>116</td>
</tr>
<tr>
<td>Viewing resource access violations in the Display Selection panel</td>
<td>118</td>
</tr>
<tr>
<td>Viewing ACF2 database maintenance activity</td>
<td>119</td>
</tr>
<tr>
<td>Viewing user events</td>
<td>121</td>
</tr>
</tbody>
</table>

Selecting a logon ID for viewing user events . . . 122

<table>
<thead>
<tr>
<th>Chapter 10. Report generation</th>
<th>125</th>
</tr>
</thead>
<tbody>
<tr>
<td>Results panel</td>
<td>125</td>
</tr>
<tr>
<td>Creating an audit report</td>
<td>125</td>
</tr>
<tr>
<td>Archiving reports</td>
<td>127</td>
</tr>
<tr>
<td>Printing reports</td>
<td>128</td>
</tr>
</tbody>
</table>

| Appendix A. Frequently asked questions | 131 |

| Appendix B. zSecure Collect memory requirements | 133 |

<table>
<thead>
<tr>
<th>Notices</th>
<th>135</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trademarks</td>
<td>137</td>
</tr>
</tbody>
</table>

| Index | 139 |
About this publication

IBM® Security zSecure™ Audit for ACF2 Version 2.1.0 provides system auditing and monitoring utilities for ACF2. It collects and analyzes data from ACF2 systems SMF event records. This data can be used to monitor user access privileges, implement scoping to limit user privileges, and report on user behavior. zSecure Audit for ACF2 improves upon existing tools to facilitate robust security auditing for mainframe systems.

Intended audience

The target audience for this book includes security administrators and mainframe systems programmers. Readers of this book should have working knowledge of ACF2 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 Audit for ACF2. This document is not a full reference manual and does not cover all features. This guide concentrates on the interactive features using ISPF panels and highlights the major functions of the product. After working through this guide, you should be able to perform typical tasks.

Except for a few introductory pages, this document is intended as a hands-on guide while you work with the product. It introduces IBM Security zSecure Audit for ACF2 and explains how to use it to analyze Logon IDs, Rules, and Global System Options, and to run reports.

Access to publications and terminology

This section provides:
• A list of publications in the “IBM Security zSecure library.”
• Links to “Online publications” on page viii.
• A link to the “IBM Terminology website” on page viii.

IBM Security zSecure library

The following documents are available online in the IBM Security zSecure library:
• IBM Security zSecure Release information
  For each product release, the release information topics provide information about new features and enhancements, incompatibility warnings, and documentation update information for the IBM Security zSecure products. You can obtain the most current version of the release information at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic= com.ibm.zsecure.doc_2.1/welcome.htm
• IBM Security zSecure CARLa-Driven Components Installation and Deployment Guide, SC27-5638
  Provides information about installing and configuring the following IBM Security zSecure components:
  – IBM Security zSecure Admin

© Copyright IBM Corp. 1998, 2013
- 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.
  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.
  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.
  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

- **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

- **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

- **Program Directory: IBM Security zSecure Admin RACF-Offline, GI13-2278**
  
  This program directory is intended for the system programmer responsible for
  program installation and maintenance. It contains information concerning the
  material and procedures associated with the installation of the IBM Security
  zSecure Admin RACF-Offline component of IBM Security zSecure Admin.
  Program directories are provided with the product tapes. You can also download
  the latest copy from the IBM Security zSecure documentation website at
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](http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss) 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**


**IBM Terminology website**


Related documentation

The IBM Security zSecure Audit for ACF2 User Reference Manual (LC27-5640) provides detailed information about the IBM Security zSecure Audit for ACF2 components.

This publication is provided on the IBM Security zSecure Documentation CD (LCD7-5373) provided with IBM Security zSecure Audit for ACF2. 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](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](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

zSecure Audit for ACF2 provides ACF2 and z/OS monitoring, Systems Management Facility (SMF) reporting, z/OS integrity checking, change tracking, and library change detection.

In zSecure Audit for ACF2, the primary processing programs are large modules that can be used in batch or interactive mode. Interactive mode is the most common, although batch mode is useful for automated periodic checks or for producing daily reports. The user interface for the interactive mode is implemented in ISPF by using the panel, skeleton, and message libraries supplied with zSecure. ISPF is the main program that is running during an interactive session. The interactive panels call the zSecure application program CKRCARLA load module as needed. Figure 1 illustrates the general flow of data. The user works through ISPF panels, which generate commands that are sent to zSecure Audit for ACF2. The results are displayed through ISPF panels.

This general design, with separate interactive and non-interactive components, has a number of 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 customizing ISPF.
- Any functions that can be run interactively can also be run in batch mode.
- An installation can create customized reports by using the CARLa command language and run these reports from the ISPF panels.
- zSecure Audit for ACF2 can be used remotely, in cases where a TSO connection is impossible or impractical; for example, in NJE networks.
zSecure Audit for ACF2 uses several different types of data. Figure 2 provides a quick overview of the data and sources of the data to help understand the product.

Figure 2. zSecure Audit for ACF2 Input Sources

zSecure Audit for ACF2 requires ACF2 data that can originate from different sources that include:

- The backup of the live ACF2 database
- Unloaded ACF2 data copied from a backup
- An alternate cluster
Old backups; for example, on tape

zSecure produces unloaded ACF2 data by reading the backup ACF2 file and creating a copy in a proprietary format suitable for high-speed searches.

The System Management Facility (SMF) data can come from the live SMF data sets, SMF log streams, or from sequential SMF data sets produced with the IFASMFDP or IFASMFDL programs. These IBM programs unload SMF records as follows: the IFASMFDP program from the live SMF data sets and the IFASMFDL program from the SMF log streams. Sequential SMF data sets can be on disk or tape, although many installations might not permit TSO users to mount tapes for interactive use. zSecure Audit for ACF2 cannot process pseudo-SMF files created by the Report Writer or the IRRADU00 SMF unload program.

zSecure Audit for ACF2 uses Direct Access Storage Device (DASD) data provided by the zSecure Collect program. This program runs as a batch job and reads all online Volume Table Of Contents (VTOCs), VSAM Volume data sets (VVDS), catalogs, selected Partitioned data set (PDS) directories, and calculates digital signatures at the member and data set level when requested. It writes all this information to a CKFREEZE data set.

The product also uses z/OS control block data. This data is gathered by zSecure Collect at the same time it gathers DASD data. It uses Authorized Program Facility (APF)-authorized functions to retrieve data from other address spaces and from read-protected common storage. Additionally, with batch collection, you can analyze a remote system where the data was collected.

Remote data

zSecure supports the use of remote data sets as input for creating reports and displays. This functionality, known as multi-system support, enables reporting and managing multiple systems from a single session. 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 to access the same data locally.

To use the multi-system support functionality, 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 ACF2 databases, SMF input files, CKFREEZE data sets, and other defined data sets. For more detailed information, see the IBM Security zSecure Audit for ACF2: User Reference Manual.

ACF2 terminology used in this guide

This section provides definitions for the ACF2 terminology used in this Getting Started guide.

**LID**  
The 1-8 character ID of a user or task. A pointer to the ACF2 1024-byte Logon ID record in the Logon ID database.

**LOGON ID**  
Used interchangeably to indicate the LID or the 1024-byte Logon ID record.

**LOGON ID RECORD**  
The 1024-byte Logon ID record stored in the ACF2 Logon ID database.
GLOBAL SYSTEM OPTIONS (GSO)
ACF2 system options that apply to base ACF2 (MVS, OS/390, z/OS).
Numerous GSO records control areas such as passwords, overall operating
mode, job submission, and bypass conditions.

MASK or MASKING
ACF2 uses two masking characters: the dash (-) and the asterisk (*). The
dash generally means multiple characters or multiple levels in data set
names. The asterisk specifies a single character or position. Masking
indicates wildcard characters for matching logon IDs, uid (ACF2 USER
field user ID) strings, or data set names.

NEXTKEY
The NEXTKEY parameter is used in the environment section of resource
and data set rules. It acts as a pointer to additional rule lines for
determining access. NEXTKEYs modularize a rule set for ease in
administration and are required when a rule set is too large to compile.
NEXTKEYed rule sets do not function as stand-alone rules. They are
dependent on the parent rule set (point of origination). During ACF2 rule
validation, NEXTKEYed rule sets might or might not be used in the
process. This is dependent on the data set or resource requested, and
whether a match is found in the parent rule set before reaching the
NEXTKEY pointer to a NEXTKEYed or child rule.

PARENT
The term parent is used to indicate the base rule set versus a NEXTKEYed
rule set. The parent or base rule set is the branching point or starting point
of NEXTKEYs.

CHILD
The term child is used to indicate NEXTKEYed rule sets versus the parent
rule set. Child rules originate or belong to parent rules. See NEXTKEY.

STOPPER LINES
Stopper lines are used to stop ACF2 rule processing in order to prevent
any rule line match further down in the rule logic. Rule lines with a dash
for the data set name and a mask character in the uid indicate any data set
name if taken out of context and any user if taken out of context. A
stopper line such as - uid(*) prevents access; notice the absence of
permissions. To protect data sets that require limited access, insert stopper
lines immediately after the rule line that grants access. These stopper lines
prevent anyone from gaining the public access found at the end of a rule
set such as
- UID(*) READ(A)

ACF2 processing stops when a match is found for data set Name (DSN)
and uid entries.

PREVENT LINES
See STOPPER lines.

RULE
Used interchangeably with rule line and rule set.

RULE LINE
Used to indicate a specific line within a rule set.

RULE SET
Used to indicate all rule lines within a $KEY; includes all rule lines in the
set.
RULE KEY
The $KEY value; that is, $KEY(SYS1). SYS1 is the rule key in this example.

HIGH LEVEL QUALIFIER (HLQ)
The first qualifier, which is node or level, in a data set name. The entire HLQ is always the $KEY value or rule key for a data set rule. Can be one to eight characters.

SCOPING
Limits security administrative capabilities and data access capabilities for powerful privileged Logon IDs.

ACF2 scoping
ACF2 scoping provides control over the security administrative Logon ID privileges: SECURITY, ACCOUNT, and AUDIT. See Table 1.

- The SECURITY privilege grants list and update access to Logon IDs and Rules. This privilege allows for storing rules in the database, changing rule sets, changing Logon ID records, and changing Infostorage records. The SECURITY privilege grants access to anything on your system. However, there are a few controls over these powerful privileges: scoping, RULEVLD, and RSRCVLD.
- The ACCOUNT privilege grants creation and update access to Logon IDs. This privilege allows for creation, change, and deletion of Logon ID records.
- The AUDIT privilege enables an ID to look at but not touch ACF2 database records.

Scoping is used to limit administrative capabilities of these powerful Logon ID privileges against the Logon ID, Rules, Infostorage databases, and data access. Scoping is site-defined through ACF2 Infostorage SCOPE records and the related SCPLIST field in the Logon ID record. Typically, the security administrative staff maintains these controls.

While scoped security privileged logon IDs have limited administrative and data access capabilities, unscoped security privileged IDs have total access. Unscoped IDs can administer all logon IDs, data set rules, and general resource rules. Additionally, unscoped IDs have access to all data sets and general resources in the system regardless of ACF2 rule limitations unless RULEVLD and RSRCVLD are present in the Logon ID record. For more information about RULEVLD and RSRCVLD, see Figure 16 on page 18.

Table 1. ACF2 Privileges

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Security Administration Capabilities Allowed with Privileges</th>
<th>Type of Access ALLOWED with Privilege: even though Rule does NOT Permit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Create and Delete LIDs</td>
<td>List LIDs</td>
</tr>
<tr>
<td>Security</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Account</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Audit</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Privilege</th>
<th>List</th>
<th>List</th>
<th>List</th>
<th>List</th>
</tr>
</thead>
</table>

Chapter 1. Overview 5
Sample scope records

Scoping is defined in Infostorage Scope records. The Scope record must be connected to a Logon ID for the scoping to function through the SCPLIST field in the Logon ID record.

The scope definition is located in the Infostorage database. Establishing the definition requires knowledge of how the ACF2 Infostorage database is structured. You can think of Infostorage as a filing cabinet with many drawers:

- Each drawer is labeled with a Class value that represents the drawer contents.
- Each drawer might contain multiple folders, each with a unique three-character type code.

Table 2. Type codes

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSN( )</td>
<td>Data set name: partial or full or High Level Qualifier</td>
</tr>
<tr>
<td>LID( )</td>
<td>LOGON ID records</td>
</tr>
<tr>
<td>UID( )</td>
<td>User ID Strings</td>
</tr>
<tr>
<td>INF( )</td>
<td>Infostorage records</td>
</tr>
</tbody>
</table>

Table 3. Class values

<table>
<thead>
<tr>
<th>Class values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Control records g50 = type code</td>
</tr>
<tr>
<td>D</td>
<td>DB2 records</td>
</tr>
<tr>
<td>E</td>
<td>Entry records</td>
</tr>
<tr>
<td>F</td>
<td>Field records</td>
</tr>
<tr>
<td>I</td>
<td>Identity records</td>
</tr>
<tr>
<td>M</td>
<td>Mandatory Access Control</td>
</tr>
<tr>
<td>P</td>
<td>Profile records</td>
</tr>
<tr>
<td>R</td>
<td>Resource Rule records fac, pgr, tgr, cmd, pan ... = type codes</td>
</tr>
<tr>
<td>S</td>
<td>Scope records scp = type code</td>
</tr>
<tr>
<td>T</td>
<td>Shift records</td>
</tr>
<tr>
<td>V</td>
<td>ACF2/VAX records</td>
</tr>
<tr>
<td>X</td>
<td>Cross-reference records</td>
</tr>
</tbody>
</table>

Scope records can contain four fields with values. Fields can contain a list of specific or masked entries.

Using zSecure Audit for ACF2, you can perform the following tasks:

- Limit a security administrator's capability to only that administrator's functional area by specifying specific LIDs, UIDs, data sets, and Infostorage records, that is, Resource Rules, because they are located in Infostorage.
- Issue ACF2 commands to list or insert Scope records by using the Class value and Type code.
- Connect the Logon ID to the Scope record by providing a value for SCPLIST in the Logon ID record.
Figure 3 shows the scope record for a security administrator, JSMITH. JSMITH is a scoped security administrator with the following privileges:

- Insert, change, and delete any Logon ID that has a uid string of **PAY.
- Administer data set rules with data set names ppay*** and tpay-
- Administer Infostorage records with a Class of R, type code of CKC, starting with PAY-.

Figure 3 and Figure 4 show the resource rules.

```plaintext
set lid
LID
list jsmith
JSMITH CHPAYMGR JSMITH SMITH, JOHN
DEPT(PAY) JOBF(MGR) LOC(CH)
PRIVILEGES ACCOUNT JOB SCPLIST(PAYROLL) SECURITY TSO
```

Figure 3. User privileges

```plaintext
set scope(scp)
SCP
list payroll
PAYROLL DSN(PPAY***, TPAY-)
LID(********) UID(**PAY) INF(RCKCPAY-)
```

Figure 4. Scope definition for PAYROLL

**Scoping by default**

Because ACF2 has protection by default, scoping is turned on by default in zSecure Audit for ACF2. This default means that general users are limited to what they can display or generate, governed by their scoping.

**LIST command**

Scoped administrators can display only the ACF2 records within their scope using native ACF2 commands and the zSecure Audit for ACF2 LIST command. See Table 3 on page 6. The ACF2 records that can be selected or displayed must in some way be in the scope of the user. Access can be allowed based on the following criteria:

- The user has a privilege that allows decompilation of all access rules and resource rules through the DECOMP setting in the GSO RULEOPTS record.
- The user has a privilege that allows listing all Infostorage records other than resource rules through the INFOLIST setting in the GSO OPTS record.
- The record is in scope according to the user’s SCPLIST record. For Logon ID records, the additional limitations posed by the default ACSALTCK exit routine shipped with ACF2 are also taken into account.
- The $KEY of an access rule set matches the PREFIX in Logon ID record of the user.
- Access to your own Logon ID record is allowed.

If a user attempts access outside of the scope of the Logon ID, the LIST Output panel displays an error message as shown in Figure 5 on page 8.
SELECT command

Scoping applies to zSecure Audit for ACF2 commands. However, if your Logon ID has READ access to resource type XFC CKR.READALL, then scoping is overridden and you can view anything through zSecure Audit for ACF2 commands.

Screen navigation

Make sure that you are logged on to TSO with a large enough region size. zSecure Audit for ACF2 uses virtual storage to reduce the 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 region size of 128 MB is sufficient in most cases.

- To open the Main menu, complete the steps in “Opening the Main menu” on page 10.
- To try out the options, complete the steps in “Trying out the options” on page 10.

From the Main menu, you can use a few display functions to ensure that everything is working correctly. IBM Security zSecure Audit for ACF2 is using your unloaded copy of the ACF2 database for input. Using the unloaded copy causes no noticeable effects on production operations.

In the following chapters, you are guided through the functions for viewing ACF2 Logon IDs, rules, and control options. Before exploring the details, review a few basic navigation steps in the following procedure.

The first time you enter the Main menu, only the major selection options are shown. When you select one of these options by typing the two character abbreviation (for example, AA) the selection options are expanded to provide more detailed options. Alternatively, the next selection submenu is displayed.
zSecure Audit for ACF2 displays everything in the unloaded ACF2 database relevant to the function of the panel, such as Logon IDs or Rules. With a large ACF2 database, you might not want to do this too many times. One or two selection or exclusion parameters greatly reduces the amount of data displayed.

zSecure Audit for ACF2 displays any Logon ID matching the criteria entered in the Logon ID Selection panel. If nothing is entered for a field, that field is ignored during the search. Several fields accept the / character. The / signifies that the option is selected, and is used for selecting Logon IDs or rules that match the specified parameter. Some other fields also accept an S indicator to activate the selection option. A blank means that the option is ignored during Logon ID selection. In the example shown in Figure 7, the Attributes selection criteria is selected and the other fields are not selected (that is, blank).

```
Menu  Options  Info  Commands  Setup
IBM Security zSecure Audit for ACF2 - Logonid Selection
Option ===>______________________________________________________ start panel
Indicates that option 'Attributes' is selected.
Logonid ........ (user id or ACF2 mask)
User's name .... (name/part of name, no filter)
UID string .... (string or ACF2 mask)

Additional selection criteria
Date fields / Attributes
Indicates that 'Date fields' and 'Print format' options are ignored.
Output/run options
  Summarize on UID group
  Print format Customize title Send as email
  Background run Full page form Sort differently Narrow print
```

Figure 7. Logon ID selection panel

- To view the Rules information, complete the steps in "Viewing the Rules information" on page 10.
- To use the Audit information, complete the steps in "Viewing Audit information" on page 10.

The letters S (SELECT) and L (LIST) apply when you want to view detailed information about a Logon ID or Rule Set. You can also use the / character to request additional choices for specific filters or logic before a database search.

When in doubt about what is the appropriate entry for a field, type / and press Enter. A window displays the appropriate characters for data entry. Some screens provide for logic selection using AND and OR keywords and Y (yes) and N (no) when selecting certain Logon ID attributes, such as privileges. These are shown in later examples.

Standard ISPF screen navigation applies:

- **PF1** Help
- **PF3** End or return
- **PF7, PF8**
  *Scrolling backward (PF7) and forward (PF8)*
- **PF10, PF11**
  *Scrolling to the right (PF10) and left (PF11)*

**Tip:** All normal ISPF functions and techniques exist in IBM Security zSecure Audit for ACF2. It is assumed that you are already familiar with ISPF, so normal usage is not described here. If your 3270 session has a 24-line screen, enter the ISPF command `PFSHOW OFF` in the command line to turn off the PF key display so that zSecure Audit for ACF2 information can be displayed in all 24 lines.
Opening the Main menu

Procedure

Open the Main menu to perform many tasks:

1. Navigate to ISPF Option 6.
2. Enter the command **CKR**.

The Main menu opens as shown in **Figure 8**.

![Main menu](image)

Trying out the options

Procedure

1. In the **Option** field, type **AA** and then press Enter to select ACF2 Administration.
2. Type **L** and then press Enter to open the Logonid Selection panel.
3. Press Enter without entering any parameters in the panel.

Viewing the Rules information

Procedure

1. Press **PF3** until you return to the Main menu.
2. In the **Option** field, type **R** for Rules.
3. Press Enter to open the Rules Selection panel.

You can request searches against specific rules or multiple rules by using filters such as data set name or uid string. This panel provides various fields that you can further investigate, such as **Specify more selection criteria**. To request this function, type **/** in the selection field for this function. For more information, see Chapter 3, “Rule analysis,” on page 27.

Viewing Audit information

Procedure

1. Press **PF3** until you return to the Main menu.
2. In the **Option** field, type **AU** for Audit.
3. Press Enter to open the Audit Selection panel.
Masking characters

ACF2 masking characters are also recognized by zSecure Audit for ACF2. In some screens, you can filter data by using the masking characters asterisk (*) and dash (-). Remember that the asterisk represents one character and the dash represents zero or more characters at the end of a uid string and Logon ID mask. A dash within a data set name can represent multiple characters or multiple data set name levels, depending on the placement of the masking character.

Date fields

Several selection fields are for date specification. You can use various values and operators. However, all year values must be specified in four digits. Figure 9 shows examples of valid date specification values.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</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>(a date was today)</td>
</tr>
<tr>
<td>= TODAY-3</td>
<td>(three days before today)</td>
</tr>
<tr>
<td>&lt; TODAY-30</td>
<td>(more than thirty days ago)</td>
</tr>
<tr>
<td>&gt; 01MAR2005</td>
<td>(any day after March 1, 2005)</td>
</tr>
</tbody>
</table>

Figure 9. Example date specification values and operators

A date of DUMPDATE is the date your ACF2 database was copied or unloaded. An operator must be entered in the small, two-character input field and the date value in the larger field in these lines.

Summary of navigation characters

Table 4 lists the valid navigation characters and their corresponding descriptions.

<table>
<thead>
<tr>
<th>Navigation Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>Option selection</td>
</tr>
<tr>
<td>S</td>
<td>Select for explanation of settings, view audit concerns</td>
</tr>
<tr>
<td>L</td>
<td>List to view the ACF2 record as stored on database</td>
</tr>
<tr>
<td>AND</td>
<td>Boolean logic – search for combination of attributes</td>
</tr>
<tr>
<td>OR</td>
<td>Boolean logic – search for any selected attributes</td>
</tr>
<tr>
<td>Y</td>
<td>Boolean logic – search for attribute</td>
</tr>
<tr>
<td>N</td>
<td>Boolean logic – do not search for attribute</td>
</tr>
</tbody>
</table>
Chapter 2. Logon ID tasks

The following topics explain how to list Logon IDs, analyze attributes, determine how users are categorized into groups by using the uid string, and see which powerful privileges are used.

Auditing the Logon ID database aids the enforcement of powerful privilege control, password standards, and proper user grouping by using the uid string.

Use the Logon ID function to complete the following tasks:
\begin{itemize}
  \item View a Logon ID as stored in the ACF2 database.
  \item View a Logon ID with explanations of field settings and audit concerns.
  \item Search for Logon IDs with matching uid strings and display all user IDs that are grouped similarly.
  \item Find a Logon ID with a specific user name value.
  \item Display all Logon IDs that have a similar naming convention.
  \item Display all Logon IDs with powerful privileges.
  You can search for any privilege combination by using Boolean logic with AND and OR criteria.
\end{itemize}

You can view and assess Logon ID records through the ACF2 Administration option in the Main menu.

To access the Logon ID functions, complete the steps described in "Accessing the Logon ID functions".

Accessing the Logon ID functions

Procedure
1. Return to the Main menu by pressing PF3.
2. Type option AA to work with the ACF2 administration functions as shown in Figure 10.
3. Press Enter to display the ACF2 Administration options in the Main menu.
4. Type option L and press Enter to view the Logon ID overview as shown in Figure 11.

Displaying your Logon ID

The Logon ID Selection panel as shown in Figure 12 provides a simple query when you enter a Logon ID, name, or a uid string. Specific selection criteria become available through the Additional selection criteria heading.

To display your Logon ID, type your Logon ID or any other Logon ID in the Logon ID field as shown in Figure 12.

The product searches the unloaded ACF2 database and displays the Logon ID information across a single line. The performance information is listed in a message on the upper right line of the display. See Figure 13 on page 15. The information shown is the elapsed and processor time used for the query.
Figure 13 is an overview display in which each Logon ID is displayed on a single line. Press PF7 to scroll up, PF8 to scroll down, PF10 to scroll left, and PF11 to scroll right to view more information. You can also enter a line command on this screen. Using a line command is reviewed in the next example.

**Tip:** Many of the zSecure Audit for ACF2 data displays are wider than 80 characters. Use PF10 and PF11 to scroll left and right.

Table 5 provides descriptions of the Logon ID fields available in the Logon ID panels. To view all the fields, scroll by pressing PF11.

**Table 5. Logon ID field descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LID</td>
<td>Logon ID</td>
</tr>
<tr>
<td>Complex</td>
<td>Name for the ACF2 security database that contains this Logon ID.</td>
</tr>
<tr>
<td>Name</td>
<td>The NAME field of this Logon ID.</td>
</tr>
<tr>
<td>UID</td>
<td>The user identification string associated with this Logon ID.</td>
</tr>
<tr>
<td>N</td>
<td>The Logon ID cannot enter the system, due to CANCEL/SUSPEND/ACTIVE/EXPIRE settings or due to an excessive number of invalid password attempts.</td>
</tr>
<tr>
<td>TOJRS</td>
<td>This Logon ID has the attributes TSO, Other (that is, CICS, IMS, or IDMS), JOB, RESTRICT, or STC.</td>
</tr>
<tr>
<td>NRB</td>
<td>This Logon ID has the attributes NON-CNCL, READALL, or TAPE-BLP.</td>
</tr>
<tr>
<td>MJ</td>
<td>This Logon ID has the attributes MUSASS or JOBFROM.</td>
</tr>
<tr>
<td>MP</td>
<td>This Logon ID has the attributes MAINT or PPGM.</td>
</tr>
<tr>
<td>ScpList</td>
<td>The name of the Scope record associated with this Logon ID.</td>
</tr>
<tr>
<td>SALCA</td>
<td>This Logon ID has the attributes SECURITY, ACCOUNT, LEADER, CONSULT, or AUDIT.</td>
</tr>
<tr>
<td>RD</td>
<td>This Logon ID has the attributes RSRCVLD or RULEVLD.</td>
</tr>
<tr>
<td>Prefix</td>
<td>The High Level Index determining data ownership for the Logon ID.</td>
</tr>
<tr>
<td>TJ</td>
<td>The Logon ID has the TSO or JOB attribute.</td>
</tr>
<tr>
<td>LastAccDa</td>
<td>The data of last system access by this Logon ID.</td>
</tr>
<tr>
<td>ATime</td>
<td>The time of last system access by this Logon ID.</td>
</tr>
<tr>
<td>AccSrc</td>
<td>The source of last system access by this Logon ID.</td>
</tr>
<tr>
<td>#Vio</td>
<td>The total number of security violations committed by this user.</td>
</tr>
</tbody>
</table>
| #I | The number of invalid password attempts made since the last logon.
Continue to scroll to the right (PF11) to view more:

### Table 6. More Logon ID field descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#V</td>
<td>The number of invalid password attempts made on PswdDate.</td>
</tr>
<tr>
<td>#P</td>
<td>Specifies the number of password phrase violations that occurred on the day that the last invalid password phrase was entered (PWP-DAT).</td>
</tr>
<tr>
<td>#K</td>
<td>Number of Kerberos key violations.</td>
</tr>
<tr>
<td>PswdDate</td>
<td>Day of the last invalid password attempt.</td>
</tr>
<tr>
<td>PwPDate</td>
<td>Date when the user made the last invalid password phrase attempt.</td>
</tr>
<tr>
<td>PswdSrc</td>
<td>Source of the last invalid password attempt.</td>
</tr>
<tr>
<td>PW change</td>
<td>Day the password was last changed.</td>
</tr>
<tr>
<td>XM</td>
<td>PSWD-EXP is on for this logon ID, indicating that this user’s password was reset by an administrator. M is a flag field that indicates whether the current password is case-sensitive.</td>
</tr>
<tr>
<td>MnD</td>
<td>Minimum number of days that must pass before the password can be changed again.</td>
</tr>
<tr>
<td>MxD</td>
<td>Maximum number of days that must pass before the password can be changed again.</td>
</tr>
<tr>
<td>Source</td>
<td>The source from which this logon ID can enter the system.</td>
</tr>
<tr>
<td>Shift</td>
<td>The name of this user’s SHIFT record.</td>
</tr>
<tr>
<td>Zon</td>
<td>The time zone associated with this logon ID.</td>
</tr>
<tr>
<td>CSP</td>
<td>The logon ID was Canceled, Suspended, or suspended for an excessive number of password violations.</td>
</tr>
<tr>
<td>Active</td>
<td>This logon ID cannot enter the system before this date is reached.</td>
</tr>
<tr>
<td>Expire</td>
<td>This logon ID cannot enter the system after this date is reached.</td>
</tr>
<tr>
<td>PGM</td>
<td>This logon ID can enter the system only when executing the program specified here.</td>
</tr>
<tr>
<td>SbA</td>
<td>Jobs specifying this logon ID can be submitted through APF-authorized programs only.</td>
</tr>
<tr>
<td>Pri</td>
<td>Audit priority for this logon ID.</td>
</tr>
<tr>
<td>Group</td>
<td>Default group.</td>
</tr>
<tr>
<td>Homenode</td>
<td>Node where this logon ID is kept in a logon ID database.</td>
</tr>
<tr>
<td>SyncNode</td>
<td>The name of the node where the synchronized logon ID for a user resides.</td>
</tr>
<tr>
<td>Phone</td>
<td>The telephone number for this user.</td>
</tr>
</tbody>
</table>

### Displaying Logon IDs using SELECT

#### Procedure

For easier viewing and interpreting of Logon ID records, perform the following steps:

1. Position the cursor beside the Logon ID.
2. Type the letter S as shown in Figure 14 on page 17.
3. Press Enter to open the detailed view. Figure 15 shows the first part of the detailed view. Press PF8 to scroll down to the remainder of the panel, shown in Figure 16 on page 18. The detail display shows Logon ID fields, settings, and any audit concerns.

Figure 14. SELECT for more detail

Figure 15. Detail display of SELECT Logon ID
To view the rest of the Logon ID details, press PF8 to scroll to the end of the record.

![IBM Security zSecure Audit for ACF2 ACF2_LID display](image)

**Results**

In Figure 16, the Audit concern section identifies issues with the RULEVLD and RSRCVLD settings. RULEVLD and RSRCVLD are recommended for SECURITY privileged logon IDs because these attributes limit data set and resource access according to rule validation. Without RULEVLD and RSRCVLD attributes, the SECURITY privileged Logon ID can access anything. Additionally, any access outside of the rule is allowed and is logged to SMF for review.

**Interpreting Logon ID settings**

Figure 16 on page 17 shows expanded Logon ID fields available through the SELECT command. Compare Figure 15 on page 17 to the display in Figure 19 on page 19. This panel shows the Logon ID settings in native ACF2 format, presented by using the LIST command. zSecure Audit for ACF2 interprets and explains the cryptic fields and settings in the Logon ID record.

The Scopable privileges section in Figure 15 on page 17 indicates whether a user has a privilege assigned, specifying a YES or NO. The Logon ID has the SECURITY and ACCOUNT privileges assigned, showing the value present. SECURITY privilege permits the user to store rules on the database, change rule sets, change Logon ID records, and change Infostorage records. ACCOUNT privilege permits the user to create, change, and delete Logon ID records. To determine whether a Logon ID has restricted database administration capabilities, look at the Scope section in Figure 15 on page 17. A value is displayed under the ScpList column. The scope list value of SECDEPT is defined in the ACF2 Infostorage database.

An ACF2 scope list record can limit the privileged user to administer certain Logon IDs, rules, and Infostorage records. To understand the limitation of the scope list record, referenced in the SCPLIST Logon ID record field of Figure 15 on page 17, list the Infostorage record using native ACF2 commands:
The first command points to Infostorage SCOPE records. The second command lists the SCOPE record.

The Password anomalies section in Figure 15 on page 17 explains the password section of the Logon ID.

---

### Displaying logonids using LIST

#### About this task

The LIST command displays the Logon ID details in native ACF2 format.

To use the native ACF2 LIST command, complete these steps:

**Procedure**

1. Press PF3 to return to the Logon ID screen.
2. Type an **L** in the selection field for a Logon ID (LID) as shown in Figure 18.
3. Press Enter to view the Logon ID information.
   
   In this example, Figure 19 displays the Logon ID in its natural state, as if you entered a native ACF2 command.

4. Press PF3 to return to the Logon ID Selection panel.
Results

In contrast to the LIST command output, the SELECT command output takes the
guesswork out of interpreting Logon ID fields: compare the native display of
Figure 19 on page 19 with Figure 15 on page 17 and Figure 16 on page 18.

The appropriate ACF2 authority is required to use the LIST and SELECT
commands in zSecure Audit for ACF2. The AUDIT, ACCOUNT, or SECURITY ACF2
Logon ID privilege is required to view any Logon ID. ACF2 SCOPE records also
affect this function. Standard ACF2 Logon ID authorization applies when using
zSecure Audit for ACF2 functions.

Displaying Logon IDs using a mask

About this task

From the Logon ID Selection panel, you can display only logon IDs matching a
logon ID mask, such as SYS-. Use a logon ID mask that applies to your
environment. You can use the ACF2 masking characters dash (-) and asterisk(*)

Procedure

To display logon IDs matching a logon ID mask, complete the following steps:

1. In the Logon ID field, type a mask that is appropriate, as shown in Figure 20.
   This example uses SYS-.

2. Figure 21 on page 21 displays all logon IDs that begin with SYS, if your
   organization uses this naming convention.
From the ACF2_LID display panel, type the **L** or **S** command in the selection field for a logon ID to view more detailed information. You can scroll the panel by using the standard ISPF function keys PF10, PF11, PF7, and PF8 from this screen.

3. Press PF3 and return to the Logon ID Selection panel.

### Displaying logon IDs with matching UID string

#### About this task

From the Logon ID Selection panel, you can specify uid string values to search for logon IDs with a matching uid string. This example requests to view all logon IDs that are in a location known as **NC** (a uid string field of **LOC**) and a department known as **SYS** (a uid string field of **DEPT**).

#### Procedure

To search for logon IDs with a matching uid string, complete the following steps:

1. In the Logon ID Selection panel, type a masked entry that is appropriate to your environment in the **UID string** field. The example in Figure 22 uses NCSYS-.

2. Press Enter to view the results.

This example, Figure 23 on page 22, shows all logon IDs that match the NCSYS-uid string. From this panel, you can scroll across using PF11, or you can specify **SELECT** and **LIST** to view a Logon ID record.
3. Press PF3 to return to the Logon ID Selection panel.

### Listing logon IDs with special privileges

**About this task**

The Logon ID Selection panel allows you to select privileges and specify filters using Boolean logic to tailor your criteria.

**Procedure**

From the Logon ID Selection panel, use the following procedure to list all logon IDs with privileges such as SECURITY and ACCOUNT:

1. **Optional**: Type a dash (-) in the Logon ID field.
2. Type a / in the Attributes field, as shown in Figure 24.
3. Press Enter to view the advanced selection criteria in the Logon ID Selection panel shown in Figure 25 on page 23.
4. Use the advanced selection criteria to set filters to select privileges using Boolean logic. To make selections, type a /, Y, or N in the selection field for a privilege field. The / and Y characters are interchangeable.
5. You can use further filters by changing the OR fields to AND. Consider carefully the search you are targeting. For example:
   - If you want to view all logon IDs with the SECURITY privilege present, type a / or Y beside the Security field. Then press Enter.
   - If you want to find all logon IDs with Security or Account, select both privileges by using a / or Y selection character. Then press Enter.

Figure 23. Display of logon IDs with matching uid string

![Figure 23. Display of logon IDs with matching uid string](image)

**Table 23. Logon IDs with matching uid string**

<table>
<thead>
<tr>
<th>LID</th>
<th>Complex</th>
<th>Name</th>
<th>UID</th>
<th>TOJRS</th>
<th>NRB</th>
</tr>
</thead>
<tbody>
<tr>
<td>JBENTLE</td>
<td>PROD</td>
<td>BENTLEY, JAN</td>
<td>NCSYSGR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCASPER</td>
<td>PROD</td>
<td>CASPER, FRANK</td>
<td>NCSYPGR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MABRAMS</td>
<td>PROD</td>
<td>ABRAMS, MARK</td>
<td>NCSYPGR</td>
<td>MABRAMS</td>
<td>T J</td>
</tr>
<tr>
<td>GWEBSTER</td>
<td>PROD</td>
<td>WEBSTER, GLENDA</td>
<td>NCSYANL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JNICHOL</td>
<td>PROD</td>
<td>NICHOLS, JIM</td>
<td>NCSYADM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 24. Logon ID overview criteria screen

![Figure 24. Logon ID overview criteria screen](image)
• If you want to find all logon IDs with SECURITY and ACCOUNT privileges, type AND over the OR overtypeable field, and type a / or Y beside the Security and Account fields. Then press Enter.

• If you want to find all logon IDs with only SECURITY and ACCOUNT privileges, complete the panel as follows then press Enter:
  – Type AND over the OR overtypeable field.
  – Type a / or Y beside the Security and Account fields.
  – Type N beside Audit, Consult, and Leader.

Results

There are differences in the example selections shown. The AND and OR selections (shown in Figure 25) provide the capability to include or exclude groups of privileges. A request to display all logon IDs with SECURITY and ACCOUNT privileges would show logon IDs with both these privileges using AND.

A request to find logon IDs with SECURITY or ACCOUNT displays logon IDs that have either attribute, using OR. To change the selection from the default OR to AND, type over the field.

![Menu Options Info Commands Setup](image)

IBM Security zSecure Audit for ACF2 - ACF2 - Logonid Selection

<table>
<thead>
<tr>
<th>Menu</th>
<th>Options</th>
<th>Info</th>
<th>Commands</th>
<th>Setup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Security zSecure Audit for ACF2 - ACF2 - Logonid Selection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>like</td>
<td>-------</td>
<td>------</td>
<td>----------</td>
<td>-------</td>
</tr>
</tbody>
</table>

Specify groups of criteria the logonids must meet:

Application privileges

OR  =  TSO  =  CICS  =  IMS  =  IDMS
    =  Batch  =  Restrict  =  Started task

System privileges

OR  =  Non-Cancel  =  Readall  =  Use Tape BLP  =  Lid for Musass
    =  Use Jobfrom  =  Maint  =  PGM

Restrictions

OR  =  Rsrcvld  =  Rulevld  =  Inactive
    =  Scoped  =  Scopelist  =  (Only valid if scoped)

Scopable privileges

OR  =  Security  =  Account  =  Leader  =  Consult
    =  Audit

Figure 25. Overtypeable fields

There are many possible combinations of OR, AND, and Y and N. For example, if you want to find all logon IDs with SECURITY and ACCOUNT and not NON-CNCL, complete the following steps: “Example: Find all logon IDs with SECURITY and ACCOUNT and not NON-CNCL:” on page 24.

If your environment has logon IDs with both the SECURITY and ACCOUNT privileges present, the results from the example selections entered in Figure 27 on page 24 look similar to Figure 26 on page 24. You might want to experiment with this selection logic to display various privilege assignments.

Chapter 2. Logon ID tasks 23
From the ACF2_LID display panel, you can use the LIST or SELECT command for a Logon ID to view more detailed information.

**Example: Find all logon IDs with SECURITY and ACCOUNT and not NON-CNCL:**

**About this task**

This procedure shows how to use Boolean logic to tailor a search for logon IDs.

**Procedure**

Follow these steps to find all logon IDs with SECURITY and ACCOUNT and not NON-CNCL:

1. Type **AND** in the Scopable Privileges selection as shown in Figure 27.
2. Type **Y** for YES in the selection field for the Account and Security selections as shown in Figure 27.

   A blank beside the field indicates that the field is not considered in the search. However, a request for SECURITY and ACCOUNT displays all logon IDs with these privileges and can display logon IDs with other privileges. If the requirement is to display logon IDs with only SECURITY and ACCOUNT and no other privileges, the **N** is required for all other fields.

3. Press Enter to view the results.
Displaying all logon IDs with the same user name

About this task

You can search for all logon IDs for a specific user name. Use a value that is appropriate for your environment.

Procedure

Complete the following steps:

1. Press PF3 to return to the Logon ID Selection panel. The dash (-) in the Logon ID field is optional.
2. Type the user name in the User's name field.
   Use a value that is appropriate for your environment; for example, John Smith, Mary, or Joe. The example shown in Figure 28 uses Bert.

   ![Figure 28. Search for all users with Bert in the Name field](image)

3. Press Enter to open the Logon Selection panel shown in Figure 29.
   This example displays all logon IDs on the unloaded ACF2 database with BERT in the Name field. The Name search matches any part of a name where BERT is found. You can SELECT or LIST any Logon ID from this panel.

   ![Figure 29. Display of matching logon IDs with same Name](image)
Chapter 3. Rule analysis

The following topics describe how to list a rule and analyze access. zSecure Audit for ACF2 rule analysis functionality provides information for determining how well rules are maintained and how well the environment is protected.

There are two types of rules in ACF2: data set rules and resource rules. For information, see "Data set rules" and "Resource rules."

Data set rules

Data set rules control access to system, user, and application data sets. Data set names are composed of multiple qualifiers separated by a period. Each qualifier has a maximum length of eight characters that count toward the maximum data set name length of 44 characters. A typical data set name might be SYS1.PARMLIB or DEMO.MASTER.PAYROLL. Each qualifier describes the content or nature of the data.

Resources are protected through ACF2 resource rules. An ACF2 resource is anything other than a data set. Resources include objects such as transaction codes, commands, programs, accounts, screens, PDS members, and UNIX files.

Use the Rules function to perform the following tasks:

- View a rule.
- Select a rule to view by sections: data set name, who has access, permissions for each group or individual.
- View the specific environmental restrictions for each rule line.
- View the structure of a rule set by NEXTKEYs.
- View who can change the rule set.
- View who last changed a rule set.
- View control statements for each rule set.
- Find all data set access defined for an individual or group.
- Display access for a specific data set name.

Resource rules

Use the Resource function to complete the following tasks:

- View all resource types.
- View all resource classes.
- View a specific resource rule.
- View all rules that match a mask.
- Find all resource rule access defined for an individual or group.

Viewing data set rules

Procedure

To view data set rules, complete the following steps:

1. Press PF3 to return to the Main menu.
2. Select the ACF2 Administration option.
3. Type R to display the Rules functions as shown in Figure 30.

![Menu Options Info Commands Setup](image)

---

IBM Security zSecure Audit for ACF2

Option === R More: +

- SE Setup Options and input data sets
- AA ACF2 ACF2 Administration
- L Logonid Logonid overview
- R Rules Rules overview
- I Resource Resource rules overview
- S Infostorage Infostorage record overview
- C Custom Custom report

AU Audit Audit security and system resources
RE Resource Resource reports
EV Events Event reporting from SMF and other logs
CO Commands Run commands from library
IN Information Information and documentation

Product/Release
S655-M17 IBM Security zSecure Audit for ACF2 2.1.0

---

![Figure 30. Select rules overview](image)

4. Press Enter to open the Rules Selection panel.

5. Type a high-level qualifier in the data set HLQ field that is appropriate for your environment; for example, SYS1. The example shown in Figure 31 uses CRM2.

In the Output/run options section, notice that the Show rule lines option, which is the default setting, is selected. This setting requests display of all rule lines for a rule set key (that is, the high-level qualifier).

![Menu Options Info Commands Setup](image)

---

IBM Security zSecure Audit for ACF2 – Rules Selection

Command ===> __start panel

Show rules that fit all of the following criteria

- Data set HLQ . . . _CRM2_ (qualifier or ACF2 mask)
- UID string . . . . (fully specified UID, no mask)
- Match data set . . (no mask)
- Match UID string . . (logonid or ACF2 mask)
- Match UID(s) of LID

Additional selection criteria

- Other fields

Output/run options

- Show rule lines
- Expand nextkey
- Print format

Customize title Send as email
Background run Form oriented Sort differently Narrow print

---

![Figure 31. Rules Selection panel](image)

6. Press Enter to open the ACF2_RULELINE display panel shown in Figure 32 on page 29.
In Figure 32, the rule set, CRM2, contains all data set rule entries for the high-level qualifier CRM2. Your display will look similar. This example shows multiple rule line entries for data sets that begin with CRM2. The entries are presented in collating sequence.

The following columns across the panel indicate rule line fields:

**DSN mask column**
Lists the data set name entries such as CRM2.ACCTNG.MASTER.

**UID mask column**
Indicates the groups of users or individuals that are associated with the data set name entry such as NEACCMDR-.

**User column**
Indicates whether this entry applies only to this user ID.

7. Press PF11 to shift right and view the permissions (for example, RW E) granted to the users in the UID mask column for the data set listed in the DSN mask column.
The rule set in Figure 32 on page 29 shows that any user with a matching uid string of **OPS can read and run the data set CRM2.ACCTNG.BACKUP. In this example, the uid (**OPS) indicates users in all locations within the operations (OPS) department that can read the specified data set. All locations are listed because location is masked.

Table 7 lists the permission codes and corresponding descriptions.

**Table 7. Permission codes and descriptions**

<table>
<thead>
<tr>
<th>Permission Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>Read</td>
</tr>
<tr>
<td>W</td>
<td>Write</td>
</tr>
<tr>
<td>A</td>
<td>Allocate - create, delete, rename, catalog, uncatalog</td>
</tr>
<tr>
<td>E</td>
<td>Execute - applies only to executable code, a program, and not data files</td>
</tr>
</tbody>
</table>

Lowercase letters under the Perm column on the panel indicate that access is allowed, but logged. For example, Rw E means that read is allowed, write is allowed and logged, and execute is allowed.

**Viewing by rule set**

**Before you begin**

1. To view additional rule line fields, press PF11 to shift right. Scroll down to view additional rule lines by pressing PF8.

2. Press PF3 to return to the previous screen, that is, the Rules Selection screen.

3. To control rule displays, use the options in the lower part of the screen under **Additional selection criteria** and **Output/run options**. Continue to use the same high-level qualifier in the Data set HLQ field.

The example in Figure 34 on page 31 is a request to view the rule CRM2 by rule set. This request specifies that rule sets be shown as opposed to rule lines. If Show rule lines is also selected, rule sets are shown with the ability to view individual rule lines within each rule set. This means that if CRM2 contains NEXTKEYs, they are...
displayed in the next panel. The rule lines of the NEXTKEY rule sets can be viewed from.

**Procedure**

To view a rule by rule set, complete the following steps:

1. In the Rules Selection panel, type a rule or high-level qualifier. The example shown in Figure 34 uses CRM2.
2. Type a / in the selection field for By rule set, shown in Figure 34.

3. Press Enter to open the ACF2_RULE display panel shown in Figure 35 on page 32.

Your screen should look similar to Figure 35 on page 32. There might be multiple entries under the $Key column in collating sequence. The example shows CRM2 as the first entry and other rule sets with a similar $Key value. These are NEXTKEYed (pointed to) rule sets from CRM2. NEXTKEYed rule sets are considered children of a parent rule set, such as CRM2. This display lists rule sets in sort order. The example demonstrates NEXTKEYs. NEXTKEYs are discussed in more detail later in this chapter.

The request was for rule lines by rule set. The CRM2 rule set contains NEXTKEYs, thus the display in Figure 35 on page 32. A request for any rule set matching a mask can also be entered in Figure 35 on page 32. For example, SYS- would show all rule sets matching SYS and any other trailing characters such as SYS1, SYS2, SYST, or SYSP.
The high-level qualifier under the $Key column is to the left with the corresponding statistics (that is, LastUpDat, StoredBy), and control statements such as Rs and $Prefix to the right.

4. To view the control statements present for each rule set, press PF11 to shift right.

Figure 35. Display of HLQ by rule set

The high-level qualifier under the $Key column is to the left with the corresponding statistics (that is, LastUpDat, StoredBy), and control statements such as Rs and $Prefix to the right.

Figure 36. Additional control statements

Table 8 lists the rule set fields and descriptions, including the fields that are visible on the right when you press PF11.

Table 8. Rule set field descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Key</td>
<td>$KEY of the rule set</td>
</tr>
<tr>
<td>Rs</td>
<td>Indicates that this rule has ROLESET specified.</td>
</tr>
<tr>
<td>$Prefix</td>
<td>$PREFIX of the rule set.</td>
</tr>
<tr>
<td>LastUpDat</td>
<td>Day this rule record was last stored.</td>
</tr>
<tr>
<td>StoredBy</td>
<td>Logon ID that last stored this record.</td>
</tr>
<tr>
<td>$N</td>
<td>The rule set has $NOSORT specified.</td>
</tr>
<tr>
<td>Complex</td>
<td>Name for the ACF2 security database that contains this record.</td>
</tr>
<tr>
<td>$Mode</td>
<td>The $MODE specified for this rule record.</td>
</tr>
<tr>
<td>$ResOwnr</td>
<td>The SMS default RESOWNER for the data sets protected by the rule set.</td>
</tr>
<tr>
<td>$Owner</td>
<td>$OWNER field of the rule record.</td>
</tr>
<tr>
<td>$Member</td>
<td>The overriding name of the PDS member into which this rule set should be DECOMPiled.</td>
</tr>
</tbody>
</table>
Table 8. Rule set field descriptions  (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$NR</td>
<td>If set, this flag indicates that this rule set should never be compiled by the long rule compiler. (ACF2 has two resource rule compilers, due to support for long resource rules, which are those over 4 KB in length.) This flag effectively prevents you from using any features in this rule set that require the long rule compiler. The GSO OPTS setting COMPDYN has no influence on this behavior.</td>
</tr>
<tr>
<td>$Userdata</td>
<td>$USERDATA of the rule record.</td>
</tr>
</tbody>
</table>

Displaying data set rules using LIST

Procedure

To display data set rules using the LIST command, complete the following steps:

1. Type the selection character $ (L) beside the first $Key entry as shown in Figure 37.
   This is the parent rule set in our example.

2. Press Enter to open the panel shown in Figure 38 on page 34.
   The appropriate ACF2 authority is required to use the LIST command in zSecure Audit for ACF2. The AUDIT or SECURITY Logon ID privilege is required to list any rule. ACF2 SCOPE records also affect this function. Standard ACF2 Logon ID authorization and scoping apply to LIST functions.
   The LIST function results are similar to the native ACF2 decompiled/list command. The panel shown in Figure 38 on page 34 assumes that you understand how to view and analyze a rule in its native form.
Displaying data set rules using SELECT

About this task

Using the Select function, you can view rule statistics, date of last update, and the user who stored the rule.

Procedure

To display data set rules using the Selection function, complete the following steps:
1. Press PF3 to return to the rule display screen.
2. Type the selection character S beside a $Key entry as shown in Figure 39.
3. Press Enter.
You see a panel similar to Figure 40. This is the same rule displayed in Figure 38 on page 34 and Figure 32 on page 29.

In the ACF2_RULE display panel shown in Figure 40, you can view information about the selected rule. The data set name or mask is to the left with the corresponding uid string, which indicates who can access these data sets. Entries in the User column indicate that the entry applies only to the user ID that is shown.

4. Press PF11 to scroll to see the environment parameters.

All environment parameters that apply to each rule line show across a single line as you scroll across the display. Environmental parameters can reference ACF2 Infostorage records. When you continue scrolling, you see additional environmental parameters as appropriate for each rule line entry.

In the example in Figure 41 on page 36, the Ro column indicates, for each entry, whether the entry applies only to users who have access granted by the specified ROLE.

The Perm column indicates the permissions that apply to each line entry. The permissions are read, write, allocate, and execute, which are shown with the following letters:

- R Read
- W Write
- A Allocate
- E Execute

Any lowercase letters indicate that the permission is allowed but logged.

Figure 41 on page 36 also has three rule lines that reference a NEXTKEY, and one other environmental parameter for Volume, Source, Shift, and Library. This is typical. Many rule lines might not need additional environmental parameters. See Table 9 on page 36 for a description of the environmental parameters.
The display in Figure 40 on page 35 shows NEXTKEYs for the parent rule set CRM2 and shows a SHIFT reference for a data set mask CRM2.CUSTOMER.-. Figure 41 shows the panel scrolled to the left with the PF10 key so that you can see the data set name.

Shift records are additional controls on when a data set can be accessed. The shift reference in Figure 41 shows a record name of NORMAL. This record is defined in Infostorage database of ACF2. Usually, NORMAL refers to normal working hours; for example, 8:00 AM until 5:00 PM.

To view a shift record using native ACF2 commands, issue the following two commands as shown in Figure 42. The first command points to the Infostorage SHIFT records. The second command lists the record.

```
SET SHIFT(SFT)
LIST NORMAL
```

Figure 42. Native ACF2 commands to List the SHIFT record

5. To view more environmental parameters, press PF11.

```
IBM Security zSecure ACF2_RULE display
Command ===>
All rules with HLQ CRM2
User  No Perm N NextKey Volume Source Shift Library
R E
Rw E
R E
Rw E
R E
C
C CRM2D NORMAL
Rw E
C
C CRM2M
C CRM2PRD
```

Figure 41. Display of additional environmental parameters

Table 9. Environmental parameter descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSN mask</td>
<td>Data sets specified in the rule set, under the high-level qualifier.</td>
</tr>
<tr>
<td>UID mask</td>
<td>UID strings specified in rule entries.</td>
</tr>
</tbody>
</table>
### Table 9. Environmental parameter descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Indicates whether this entry applies only to this user ID. This field does not support masking, except that a value of &quot;-&quot; (dash) indicates that this entry applies to all users.</td>
</tr>
<tr>
<td>Role</td>
<td>Indicates whether this entry applies only to users who have access granted by this ROLE. This field does not support masking, except that a value of &quot;-&quot; (dash) indicates that this entry applies to all users.</td>
</tr>
<tr>
<td>Perm</td>
<td>Type of access for each data set entry. Read, Write, Allocate, Execute. Uppercase indicates that access is allowed; lowercase indicates that access is logged.</td>
</tr>
<tr>
<td>Nextkey</td>
<td>$KEY of rule set to be used for further validation processing.</td>
</tr>
<tr>
<td>Volume</td>
<td>Applies only to data sets residing on a volume that matches this mask.</td>
</tr>
<tr>
<td>Source</td>
<td>Applies if access attempt is made from a source that matches this mask.</td>
</tr>
<tr>
<td>Shift</td>
<td>Applies if access attempt is made at a time allowed by this SHIFT record.</td>
</tr>
<tr>
<td>Library</td>
<td>Applies if access attempts are made through a program residing in a library that matches this mask.</td>
</tr>
<tr>
<td>Program</td>
<td>Applies if an access attempt is made through a program that matches this mask.</td>
</tr>
<tr>
<td>Ddname</td>
<td>Applies if an access attempt is made for a data set allocated under this volume.</td>
</tr>
<tr>
<td>Until</td>
<td>The last day this entry applies.</td>
</tr>
<tr>
<td>Active</td>
<td>The first day this entry applies.</td>
</tr>
<tr>
<td>Data</td>
<td>Additional information about this entry, for documentation purposes.</td>
</tr>
</tbody>
</table>

6. Press PF8 to view any remaining rule lines and additional rule set explanations. You can also use the standard ISPF keys to scroll forward, backward, and sideways.

---

**IBM Security zSecure ACF2_RULE display**  
Line 27 of 42  
Command ===> _______________________________________________  
Scroll==> CSR_

All rules with HLQ CRM2 9 May 2011 22:10

**Rule attributes**

- Name of this rule set: CRM2
- Roleset access rule: No
- HLQ(s) to which rules apply
- Date of last rule set update: 22Nov2004
- LID that stored rule set: DHOGAN
- SMS ResOwner of rule set: DIANE B HOGAN
- $Owner of this rule set:
- Member wherein to DECOMP rule
- Force use of old compiler
- Site info on this rule set

**Rule attributes subject to GSO**

- Non-standard evaluation order: No
- Action when no entry matches
- UIDs that can change rule set: NCACCMGR-
- UIDs that can change entries

**********************************************************************

**Figure 44. Rule overview display**
Notice the entries in Figure 44 on page 37, such as Rule attributes subject to GSO. You can find valuable information pertinent to rule processing and administration under this heading. See Table 10.

### Table 10. Rule processing and administration attributes

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of this rule set</td>
<td>$KEY of the rule set.</td>
</tr>
<tr>
<td>Roleset access rule</td>
<td>The rule has ROLESET specified.</td>
</tr>
<tr>
<td>HLQ(s) to which rules apply</td>
<td>The $PREFIX of the rule set.</td>
</tr>
<tr>
<td>Date of the last rule set update</td>
<td>Day the rule record was last stored.</td>
</tr>
<tr>
<td>LID that stored rule set</td>
<td>The LID and NAME of the user that last stored the rule.</td>
</tr>
<tr>
<td>SMS ResOwner of rule set</td>
<td>$RESOWNER field in the rule set. SMS uses this.</td>
</tr>
<tr>
<td>$Owner of this rule set</td>
<td>$OWNER field in the rule set. Documentation only.</td>
</tr>
<tr>
<td>Member in which to DECOMP rule</td>
<td>The overriding name of the PDS member into which this rule set should be decompiled.</td>
</tr>
<tr>
<td>Force use of old compiler</td>
<td>If set, this flag field indicates that this rule set is not to be compiled by the long rule compiler under any circumstances. ACF2 has two resource rule compilers to provide support for long resource rules that are over 4kb long. This flag effectively prevents you from using any features in this rule set that require the long rule compiler. The GSO OPTS setting COMPDYN has no influence on this behavior.</td>
</tr>
<tr>
<td>Site info on this rule set</td>
<td>$userdata field if one is present in the rule set.</td>
</tr>
<tr>
<td>Non-standard evaluation order</td>
<td>The rule has $nosort specified.</td>
</tr>
<tr>
<td>Action when no entry matches</td>
<td>If your GSO OPTS record is set to RULE mode, $mode statements will be recognized in rules, if one is present. This could introduce an exposure.</td>
</tr>
<tr>
<td>UIDs that can change rule set</td>
<td>UIDs matching the %change statement if one is present in the rule set.</td>
</tr>
<tr>
<td>UIDs that can change entries</td>
<td>UIDs matching the %rchange statement if one is present in the rule set.</td>
</tr>
</tbody>
</table>

**Audit concerns**

Figure 44 on page 37 and Table 10 display useful information for rule review. Auditing rule administration includes assessment of factors as follows:

- Access to data sets
  - UID strings: the groups or individuals granted access
  - Type of access: read, write, allocate, execute
- Rule administration
  - Who can change the rule set?
  - When did the last rule update occur?
  - Does ACF2 control rule line sorting?

**Suggestions for rule reviews**

Assess the following rule areas carefully and investigate the findings indicated in the descriptions.

- Review $NOSORT settings.
Bypassing ACF2 sorting capability is not recommended. The ACF2 GSO RULEOPTS default sort value is NOSNOSORT (no – do not disable ACF2 sorting). Using the default setting is recommended. Use of $NOSORT in rules can indicate that the GSO RULEOPTS sorting default is disabled. See Table 10 on page 38.

- Review the GSO RULEOPTS CENTRAL/NOCENTRAL and CHANGE/NOCHANGE settings.
  Does the organization desire centralized or decentralized rule administration and should % statements be recognized during rule validation? The presence of % statements in rules can indicate that decentralized rule administration is recognized.

- Determine the MODE of ACF2 designated in the GSO OPTS record, MODE parameter.
  ABORT mode is preferred. The presence of $MODE statements in rules can indicate that the GSO OPTS MODE setting is RULE versus ABORT.

Displaying who last stored a rule

Procedure

1. While still in the rule display panels, type an L in the selection field for LID that stored rule set field as shown in Figure 45.

2. Press Enter.
   The ACF2 LIST OUTPUT panel opens to display the ACF2 logon ID record of the user that last changed the rule set, as shown in Figure 46 on page 40.
Figure 46 is a quick way to view the entire logon ID record of the person that last changed the rule. In Figure 45 on page 39, the logon ID and name are displayed. Use the LIST function L to examine uid string values and assigned privileges.

### Listing rule lines for a specific data set

**Procedure**

1. Press PF3 to return to the Rule Selection panel (Figure 47).
2. Type a data set name in the Match data set field. Use a data set name that applies to your environment. Figure 47 uses CRM2.VENDOR.ACCTS.
3. Type a / character beside Show rule lines.
4. Press Enter.
5. Remove the / beside By rule set.

---

**Figure 46. ACF2 LIST OUTPUT panel**

To understand the next display in Figure 48 on page 41, notice the headings DSN mask and UID mask.
6. Press PF11 to view the $Key column heading (Figure 49).

7. Analyze the $Key column before continuing. Rule line permissions can be taken out of context if the $Key column is not reviewed.

The $Key column shows two values: CRM2 and CRM2LAST. Notice the rule line entries associated with each $Key value. CRM2 is the parent rule set. CRM2LAST is a NEXTKEYed rule set. To understand how CRM2LAST is used, see Figure 59 on page 48 and Figure 61 on page 49.

Access for the data set CRM2.VENDOR.ACCTS is determined by the first three rule lines in Figure 48. In this example, the following access settings are in place:

- Users in the group **PUR (which means any location, department PUR) can Read, Write, and Execute against the CRM2.VENDOR.ACCTS data set.
- Users in the group **ACC (which means any location, ACC department) can Read and Execute CRM2.VENDOR.- data sets, that is, all data sets that have the first two qualifiers.
- All users (uid of -) do not have any access to any data set that begins with CRM2.

Each rule line becomes less specific. After the requested access matches a rule line, ACF2 rule processing stops. Therefore, it is important not to misinterpret individual rule lines in Figure 48 and Figure 49. These rule lines are associated with the parent rule set CRM2. CRM2 is the only rule set that controls access to our sample data set name.

Figure 50 on page 42 shows the entire parent rule set CRM2. Note the location of each rule line that matches CRM2.VENDOR.ACCTS data set name. The order goes from most specific to least specific. Understand that these three rule lines are the only ones that affect access to the CRM2.VENDOR.ACCTS data set. The
NEXTKEYed rule sets in Figure 49 on page 41 do not affect access.

8. To shift the information left, press PF10.

Analyzing data set access

Your screen should be similar to Figure 51 on page 43 with the column headings DSN mask, UID mask, and User. Nine entries in the CRM2 rule set match the data set name CRM2.VENDOR.ACCTS. The data set rule lines in Figure 51 on page 43 are in sort order from most specific to most generic.

Understanding that only the first three entries are important due to the $Key column (shown in Figure 49 on page 41 and Figure 52 on page 43), the last six entries are ignored when determining access.

In this example, only two groups, PURchasing and ACCounting, can access the CRM2.VENDOR.ACCTS data set.
Follow the data set line to the UID mask column. Press PF11 to scroll and view the permissions (Perm) column.

The Perm column indicates that the group **PUR- is allowed to read, write, and execute against the data set. The group **ACC is allowed to read and execute against the data set through the masked entry CRM2.VENDOR.-. The last entry indicates that everyone, UID (-), is prevented access to any other CRM2 data set, which is referred to as a stopper or prevent rule line entry.

- Everyone in group **PUR- is allowed to read, write, and execute
  - ** indicates any location - LOC(**) in the sample UID string
  - PUR indicates the department - DEPT(PUR) in the sample UID string
- Everyone in group **ACC is allowed to read and execute
  - ** indicates any location – LOC(**) in the sample UID string
  - ACC indicates the department – DEPT(ACC) in the sample UID string
- No other access is allowed due to the UID(-) rule line. No other users have access to the CRM2.VENDOR.ACCTS data set.

Figure 51 on page 49 helps explain this example. Understanding rule structure is critical in access analysis. During ACF2 rule processing, the VENDOR data set access is determined in the parent rule set CRM2. See the V entry in Figure 51 on page 49.

**Listing data set rule lines specific to a uid string**

**About this task**

To find all data set access for a group or individual, you must specify a uid string.
Procedure
1. Press PF3 to return to the Rule Selection panel [Figure 53].
2. Type a uid string appropriate to your environment in the UID String field. Our example uses NEACC-. This is interpreted as location NE and all users in the accounting department (ACC), which is specific to our uid string. Make sure to include the dash (-) character at the end of the uid string.
3. Type a forward slash (/) character to treat the uid string as an ACF2 mask.

**Important:** Without the Treat as ACF2 mask indicator, the search treats the uid entry as a literal.
4. Type a forward slash (/) character to indicate display rule line.
5. Press Enter.

When selecting rules lines by uid string without selecting the **Treat as ACF2 mask** option, only those entries that match the specified uid string exactly are selected. Masking characters are treated as literals in this case. For example, our uid string example of NEACC- targets all users in the ACC department that are in location NE (the Netherlands). The dash (-) designates inclusion of uid entries in a rule line with NEACC and any other trailing characters. The forward slash (/) directs zSecure Audit for ACF2 to treat the dash as a mask versus a literal. There are no uid strings entries in our database with a dash. If the dash was treated as a literal, no matches would be found.

If the **Treat as ACF2 mask** option is selected, all entries that are at most as specific as the specified mask are selected. Embedded blanks are not supported if the **Treat as ACF2 mask** option is selected.

[Figure 54 on page 45] and [Figure 55 on page 45] show the results of the search requested in [Figure 53]. All users with a uid string of NEACC can access data sets listed under the **DSN mask** column.
6. Press PF11 to shift right and view the type of access in the Perm column. The lowercase letters indicate allow and log. In this case, the w lowercase letter indicates that write access is allowed and logged to SMF for review.

To understand access to the data sets in Figure 55, the $Key column must be analyzed. NEXTKEY processing effects how the data set access is granted. Figure 54 and Figure 55 show that users with a matching uid mask of NEACC- have read and execute access to any CRM2.- data set. This is not accurate for our sample rule. See Figure 61 on page 49 to understand the structure of the CRM2 rule set. In our sample rule, NEACC- users do not have read access to any CRM2.- data set.

Important: Do not analyze rules out of context.

This entry resides in the NEXTKEY rule set CRM2LAST (Figure 53 on page 44). This access is used only if no matches are found in rule lines processed before CRM2LAST.

**Displaying NEXTKEYs in data set rules**

**About this task**

NEXTKEYs can be displayed through various panel selections, such as:

- Native ACF2 List display as in Figure 50 on page 42
- Use of the Other fields option as in Figure 56 on page 46
- Use of the Expand nextkey option as in Figure 63 on page 51
**Procedure**

To view NEXTKEYs chained to a parent rule set, complete the following steps:

1. Press PF3 to return to the Rules Selection panel.
2. Type a high-level qualifier appropriate for your environment. The example shown in Figure 56 uses CRM2.
3. Type a forward slash (/) character beside **Other fields**.
4. Type a forward slash (/) character beside **Show rule lines**.
5. Press Enter.

---

**Specifying additional selection criteria**

**About this task**

The **Specify additional selection criteria** section in the Rules Selection panel enables specific rule search criteria. There are a number of approaches to view NEXTKEYs; using additional selection criteria is one approach.

Other types of inclusion criteria such as rule permissions can be requested. You can think of these as filtering mechanisms when analyzing specific rule issues.

In the Rules Selection panel shown in Figure 57 on page 47 select the NEXTKEY criteria:

**Procedure**

1. Move down to the bottom of the panel.
2. Move over to the **NEXTKEY** field.
3. Type a forward slash (/) character in the selection field for NEXTKEY.
4. Press Enter.
Results

Figure 58 is the display result for all NEXTKEYs chained from the parent rule set of CRM2.

There are four NEXTKEYed rule sets within the rule CRM2 as indicated in the NextKey column: CRM2D, CRM2M, CRM2PROD, and CRM2LAST. Access for data sets with the high-level qualifier of CRM2 is contained in the parent CRM2 and the NEXTKEYed (children) rule sets. A graphical view of the CRM2 structure is depicted in Figure 61 on page 49. Comparing the graphical structure with Figure 59 on page 48 can help you to understand the display.
The entries in the DSN mask column shown in Figure 59 are rule lines in the parent rule set CRM2. These rule lines contain NextKey parameters that direct ACF2 to a separate rule set for further rule validation processing.

In this example, the data set name mask CRM2.D-. points ACF2 to the rule set CRM2D. A request for any data set name that matches the CRM2.D-. , such as CRM2.DAILY.BACKUP causes ACF2 to search the child rule set, CRM2D, for a data set name match. The child rule set, CRM2D, contains data set access rule lines for CRM2.D-. data set names. Access for any data set matching the mask of CRM2.D-. is in the child rule set CRM2D.

The $Key column contains the rule set key from which the NextKey column reference originates. For example, the CRM2D NEXTKEY originates in the parent rule set CRM2. The CRM2LAST NEXTKEY originates from the CRM2D, CRM2M, and the CRM2PROD rule sets.

The DSN mask column entry contains the rule line that points to the NEXTKEY rule set shown in the $Key column. For example, the rule line CRM2.D-. points to a NEXTKEY labeled CRM2D:

```
CRM2.D-. UID(*) NEXTKEY(CRM2D)
```

Review the diagrams in Figure 61 on page 49 for a visual reference of the data set names, NEXTKEY, and $KEY relationships.

**Figure 59. NEXTKEYs for requested high-level qualifier**

**Data set rule structure and NEXTKEYs**

In Figure 61 on page 49 the parent rule set CRM2 has three NEXTKEY statements that point to child rule sets CRM2D, CRM2M, and CRM2PROD.

Child rule sets CRM2, CRM2M, and CRM2PROD point to child rule set CRM2LAST. This is a common rule chaining structure. Use the example in Figure 61 on page 49 to understand the NEXTKEY display in Figure 59.
Displaying rules lines in expanded NEXTKEY format

About this task

An easier approach to displaying NEXTKEYs is provided by the Expand nextkey option in the Rules Selection panel. See the previous rule example in “Data set rule structure and NEXTKEYs” on page 48 for the rule set CRM2. The following procedure shows an alternate approach to viewing NEXTKEYs for our rule set example.

Procedure

1. To use the expanded NEXTKEYs function, complete the steps in “Using the expanded NEXTKEYs function” on page 50.

2. To review the expanded NEXTKEY rule lines for each X line, complete the steps in “Reviewing the expanded NEXTKEY rule lines for each X line” on page 54.

Figure 62 on page 50 shows the native ACF2 List display of the parent rule CRM2. The NEXTKEY statements are difficult to locate and you must list the child rules separately to view their rule lines. The expanded NEXTKEY function places structural information about one screen, making it much easier to view rule structure.
Using the expanded NEXTKEYs function

About this task

The **Expand nextkey** option in the Rules Selection panel provides an easy approach to displaying NEXTKEYs.

**Procedure**

1. In the Rules Selection panel, type the high-level qualifier in the **data set HLQ** field. This example uses CRM2.
2. Select the **Show rule lines** option by using the forward slash (/) character.
3. Select the **Expand nextkey** option by using the forward slash (/) character.
4. Press Enter to view the results as shown in Figure 64 on page 52.
Figure 64 shows another view of the entire parent rule set CRM2. This display has an additional column X for NEXTKEYed rule lines. The column indicates whether the rule line has an expanded NEXTKEY that you can view in more detail. Each line with an X directs ACF2 rule processing to another rule set, the child rule, for further rule validation processing.

To understand the NEXTKEY concept, recall the previous example of the CRM2 rule. The parent CRM2 contains three NEXTKEY statements, pointing to three
child rule sets, CRM2D, CRM2M, and CRM2PROD (Figure 65). These child rule sets contain a NEXTKEY statement that points to CRM2LAST, the catchall for all other CRM2 data sets. Figure 65 illustrates this example.

Figure 65. Rule structure

Figure 66 on page 54 is an abbreviated display of only the NEXTKEYed rule lines for ease in understanding the X column. Only the X columns are shown in Figure 66 on page 54. This example is for demonstration purposes only. The NEXTKEY entries in Figure 66 on page 54 match the entries in Figure 64 on page 52 and Figure 65. These figures are different views of the same rule.
Reviewing the expanded NEXTKEY rule lines for each X line

Before you begin

Complete the procedure described in "Using the expanded NEXTKEYs function" on page 50.

Procedure

1. Type the selection character S beside the line you want.
2. Press Enter to open the display panel shown in Figure 67.

In this example, CRM2 points to CRM2D, which points to CRM2LAST.

Results
The **Expand nextkey** option represents a visual of the rule set structure by expanding each NEXTKEY statement. The NEXTKEYs are indented, showing the relationship from parent rule to child rule and also the applicable data set name or data set name mask.

**Figure 67 on page 54** shows an example of an expanded NEXTKEY showing the **$Key** column with CRM2 as the parent rule and the indented entries underneath. This example has the following characteristics:

- The parent rule CRM2 has the NEXTKEY(CRM2D) for the data set name mask of CRM2.D-.-. Rule validation for these data sets is determined by the child rule CRM2D.
- The CRM2D indented entries are the actual CRM2D child rule set for all the data sets that match the mask. Data set access for these data sets are controlled in the child rule, CRM2D.
- CRM2D has the NEXTKEY(CRM2LAST) for all other CRM2.DAILY.- data set access. Rule validation for any of these data sets is determined by the child rule CRM2LAST.

The expanded NEXTKEY function also provides the following additional information:

- Evaluation order
- Action on match
- Rule attributes
- Rule attributes subject to GSO

In **Figure 68 on page 56** the **Sequence number** field indicates that the rule line displayed is number 8 within the parent rule.

D-.-. UID(*) NEXTKEY(CRM2D)
Viewing individual data set rule lines

About this task

You can view individual rule lines by specifying the high-level qualifier.

Procedure

To view individual rule lines, complete the following steps:

1. Press PF3 to return to the Rules Selection panel.
2. Type a high-level qualifier in the Data set HLQ field.
   The last high-level qualifier requested remains present in this field. The example in Figure 69 on page 57 uses the qualifier CRM2
3. Leave the forward slash (/) character in the Show rule lines field as shown in Figure 69 on page 57

The expanded NEXTKEY provides a great visual for understanding rule structures. Without this capability, NEXTKEY branching is difficult to follow.
4. Press Enter to open the Rule display panel shown in Figure 70.

In the Rule display panel (Figure 70), you can select a specific rule line to view more information or press PF11 to scroll sideways. Selecting a specific rule line displays additional information that is not available when scrolling sideways.

In Figure 71 on page 58, you can view detailed information for the selected rule line CRM2.HELP.FILES.
The RuleEntry heading provides the following information:

- The data set name is specified.
- The uid string is listed.
- All users in the location NE and the department HLP can read, write, and execute against the CRM2.HELP.FILES data set.

Any other environmental parameters would be listed in this section alongside the corresponding item. This example does not have additional environmental parameters.

To view the remaining rule line details, press PF8 until you see Bottom of Data.

### Viewing a resource rule

#### About this task

You can view and analyze resource rules by using capabilities similar to those used for viewing and analyzing data set rules.
Procedure

To work with resource rules, complete the following steps:

1. Press PF3 to return to the Main menu.
2. Type I, which is Resource rule overview, in the Option line as shown in Figure 72.
3. Press Enter to open the Resource panel.
4. To view all resource rule types, complete the following steps:
   a. In the Resource panel, type three asterisks (*** in the Resource type field to mask it as shown in Figure 73.
   b. Press Enter.

Figure 72. Select Resource rules overview

Figure 73. Mask the resource type field to view all resource types
Resource rules contain a two-part key: the resource name and the resource type code. The type code is always three characters and is descriptive of the type or category of resource rule. For example, the OPR type code represents Operator Commands. Resource rules with this type code control the use of JES and MVS operator commands.

Figure 74 displays a list of all resource type codes for our sample ACF2 database. Masking the resource type field provides an excellent starting point for analysis of resource rules. Notice the column heading #Rules. The example shows that there are 56 resource rules with a type code of FAC (Facility rules). There are also three resource rules with a type code of OPR (Operator Command rules), and six resource rules with a type code of PDS (Partitioned data set rules).

![Resource Rule Type Codes Table]

Resource rules can also be shown by providing the MVS eight-character resource class name, such as OPERCMDS and a uid string as shown in Figure 75 on page 61. This selection criteria finds the users who have access to the MVS eight-character resource class name - OPERCMDS uid(........) within the uid NESYSPRG.
Chapter 4. Infostorage records

The following topics describe how to view Scope and cross-reference records through zSecure Audit for ACF2. These records are stored in the Infostorage database and are not resource rules. They are definitions of relationships.

Use the Infostorage functions to perform the following tasks:

- Review SCOPE records – SCOPE(SCP)
- Review cross-reference records – XREF(RGP), XREF(SGP), and XREF(ROL)

Infostorage record types and attributes

The Infostorage database contains definitions and resource rules. As described in Chapter 1, “Overview,” on page 1, the Infostorage database is like a filing cabinet with many drawers. Each drawer has the following attributes:

- Uniquely labeled, containing a special type of record such as resource rules, scope records, and cross-reference records.
- Identified with a Class value to represent the drawer contents. See Table 11.
- Can contain multiple folders, each with a unique three-character type code to further identify the contents.

Table 11 lists the InfoStorage database class values and descriptions. You can think of each row, or class, of the table as representing a drawer in the database.

<table>
<thead>
<tr>
<th>ClassValues</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Description Control records</td>
</tr>
<tr>
<td>D</td>
<td>DB2 records</td>
</tr>
<tr>
<td>E</td>
<td>Entry records</td>
</tr>
<tr>
<td>F</td>
<td>Field records</td>
</tr>
</tbody>
</table>
Table 11. InfoStorage database class values and descriptions (continued)

<table>
<thead>
<tr>
<th>ClassValues</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Identity records</td>
</tr>
<tr>
<td>M</td>
<td>Mandatory Access Control</td>
</tr>
<tr>
<td>P</td>
<td>Profile records</td>
</tr>
<tr>
<td>R</td>
<td>Resource Rule records</td>
</tr>
<tr>
<td>S</td>
<td>Scope records SCP</td>
</tr>
<tr>
<td>T</td>
<td>Shift records</td>
</tr>
<tr>
<td>V</td>
<td>ACF2/VAX records</td>
</tr>
<tr>
<td>X</td>
<td>Cross-reference records SGP, RGP, ROL</td>
</tr>
</tbody>
</table>

This table provides an overview of the records in the InfoStorage database. For zSecure Audit for ACF2, the records of interest are the Scope and cross-reference records, which have the following characteristics:

- Scope records have a type code of SCP.
  - SCOPE records reside in the S drawer or class of the Infostorage database as shown in Table 11 on page 61.
- Cross-reference records have three types: RGP, SGP, and ROL.
  - Cross-reference records reside in the X drawer or class of the Infostorage database as shown in Table 11 on page 61.
    - RGP records are resource groups.
      - Resource groups represent resource rules that are grouped for ease in rule writing.
    - SGP records represent source groups.
      - Source groups are used to control access to a resource such as an application, system entry, or a transaction. Access to a resource can be controlled through a Logon ID field or a rule.
    - ROL records represent role groups.
      - Role groups are used to aggregate users and separately aggregate accesses to functions, and then relate user access to the performance of those functions.

Viewing scope records

About this task

ACF2 Scoping provides control over the security administrative Logon ID privileges: SECURITY, ACCOUNT, and AUDIT.

Scoping is used to limit administrative capabilities of these powerful Logon ID privileges against the Logon ID, Rules, and Infostorage databases and data access. Scoping is site-defined through ACF2 Infostorage SCOPE records and the related SCPLIST field in the Logon ID record. Typically, the security administrative staff maintains these controls.

To view scope records, complete the following steps:

Procedure

1. Press PF3 to return to the Main menu.
2. **From the Main menu**, type S in the Option command line, as shown in [Figure 76](#).

![Figure 76](#)

*IBM Security zSecure Audit for ACF2 - Main menu*

<table>
<thead>
<tr>
<th>Menu</th>
<th>Options</th>
<th>Info</th>
<th>Commands</th>
<th>Setup</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Option ====&gt;</td>
<td>S</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

More: +

SE  Setup  Options and input data sets
AA  ACF2  ACF2 Administration
L  Logonid  Logonid overview
R  Rules  Rules overview
I  Resource  Resource rules overview
S  Infostorage  Infostorage record overview
C  Custom  Custom report
AU  Audit  Audit security and system resources
RE  Resource  Resource reports
EV  Events  Event reporting from SMF and other logs
CO  Commands  Run commands from library
IN  Information  Information and documentation

5655-N17 IBM Security zSecure Audit for ACF2 2.1.0

*Figure 76. Select Infostorage record overview*

3. **Press Enter** to open the Infostorage panel shown in [Figure 77](#).

On this panel, you specify selection criteria for Scope (SCP), cross-reference resource group (X-RGP), cross-reference source group (X-SGP), and cross-reference role (X-ROL) Infostorage records.

![Figure 77](#)

*IBM Security zSecure Audit for ACF2 - ACF2 - Infostorage*

<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>-------------</td>
</tr>
<tr>
<td>Command ===&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Show infostorage records that fit all of the following criteria

Record key . . . . . (record name or ACF2 mask)
Complex . . . . . . . . (complex name or ACF2 mask)

Select the infostorage record types you want to display
- Scope (S-SCP) records
- Cross-reference resource group (X-RGP) records
- Cross-reference source group (X-SGP) records
- Cross-reference role group (X-ROL) records

Additional selection criteria
- Other fields

Output/run options
- Print format  Custom title  Send as email
  - Background run  Form oriented  Sort differently  Narrow print

*Figure 77. Infostorage record selection criteria.*

4. **To view the scope records**, enter S in the selection field for the Scope (S-SCP records) option. Then press Enter to display the panel shown in [Figure 77](#) on page 64.
Figure 78 shows a list of scope records. The ResT column shows the class value of S and a type code of SCP. The Key column displays the record name such as PAYROLL. You can define controls for security administration over Payroll resources within this scope record.

5. To view an individual Scope record, complete the following steps: “Viewing an individual Scope record”

Viewing an individual Scope record

Procedure

1. In the Scope record list panel, tab down in the ResT column and type S in the selection field for one of the records. Then press Enter. In the example shown in Figure 79, the SSCP COSTING record is selected.

2. Press Enter to open the display panel as shown in Figure 80 on page 65
Figure 80 shows the definition for scope record COSTING. This definition controls security administration for any of the following privileges:

- Logon ID with the naming convention of CRM2
- UID string that starts with COST
- Data sets with a high-level qualifier that starts with COST

### Viewing cross-reference records

**Procedure**

1. Press PF3 to return to the Infostorage panel.
2. Tab down to the Cross-reference resource group (X-RGP) records option; type / in the selection field as shown in Figure 81.
3. Press Enter to display the list of cross-reference resource group records as shown in Figure 82 on page 66.

This panel shows the list of cross-reference records for class X and type RGP resource groups.
4. To view an individual cross-reference group record, complete the following steps: "Viewing an individual cross-reference group record"

**Viewing an individual cross-reference group record**

**Procedure**

1. In the cross-reference group record list panel, tab down in the **ResT** column and type S in the selection field for one of the records.

   In the example shown in [Figure 82](image), the XRGP ACCOUNTS record is selected.

2. Press Enter to open the display panel as shown in [Figure 83](image).
Figure 83 on page 66 shows the detail for the cross-reference record ACCOUNTS. Notice the entries under the Record attributes section. ACCOUNTS is a Grouping record, which means that it is a group of groups. The groups defined to ACCOUNTS are ACCTPAY and ACCTREV. These groups are listed under the Include section.

The groups ACCTPAY and ACCTREV are most likely resource rules for CICS transactions. Resource groups are used to reduce the number of resource rules. By grouping transactions under a group name and by grouping groups of groups under a cross-reference record, fewer rules are needed to control access to the CICS transactions.
Chapter 5. SETUP functions for data management

The SETUP functions control which data is used by zSecure Audit for ACF2. With them, you can switch data sources while using the products. Other SETUP functions set global switches and parameters. The following section addresses several SETUP options that are most important to your evaluation.

Inputting data

About this task

So far, you used only your live ACF2 data to display various profiles. This procedure shows how to create the additional data sources:

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

Procedure

To create the data sources, complete the following steps:

1. Return to the Main menu. Press PF3 if necessary.
2. In the Option command line, type **SE** to select the Setup option.

The Setup menu shown in **Figure 84** is displayed.

```
Menu Options Info Commands Setup
0 Run Specify run options
1 Input files Select and maintain sets of input data sets
2 New files Allocate new data sets for UNLOAD and CKFREEZE
3 Preamble Carla commands run before every query
7 Output Specify output options
8 Command files Select and maintain command library
B Collections Select and maintain collections of input sets
U User defined User defined input sources
C Change Track Maintain Change Tracking parameters
N NLS National language support
T Trace Set trace flags and CARLa listing for diagnostic purposes
D Default Set system defaults
R Reset Reset to system defaults
```

**Figure 84. Setup menu**

Inputting new files

Procedure

To input new files, complete the following steps:

1. From the initial Setup menu (**Figure 84**), select **Option 2** to open the New files panel, as shown in **Figure 85 on page 70**
2. Type a data set name in the **Unload** line.
   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 currently exist. However, if they do exist, they must be cataloged.

3. Type a short, unique description of the files in the third input 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. Completing this field can prevent the need to later open the set in browse or edit mode to examine which data sets are included.

4. Press Enter.
   If any of the data names you specify do not exist, the New files panel shown in **Figure 86** is displayed to allocate and catalog the new data sets.

5. Type a data set name in the **CKFREEZE** line; use quotation marks if necessary.
6. Type the appropriate allocation parameters, but do not change the DCB attributes.

7. Press Enter.

If both named data sets are new, you see the allocation panel a second time. Executing these panels allocates and catalogs your new data sets using dynamic allocation. The first time you create an unloaded ACF2 copy and a CKFREEZE data set, be sure to specify ample disk space. For ACF2, allow as much space as used by your live ACF2 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 gigabyte 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 Audit for ACF2: 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 creating your first unloaded ACF2 copy and CKFREEZE data sets, examine them with ISPF to determine how much disk space was used. This information makes future usage easier.

After the files are allocated, you see the panel shown in Figure 87.

---

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 ACF2 unload, or multiple ACF2 data sets (the components of a single ACF2 system).

Procedure

To refresh and load files, complete the following steps:

1. In the Input file panel as shown in Figure 87, type REFRESH in the command line. Then press Enter to display the Job submission panel.

2. In the Job submission panel, type a valid job card in the Job statement information section.

3. Use Edit JCL Option (2) to open the 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 in order to access the product. If you
copied zSecure Collect (CKFCOLL) to an authorized library in the LNKLST, you do not need a JOBLIB or STEPLIB for it. Assign a job class with a large or unlimited region size.

4. Submit the job.

5. Wait until the job runs.
   If there is a long queue of jobs that are waiting to run, you might want to exit from the product while the job completes. The job itself takes only a minute or two 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. zSecure Collect can use regions in excess of 32 MB. If the zSecure Collect step fails and you provided the largest region size you can obtain, refer to Appendix B, “zSecure Collect memory requirements,” on page 133.

Selecting the input set

Procedure

1. To open the Input file panel, type SE.1 in the Command line, which is Option 1 in the Setup menu.
   The Input file panel should look like the input set you created, with the description you entered for the input files. An example is shown in Figure 88.

2. You can use the following 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(r) 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 (Figure 84 on page 69).
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.

   ![Figure 89. Setup collections definition panel](image)

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

   ![Figure 90. Setup collections display](image)

   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:

```
Menu Options Info Commands Setup
Command ====> zSecure Suite - Setup - Collections Row 1 from 6

Description .. Collection for systems of SYSPLEX TEST
(Un)select (U/S/C/M) input sets to be added to or removed from collection

Description
  - CKFREEZE for system TST1 selected
  - CKFREEZE for system TST2 selected
  - CKFREEZE for system TST3 selected
  - CKFREEZE for system PRD1
  - CKFREEZE for system PRD2
  - CKFREEZE for system PRD3

*********************************************************************** Bottom of data ********************************************************************************
```

Figure 91. 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.
Chapter 6. Security control analysis

This topic describes how to view audit concerns generated by zSecure Audit for 
ACF2. It provides information for determining how well the Global System 
Options are implemented and flags abuse of powerful Logon ID privileges. It also 
provides various password control reports, and presents a broad view of access by 
trusted users.

Use the Audit functions to review:
- GSO records
- CLASMAP records
- ACF2 field Definition Entries (ACFFDR @CFDR macros)
- Logon IDs with powerful privileges
- Password aging
- Password intervals
- Logon IDs without passwords
- Logon IDs with expired passwords
- Logon IDs that have never been used
- Logon ID last logon
- Access available to trusted users
- Sensitive data set controls
- UNIX System Services support

Audit concerns

The Audit section provides valuable information about the Global System Options 
defined in the Infostorage database.

To select the Audit function, complete the steps in “Selecting the Audit function.”

To view audit concerns detected by zSecure Audit for ACF2, complete the steps in 
“Viewing audit concerns detected by zSecure Audit for ACF2” on page 76.

To review the audit concerns overview by priority, complete the steps in 
“Reviewing audit concerns overview by priority” on page 77.

Selecting the Audit function

Procedure
1. Press PF3 to return to the Main menu as shown in Figure 92 on page 76.
2. Type AU in the command line to work with the Audit security and system 
resources.
3. Press Enter.
4. To select status, type S in the command line as shown in Figure 93.

5. Press Enter to open the Audit panel.

### Viewing audit concerns detected by zSecure Audit for ACF2 Procedure

1. In the Audit panel, tab to the ACF2 control heading.
2. Type the / character beside the ACF2 control field as shown in Figure 94 on page 77.
3. Move to the bottom of the screen.
4. Type the / character beside the Include audit concern overview, higher priorities only field as shown in Figure 94 on page 77. Press Enter.
The resulting screen shown in Figure 95 presents selections for review:
OVERVIEW, GSO, GSOAUDIT, CLASMAP, and FDE. The following examples focus on OVERVIEW and GSO audit displays.

**Reviewing audit concerns overview by priority**

**Procedure**

Follow these steps to open the Audit concern overview panel:
1. In the ACF2 Display Selection panel, tab to the Overview record.
2. To select the record, type S in the selection field.
3. Press Enter to open the Audit concern overview panel. For information about using this panel, continue with the next section.

**Audit concern overview by priority**

IBM Security zSecure Audit for ACF2 lists the audit concerns by priority and provides a description of the findings. The Audit concern overview display as shown in Figure 96 on page 78 identifies the most important audit concerns across all systems, sorted by numerical audit priority. Each line describes a single audit concern with the audit priority, complex, system, area, that is, GSO records, key and current value, that is, parameter and setting, and a description of the audit concern.
The numerical audit priorities shown in Figure 96 indicate the severity of the audit concerns identified.

<table>
<thead>
<tr>
<th>Priority</th>
<th>GSO record parameter</th>
<th>Parameter setting</th>
<th>Audit concern</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PSWD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0-10</td>
<td>informational</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10-20</td>
<td>desired</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20-40</td>
<td>review required</td>
<td></td>
<td></td>
</tr>
<tr>
<td>40 and up</td>
<td>serious exposure</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In Figure 96, the Overview audit concerns indicate multiple problems about GSO record settings. Table 12 lists the audit priority values and the associated meaning.

**Table 12. Audit Priority values**

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-10</td>
<td>informational</td>
</tr>
<tr>
<td>10-20</td>
<td>desired</td>
</tr>
<tr>
<td>20-40</td>
<td>review required</td>
</tr>
<tr>
<td>40 and up</td>
<td>serious exposure</td>
</tr>
</tbody>
</table>

An understanding of the individual GSO records can be helpful in evaluating the audit concerns listed in the overview panel. There are multiple GSO records, such as OPTS, PSWD, RULEOPTS, and BACKUP. The actual GSO record name, PSWD, for example, does not display in the Audit concern overview panel. However, you can obtain the GSO record name for any necessary follow-up by using native ACF2 commands (see Figure 97 on page 79), or from the GSO System Settings panel (Figure 101 on page 80, Figure 102 on page 81, and Figure 103 on page 82).

The following information explains the sample audit concerns in Figure 96:

- The GSO PSWD record contains multiple parameters, some of which are listed in the Key column of Audit concern overview panel. The GSO System Settings panel as shown in Figure 101 on page 80 provides another view of the GSO parameters and settings listed in the Key column. Some parameters hold a value, that is, a number, and others act as ON and OFF switches.

The PSWD record parameter PSWDJES is set as N for no or off. In native ACF2 commands, this setting displays as NOPSWDJES as shown in Figure 97 on page 79. This value is the default value for the PSWD parameter.

The audit concern shown in the Overview panel notes that password guessing through batch processing is possible due to the default setting of the parameter PSWDJES. This default setting is not recommended because password guessing through batch processing goes undetected. To prevent password hacking through batch jobs, change the value of PSWDJES to Y for yes or on. In native ACF2 commands, this setting displays as PSWDJES.
For details on changing GSO record values, see the information about the native command GO PSWD provided in Figure 98 and Figure 99 and the GSO System settings information shown in Figure 105 on page 84.

- Recommended GSO PSWD settings are: MINPSWD(6), PSWDJES, PSWDHST, PSWDLID, PSWDNUM, PSWDREQ, PSWDRSV, PSWDFTC, PASSLMT(3), MAXTRY(3), PSWDALPH, PSWDNMIC, PSWDMIN(1), PSWDPAIR(2), PSWDSIM(3), PSWDNAGE, PSWXHIST, PSWXHIST(#9). These settings are set to YES or ON or assigned a value (values are noted with a number inside a parentheses such as MINPSWD). A NO or N displayed with the parameter indicates that the setting is off or set to NO, that is, PSWDJES.

- The GSO OPTS JOBCHK/NOJOBCHK parameter is set to NOJOBCHK, the default setting. The recommended value is Y, for yes. This value prevents anyone with TSO access from submitting a batch job unless the JOB privilege is present in the Logon ID. Changing the parameter to Y displays JOBCHK.

The GSO System Settings panel (as shown in Figure 101 on page 80, Figure 102 on page 81, and Figure 103 on page 82) provides a comprehensive and easy to understand display of the GSO record settings. In contrast, viewing GSO records using ACF2 native commands as shown in the following examples is tedious and requires a knowledge of commands and syntax. In the example shown in Figure 97 you need to issue the set control (gso) command to point to the Infostorage GSO records, before you can issue the list pswd command.

```
set control(gso)
CONTROL
list pswd
    PROD / P Swd LAST CHANGED BY JSMITH ON 11/26/00-14:31
    MAXTRY(2) MINPSWD(5) PASSLMT(4) PSWDALT PSWDHST NOPSWDJES NOPSWDLID NOPSWDNCH NOPSWDNUM PSWDREQ NOPSWDRSV NOPSWDXTR WRNDAYS(1)
```

Figure 97. ACF2 native command to list all GSO PSWD record parameter settings

In response to the audit concerns detected through zSecure Audit, changes to ACF2 GSO record values require the use of ACF2 native commands. For example, you must issue the SET CONTROL (GSO) command to point to the Infostorage GSO records before you issue the CHANGE PSWD command with the correct syntax, as shown in Figure 98.

```
SET CONTROL(GSO)
CHANGE PSWD PSWDHST PSWDJES
```

Figure 98. ACF2 native command to change GSO PSWD record parameter settings

Finally, you must issue the ACF2 REFRESH command shown in Figure 99 to make the GSO changes effective immediately.

```
F ACF2, REFRESH(PSWD)
```

Figure 99. Native command to make GSO PSWD changes effective immediately

**Viewing GSO system settings**

**About this task**

Review the GSO system settings in detail.
Procedure

1. Press PF3 to open the ACF2 Display Selection panel as shown in Figure 100.
2. In the ACF2 Display Selection panel, tab to the GSO record.
3. To select the record, type S in the selection field as shown in Figure 100.

4. Press Enter to open the GSO system settings panel as shown in Figure 101.

   This panel shows the GSO system settings in an easy-to-read format with settings categorized by type such as Option settings (OPTS) and Backup parameters (BACKUP).

   The display might span several screens as shown in Figure 101, Figure 102 on page 81, and Figure 103 on page 82. Press PF7 or PF8 to scroll up or down.

   For additional information about these settings, see “Global System Options” on page 82.

---

**Figure 100. Select GSO system settings**

---

**Figure 101. GSO system settings (Screen 1)**
## GSO System Settings (Screen 2)

### Password Settings (PSWD)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum tries MAXTRY</td>
<td>2</td>
</tr>
<tr>
<td>Minimum length MINPSWD</td>
<td>5</td>
</tr>
<tr>
<td>Daily pswd limit PASSLMT</td>
<td>4</td>
</tr>
<tr>
<td>Warning days WARN DAYS</td>
<td>5</td>
</tr>
<tr>
<td>Default MaxDays PSWDMAX</td>
<td></td>
</tr>
<tr>
<td>Check pswd history PSWDSH</td>
<td>Yes</td>
</tr>
<tr>
<td>Default MinDays PSWDMIN</td>
<td></td>
</tr>
<tr>
<td>Effective pswd history #</td>
<td>4</td>
</tr>
<tr>
<td>JES updates Pswd-Vio PSWDOJES</td>
<td>No</td>
</tr>
<tr>
<td>Extended pswd hist PSWXHIST</td>
<td>No</td>
</tr>
<tr>
<td>Force pswd change PSWDFRC</td>
<td>Yes</td>
</tr>
<tr>
<td>Extended pswd hist # PSWXHIST#</td>
<td>0</td>
</tr>
<tr>
<td>Change pswd at logon PSWDALT</td>
<td>Yes</td>
</tr>
<tr>
<td>Similar char checking PSWDSIM</td>
<td>2</td>
</tr>
<tr>
<td>Volatile temp pswds PSWNAVAGE</td>
<td>No</td>
</tr>
<tr>
<td>Extract password PSWDXTR</td>
<td>No</td>
</tr>
<tr>
<td>Allow ACF Ch pswd PSWDCH</td>
<td>Yes</td>
</tr>
<tr>
<td>Pswd=LID allowed NOPSWDLID</td>
<td>Yes</td>
</tr>
<tr>
<td>New LIDs need pswd PSWDREQ</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow all-numeric NOPSWDNUM</td>
<td>No</td>
</tr>
<tr>
<td>Allow password verify PSWDFVY</td>
<td>No</td>
</tr>
<tr>
<td>Use RESWORD table PSWDRSV</td>
<td>Yes</td>
</tr>
<tr>
<td># consecutive PSWDPAIR</td>
<td>1</td>
</tr>
<tr>
<td>Req alphabetic char PSWDAH</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow vowels PSWOVOWL</td>
<td>Yes</td>
</tr>
<tr>
<td>Req numeric char PSWDNMC</td>
<td>Yes</td>
</tr>
<tr>
<td>Case-sensitive pswds PSWDMXED</td>
<td>No</td>
</tr>
<tr>
<td>Req nat./special char PSWDSPLT</td>
<td>No</td>
</tr>
<tr>
<td>Pswd needs uppercase PSWDUC</td>
<td>No</td>
</tr>
<tr>
<td>LID in passwords PSWDPWD</td>
<td>Yes</td>
</tr>
<tr>
<td>Pswd needs lowercase PSWDLC</td>
<td>No</td>
</tr>
<tr>
<td>Part of name in pswd PSWDMNAME</td>
<td></td>
</tr>
<tr>
<td>Logon ok: reset vio# CLEARVIO</td>
<td>No</td>
</tr>
<tr>
<td>Password encryption PSWDENC</td>
<td>XDES</td>
</tr>
<tr>
<td>Non-std chars allowed in pswd &amp;!*%_=</td>
<td></td>
</tr>
</tbody>
</table>

### Password Phrase Settings (PWPHRASE)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PwP usage for all users ALLOW</td>
<td>No</td>
</tr>
<tr>
<td>Max PwP length MAXLEN</td>
<td>100</td>
</tr>
<tr>
<td>Age temporary PwPs TEMP-AGE</td>
<td>Yes</td>
</tr>
<tr>
<td>Min PwP length MINLEN</td>
<td>9</td>
</tr>
<tr>
<td>Max PwP age (days) MAXDAYS</td>
<td></td>
</tr>
<tr>
<td>Warning days for PwP WARN DAYS</td>
<td>1</td>
</tr>
<tr>
<td>Min PwP age (days) MINDAYS</td>
<td></td>
</tr>
<tr>
<td>PwP history size HISTORY</td>
<td>0</td>
</tr>
<tr>
<td>Permit PwP change CMD-CHG</td>
<td>Yes</td>
</tr>
<tr>
<td>Min numerics in PwP NUMERIC</td>
<td>0</td>
</tr>
<tr>
<td>EXTRACT calls for PwP EXTRACT</td>
<td>No</td>
</tr>
<tr>
<td>Min alphabolics in PwP ALPHA</td>
<td>0</td>
</tr>
<tr>
<td>Permit Logon ID in PwP LID</td>
<td>Yes</td>
</tr>
<tr>
<td>Min spec. chr. in PwP SPECIAL</td>
<td>0</td>
</tr>
<tr>
<td>Min words in PwP MINWORD</td>
<td>1</td>
</tr>
<tr>
<td>Max rep. chars in PwP REPCHAR</td>
<td></td>
</tr>
<tr>
<td>Special chars in PwP SPECLIST</td>
<td></td>
</tr>
</tbody>
</table>

---

Figure 102. GSO system settings (Screen 2)
Global System Options

Figure 101 on page 80 displays GSO records, interpreted by IBM Security zSecure Audit for ACF2. In contrast, the native ACF2 command to view GSO records does not provide this interpretation. The Option settings heading shown in Figure 101 on page 80 is an explanation of the GSO OPTS record parameters. The OPTS record is a key GSO record providing control of settings such as system mode, date format, default logonids, last logon notify, started task checking, and authority to submit batch jobs.

Important OPTS parameters to review are:

**MODE**
If this parameter is set to any mode other than ABORT, it must be investigated.

---

**Figure 103. GSO system settings (Screen 3)**

<table>
<thead>
<tr>
<th>GSO system settings</th>
<th>Line 51 of 75</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command =/&gt; Scroll=/&gt; CSR</td>
<td></td>
</tr>
<tr>
<td>MLS related settings (MLSOPTS)</td>
<td>Access rule settings (RULEOPTS)</td>
</tr>
<tr>
<td>MLS active</td>
<td>MLACTIVE No</td>
</tr>
<tr>
<td>MLS mode of operation</td>
<td>MODE</td>
</tr>
<tr>
<td>MLS writedown allowed</td>
<td>MLWRITE</td>
</tr>
<tr>
<td>Unix reqs seclabels</td>
<td>MLFSOBJ</td>
</tr>
<tr>
<td>IPCobj reqs seclabels</td>
<td>MLIPCOBJ</td>
</tr>
<tr>
<td>Seclabels SYS-depdt</td>
<td>MLSECBYS</td>
</tr>
<tr>
<td>DSNs/rsrs req label</td>
<td>MLSLBLRQ No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UNIX options (UNIXOPTS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAF HFS Security enable</td>
</tr>
<tr>
<td>Default user</td>
</tr>
<tr>
<td>Default group</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Erase settings (AUTOERAS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erase VSAM</td>
</tr>
<tr>
<td>Erase everything</td>
</tr>
<tr>
<td>EOS SecLevel-based</td>
</tr>
<tr>
<td>EOS decided by</td>
</tr>
<tr>
<td>Volumes protected by dataset (RESVOLS)</td>
</tr>
<tr>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Logged programs (LOGPGM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMASPZAP IMASPZAP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protected programs (PPGM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRW*- FDF** IEHD-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Programs with tape-BLP (BLPPGM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRMBMR1 ADROSSU SYS1.LINKLIB</td>
</tr>
<tr>
<td>CRMBMR1 TESTJE TEST.LIBR</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PDSes with member-level protection (PDS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRMBMR1.ISPF.CNTL</td>
</tr>
<tr>
<td>TEST.LIBRARY</td>
</tr>
<tr>
<td>TEST.LIBRARY</td>
</tr>
<tr>
<td>TEST.PDSALLOW</td>
</tr>
<tr>
<td>TEST.PDSALLOW</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Linklist libraries (LINKLST)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS1.LINKLIB</td>
</tr>
</tbody>
</table>

****************************************************************************** TOP OF DATA **************************************************************************
**Default logonids**
Determine batch and started task logonids and investigate how and why they are used.

**Started task checking (STC)**
STC indicates that ACF2 is to validate data set access by started tasks. This option should be set to `ON`.

The following table provides the recommended password settings. You can also set a password phrase. For more information about using password phrases, see *IBM Security zSecure Audit for ACF2: User Reference Manual*.

<table>
<thead>
<tr>
<th>Password Controls</th>
<th>PSWD Record Parameter Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Controls Minimum length of 6</td>
<td>MINPSWD(6)</td>
</tr>
<tr>
<td>Password history checking enabled</td>
<td>PSWDHST</td>
</tr>
<tr>
<td>Prevent Logonid used as password</td>
<td>PSWDLID</td>
</tr>
<tr>
<td>Prevent all numeric password</td>
<td>PSWDNUM</td>
</tr>
<tr>
<td>Password required for all user logonids</td>
<td>PSWDREQ</td>
</tr>
<tr>
<td>New password forced when password reset</td>
<td>PSWDFRC</td>
</tr>
<tr>
<td>Password violation detected via batch jobs</td>
<td>PSWDJES</td>
</tr>
<tr>
<td>Restrict password selections</td>
<td>PSWDRSV</td>
</tr>
<tr>
<td>Threshold of password attempts in one session</td>
<td>PASSLMT(3)</td>
</tr>
<tr>
<td>Threshold of password attempts in one day</td>
<td>MAXTRY(3)</td>
</tr>
<tr>
<td>Require at least one alphabetic character in the password</td>
<td>PSWDALPH</td>
</tr>
<tr>
<td>Require at least one numeric character in the password</td>
<td>PSWDNMIC</td>
</tr>
<tr>
<td>Force users to wait at least one day between password changes</td>
<td>PSWDMIN(1)</td>
</tr>
<tr>
<td>Allow a maximum of two pairs of identical characters in the password</td>
<td>PSWDPAIR(2)</td>
</tr>
<tr>
<td>Temporary passwords are not added to the password history</td>
<td>PSWDNAGE</td>
</tr>
<tr>
<td>Allow a password history of more than 4 entries</td>
<td>PSWXHIST</td>
</tr>
<tr>
<td>Keep a password history of 13 (4+9) entries</td>
<td>PSWXHST#(9)</td>
</tr>
</tbody>
</table>

The GSO BACKUP record enables automatic backup of the ACF2 databases (VSAM clusters). A setting of `TIME(00:00)` indicates the automatic backup has been disabled. Confirm that the ACF2 database is backed up daily by ACF2 or another mechanism. `TIME(00:01)` directs ACF2 to back up the database at one minute after midnight. A command in the STRING field directs ACF2 to start a procedure after the automatic backup is complete. `STRING(S ACFBKUP)` is a START command for a procedure called ACFBKUP, supplied by your organization, that is, a member in SYS1.PROCLIB. This procedure copies the primary backup files to an alternate VSAM cluster for recovery purposes.

To change settings in the GSO PSWD record, issue the following ACF2 commands:
The first command points to the GSO Infostorage records. The second command changes the PSWD settings.

**GSO Maintenance record**

The MAINT record as shown in [Figure 105](#) must be carefully monitored. MAINT records are established for a maintenance condition such as batch production processing. Data set rule validation processing is bypassed when a maintenance condition is met.

In the **Maintenance programs and LIDs** section of the panel shown in [Figure 105](#), the Logon ID, which is the first column in the list, SMCLEAN in this example, can run the program in the middle column. The middle column is ADRDSSU, from the specified load library, which is the last column, SYS1.LINKLIB in this example, uninhibited by ACF2 data set rule processing. This means that the Logon ID can access any data set in any fashion through the specified program execution. The access is limited or controlled through the program execution. MAINT should be used for production purposes.

**GSO PDS record**

ACF2 resource rules can provide access control to members within a partitioned data set or PDS. This specific designation is established by way of the GSO PDS record as shown in [Figure 106](#). Any PDS with this protection is registered in the PDS record with the corresponding resource type.
Auditing user concerns

About this task

Review the user audit concerns in detail.

Procedure

1. Press PF3 to return to the Audit selection panel as shown in Figure 107.
2. In the selection panel, tab to the ACF2 user option.
3. Type / in the ACF2 user selection field as shown in Figure 107.
4. Move to the bottom of the screen.
5. Type / in the Include audit concern overview in overall prio order selection field.

6. Press Enter to open the Display Selection panel as shown in Figure 108 on page 86.

Many reports and tables provide analysis of Logon ID audit concerns. Figure 108 on page 86 lists the available reports for determining exposures and monitoring user activity. Items such as password aging, last logon statistics, excessive data set and resource access allowed via rules, and excessive access due to Logon ID privileges are detected through this display.
In Figure 108, the following line provides information about trusted logon IDs.

_TRUS2USR 1 18457 Trusted logonids (may bypass security)

The following line provides an example of password concerns.

_PWAGSUM2 2 939 ACF2 password age overview

This line provides an example of last logon activity.

_LGAGSUM2 2 939 ACF2 last logon overview

To review the Overview report selection, complete the following steps:

_Reviewing the Overview report selection._

Procedure

1. In the Display Selection panel, type S in the selection field for the OVERVIEW summary record as shown in Figure 108.
2. Press Enter to open the Overview display panel.
   For information about this panel, continue with the following section: “User audit concerns by priority.”

**User audit concerns by priority**

The Audit concern overview by priority panel shown in Figure 109 is a simple summary of the most important audit concerns. These concerns are identified across all systems examined and are sorted by numerical audit priority.

*Table 14. Audit Priority values*

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 10</td>
<td>informational</td>
</tr>
<tr>
<td>10 - 20</td>
<td>desired</td>
</tr>
<tr>
<td>20 - 40</td>
<td>review required</td>
</tr>
<tr>
<td>40 and up</td>
<td>serious exposure</td>
</tr>
</tbody>
</table>

In Figure 109, the JOBFROM attribute allows the Logon ID JOHNTTEST to submit a batch job by using any Logon ID in the ACF2 database without specifying a password. The JOBFROM attribute assumes trusted communication and must be carefully controlled. The attribute is meant for address spaces that support multiple users such as CICS and ROSCOE. It is not intended for individual user IDs and is dangerous if assigned to users versus address spaces.

Use of the PREFIX field in the Logon ID record indicates data set ownership. Logon IDs with a PREFIX value, that is, SYS1, matching the high-level qualifier of a
requested data set prompt ACF2 to ignore data set rule validation. PREFIX values are set to match the Logon ID or set to null. The presence of RULEVLD in the Logon ID forces ACF2 to perform rule validation even if the requesting Logon ID owns the data set.

The RESTRICT attribute is intended for production batch processing. RESTRICT eliminates the need for password assignment. Compensating controls such as SOURCE and PROGRAM restrict the use of the exposed Logon ID. Ensure that all logon IDs with the RESTRICT attribute have at least one other compensating control: SUBAUTH (submitting program is APF-authorized), SOURCE, for example, STCINRDR, and PROGRAM, for example, your scheduler program name. Reference the ACF2 report ACFRPTJL for the appropriate parameter values associated with production jobs.

### Auditing password concerns

#### About this task

IBM Security zSecure Audit for ACF2 provides various informational reports about password controls. As shown in the Audit concern overview by priority panel in Figure 109 on page 87, there are over 20 password reports to view. Password controls analyze concerns such as logon IDs without an assigned password, passwords that never expire, and passwords that were not changed over certain time frames.

The following examples show how to access information about the Logon IDs without a password interval report. Logon IDs without a password do not have a MAXDAYS value assigned. MAXDAYS is a Logon ID field that controls the maximum usage of a password, forcing the password to expire when the interval is reached. When no MAXDAYS is assigned, the password does not expire automatically.

Logon IDs whose passwords do not expire can become targets for hacking. This information can aid anyone who attempts to guess passwords and gain unauthorized entry to your system. A recommended setting for MAXDAYS, maximum password usage, is 30 days.

To review logon IDs without a password interval information, see the PWINNON2 report. To view this report, complete the following steps:

**Procedure**

1. Press PF3 to return to the ACF2 Display Selection panel.
2. Move to the PWINNON2 heading.
3. Type S in the selection field for PWINNON2 as shown in Figure 110.

---

**Figure 110. Select a password audit report**
4. Press Enter to open the Users without a password interval summary panel as shown in Figure 111.

This summary display indicates the number of inactive and active logon IDs without a password interval. This example of Figure 111 reveals that out of 74 users without a password interval, 57 logon IDs are active and 17 are inactive.

Figure 111. Password interval summary

Listing logon IDs without a password interval

Procedure

1. In the summary panel, move to the No entry in the Inactivated Users section as shown in Figure 111.

   This entry represents the active logon IDs, that is, the logon IDs that are not deactivated.

2. Type S in the selection field for the No entry.

3. Press Enter to view the list of active logon IDs without a password interval as shown in Figure 112.

Figure 112 lists the active logon IDs without a MAXDAYS value. In this example, the MxD column is blank for each Logon ID listed. Blanks indicate no password interval, which means that a password is vulnerable to hacking.

The report provides the following information:

- Logon ID
- Name
- UID string
- Password interval (MxD)
- Date that the password was last changed (PW change)

Logon IDs without a password interval are vulnerable to attack. Determine whether any user logon IDs, as opposed to production batch or started task logon IDs, have powerful privileges assigned. Also determine whether any user logon IDs might have access to sensitive data by way of the uid string values. These logon IDs are even more vulnerable to attack.
4. To view more detailed information about the Logon ID, complete the following steps: "Viewing information about the Logon ID"

Viewing information about the Logon ID

Procedure

1. In the Users without password interval panel as shown in Figure 112 on page 89, move down to the LID list column and select a Logon ID to view.
2. Type S in the selection field for the Logon ID.
   In the example shown in Figure 112 on page 89, BSMITH1, Bert Smith is selected.
3. Press Enter to open the detail panel as shown in Figure 113 on page 91
Both Figure 112 on page 89 and Figure 113 show detailed information displays of a Logon ID. When additional information is necessary from Figure 112 on page 89, it is easy to select the Logon ID in question. You can also view all the fields in the Logon ID record as shown in Figure 113. In addition, IBM Security zSecure Audit for ACF2 provides audit concerns for any Logon ID settings such as:

### Figure 113. Detail Logon ID display of user without password interval

<table>
<thead>
<tr>
<th>Identification</th>
<th>Full UID</th>
<th>Scope</th>
<th>Application privileges</th>
<th>Systemwide privileges</th>
<th>Miscellaneous privileges</th>
<th>Audit trail</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACF2 logonid</td>
<td>NCTST</td>
<td>ScpList</td>
<td>Yes TSO</td>
<td>Allow all access</td>
<td>Step-Must-Complete bypassed</td>
<td>Write all logons to SMF</td>
<td>Logonid has been cancelled</td>
</tr>
<tr>
<td>User name</td>
<td>BSMITH1</td>
<td>DSNscope</td>
<td>User has SECURITY privilege</td>
<td>Read/Execute to all data sets</td>
<td>ACF2 refresh allowed</td>
<td>Trace all data access</td>
<td>Cancel/Suspend/Monitor by</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UIDscope</td>
<td>User has ACCOUNT privilege</td>
<td>Bypass tape Label Processing</td>
<td>User can always generate dump</td>
<td>Trace all TSO commands</td>
<td>Logonid has been suspended</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User has LEADER privilege</td>
<td></td>
<td>User can always generate dump</td>
<td>Warm security of all logons</td>
<td>Cancel/Suspend/Monitor since</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User has CONSULT privilege</td>
<td></td>
<td>Bypass restricted cmd list</td>
<td>Password phrase anomalies</td>
<td>Suspended: too many pswd vios</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Not bound to shifts</td>
<td>PwPhrase effectively allowed</td>
<td>Activation date</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Logonid has MAINT privilege</td>
<td># PwP violations on PWP-DATE</td>
<td>Expiration date</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>User can execute PPROMs</td>
<td>0</td>
<td>Last LID record update</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Dynamic logon privilege</td>
<td>RESTRICT - no password needed</td>
<td>Date of last access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Disable violation counter</td>
<td></td>
<td>Last password change date</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Maximum password lifetime</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Audit concern</td>
</tr>
</tbody>
</table>

The table above includes the following details for the user without password interval:

- **Identification**
  - User name: SMITH, BERT

- **Full UID**
  - NCTST: BSMITH1

- **Scope**
  - ScpList: BSMITH1
  - DSNscope: BSMITH1
  - UIDscope: BSMITH1

- **Application privileges**
  - Effective TSO setting: Yes TSO
  - User can sign on to CICS
  - User can sign on to IMS
  - User can sign on to IDMS
  - Effective JOB setting: Yes JOB

- **Systemwide privileges**
  - Allow all access
  - Read/Execute to all data sets
  - Bypass tape Label Processing

- **Miscellaneous privileges**
  - Step-Must-Complete bypassed
  - ACF2 refresh allowed
  - User can always generate dump
  - Limited BLP
  - Bypass restricted cmd list
  - Not bound to shifts
  - Logonid has MAINT privilege
  - User can execute PPROMs
  - Dynamic logon privilege
  - Disable violation counter

- **Audit trail**
  - Write all logons to SMF
  - Trace all data access
  - Trace all TSO commands
  - Warm security of all logons
  - Password phrase anomalies
  - PwPhrase effectively allowed: Yes
  - # PwP violations on PWP-DATE: 0

- **Access**
  - Logonid has been cancelled
  - Logonid has been suspended
  - Suspended: too many pswd vios
  - Activation date
  - Expiration date
  - Date of last access
  - Last LID record update: 29Jan2005
  - Last password change date: 2May2005
  - Maximum password lifetime

- **Audit concern**
  - Password change not enforced, Can change password back to old value

**************************************************** END OF DATA *****************************************************
as MAXDAYS and MINDAYS. In Figure 113 on page 91, the following line shows that no value was assigned to these fields for BSMITH1.

```
# days before pswd expires   # days wait before pswd
```

The maximum and minimum usage of a password is not enforced for this sample user. The result is that a password that might never be altered by the user.

---

**Creating audit reports for resource concerns**

**About this task**

IBM Security zSecure Audit for ACF2 provides reports to audit access to resources and data sets. The following reports are available within this category:

- Sensitive Data reports
- Authorized Programs report
- Started Task Protection report
- Globally Writable Files report
- Sensitive Data Trustees report
- Sensitive Data by Rule reports

**Procedure**

To view audit concerns related to resources and data sets, complete the following steps:

1. Press PF3 until you return to the Audit Status panel as shown in Figure 114.
2. Move to the ACF2 resource option.
3. Type / in the selection field for ACF2 resource as shown in Figure 114.
4. Move to the bottom of the screen.
5. Type / in the selection field for **Include audit concern overview, higher priorities only** as shown in Figure 114.

6. Press Enter to open the reports panel as shown in Figure 115 on page 93.
This panel shows the reports available to audit resources.

<table>
<thead>
<tr>
<th>Name</th>
<th>Summary</th>
<th>Records Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVERVIEW</td>
<td>3474</td>
<td>0 Audit concern overview by priority (higher prioritie</td>
</tr>
<tr>
<td>SENZAPF</td>
<td>1</td>
<td>103 APF data sets with full ACL</td>
</tr>
<tr>
<td>SENSENW</td>
<td>1</td>
<td>39 LPA list data sets with full ACL</td>
</tr>
<tr>
<td>SENZALL</td>
<td>1</td>
<td>192 All sensitive data sets by priority and type with fu</td>
</tr>
<tr>
<td>SENZTRUS</td>
<td>1</td>
<td>18457 Sensitive data trustees with full audit concerns / r</td>
</tr>
<tr>
<td>SENZRULE</td>
<td>1</td>
<td>18349 Rules protecting sensitive data with full audit conc</td>
</tr>
<tr>
<td>TSOAUTH</td>
<td>1</td>
<td>3 TSO authorized commands</td>
</tr>
<tr>
<td>LPAPROT2</td>
<td>1</td>
<td>285 LPA module protection overview</td>
</tr>
<tr>
<td>APFPROT2</td>
<td>1</td>
<td>285 APF module protection overview</td>
</tr>
<tr>
<td>UNIXAPF2</td>
<td>0</td>
<td>0 UNIX files with APF authorization</td>
</tr>
<tr>
<td>UNIXCTL2</td>
<td>0</td>
<td>0 UNIX files that are program controlled (daemons etc.</td>
</tr>
<tr>
<td>UNIXSGI2</td>
<td>0</td>
<td>0 UNIX files with SETGID authorization</td>
</tr>
<tr>
<td>STCPROT2</td>
<td>0</td>
<td>0 Started task overview</td>
</tr>
<tr>
<td>GLB2UNIX</td>
<td>0</td>
<td>0 UNIX files vulnerable to trojan horse &amp; back door at</td>
</tr>
</tbody>
</table>

Figure 115. Reports available to audit resources

In the example shown in Figure 115, you can see the following reports:

- Sensitivity reports (report record names begin with SENZ*)
- Authorized program reports (LPAPROT2 and APFPROT2)
- STC Overview report (STCPROT2)
- Globally Writable report (GLB2UNIX)

The following sections provide more information about selecting and viewing audit concerns in reports.

**Sensitive Data report**

Sensitive data reports show the data set name, type of risk (that is, update access), and the number of users with access. These users are labeled as trusted because access is granted through rules. Data sets might be selected from these panels to view rule lines that grant access.

**Authorized Programs report**

The authorized programs report shows load modules that have the potential to circumvent ACF2. This report also includes UNIX files with APF authorization.

**Started Task Protection report**

The started task protection report shows the authority and protection of started tasks. This report shows the procedure name, Logon ID associated with the started task, and the associated ACF2 Logon ID privilege. The last modification date and the Logon ID that performed the update are also noted.

**Globally Writable Files report**

This report shows what z/OS UNIX files can be updated and by whom.

**Sensitive Data Trustees report**

Sensitive Data Trustees reports display logon IDs granted access to sensitive data sets through rules. These reports provide a broad view of access granted to data sets such as APF libraries and the ACF2 databases.
To view this report, complete the following steps: “Displaying the sensitive data trustees report.”

To see more detail, complete the following steps: “Viewing more detail.”

To select an entry, complete the following steps: “Selecting an entry” on page 96.

To view similar information for rules, complete the following steps: “Viewing similar information for rules” on page 97.

Displaying the sensitive data trustees report

Procedure

To view information in a sensitive data trustees report, follow these steps.

1. Move down to select **SEN2TRUS**.
2. In the selection field, type `/`. Then, press Enter to open the report display as shown in Figure 116.

<table>
<thead>
<tr>
<th>Name</th>
<th>Summary</th>
<th>Records</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>OVERVIEW</em></td>
<td>3474</td>
<td>0</td>
<td>Audit concern overview by priority (higher prioritie</td>
</tr>
<tr>
<td><em>SEN2APF</em></td>
<td>1</td>
<td>103</td>
<td>APF data sets with full ACL</td>
</tr>
<tr>
<td><em>SEN2LINK</em></td>
<td>1</td>
<td>39</td>
<td>Linklist data sets with full ACL</td>
</tr>
<tr>
<td><em>SEN2LPA</em></td>
<td>1</td>
<td>14</td>
<td>LPA list data sets with full ACL</td>
</tr>
<tr>
<td><em>SEN2ALL</em></td>
<td>1</td>
<td>192</td>
<td>All sensitive data sets by priority and type with fu</td>
</tr>
<tr>
<td>/ <em>SEN2TRUS</em></td>
<td>18457</td>
<td>Sensitive data trustees with full audit concerns / r</td>
<td></td>
</tr>
<tr>
<td><em>SEN2RULE</em></td>
<td>18349</td>
<td>Rules protecting sensitive data with full audit conc</td>
<td></td>
</tr>
<tr>
<td><em>TSOAUTH2</em></td>
<td>1</td>
<td>3</td>
<td>TSO authorized commands</td>
</tr>
<tr>
<td><em>LPPAPROF2</em></td>
<td>1</td>
<td>285</td>
<td>LPA module protection overview</td>
</tr>
<tr>
<td><em>APFPAPROF2</em></td>
<td>1</td>
<td>285</td>
<td>APF module protection overview</td>
</tr>
<tr>
<td><em>UNIXAPF2</em></td>
<td>0</td>
<td>0</td>
<td>UNIX files with APF authorization</td>
</tr>
<tr>
<td><em>UNIXCTL2</em></td>
<td>0</td>
<td>0 UNIX files that are program controlled (daemons etc.</td>
<td></td>
</tr>
<tr>
<td><em>UNIXSUI2</em></td>
<td>0</td>
<td>0 UNIX files with SETUID authorization</td>
<td></td>
</tr>
<tr>
<td><em>UNIXSUGI2</em></td>
<td>0</td>
<td>0 UNIX files with SETGID authorization</td>
<td></td>
</tr>
<tr>
<td><em>STCPROF2</em></td>
<td>0</td>
<td>0 Started task overview</td>
<td></td>
</tr>
<tr>
<td><em>GLBZUNIX</em></td>
<td>0</td>
<td>0 UNIX files vulnerable to trojan horse &amp; back door at</td>
<td></td>
</tr>
</tbody>
</table>

Figure 116. Sensitive data trustees

Resources are grouped to demonstrate a broad view such as access to APF libraries and ACF2 database files. The reports show the number of resources within a group, the number of trustees with access, and the number of audit concerns. Detail displays show the data set name, Logon ID, the audit concern, and the rule line that grants access. Figure 117 on page 95 lists each sensitivity group, the class, that is, data set, number of resources within the group, and the number of audit concerns identified (trust relations).

Viewing more detail

Before you begin

Complete the steps in “Displaying the sensitive data trustees report.”

Procedure

Follow these steps to view more information in the sensitive data trustees report:

1. Move to an entry such as **Privilege**.
2. Type / in the selection field for Privilege as shown in Figure 117. Then, press Enter.

<table>
<thead>
<tr>
<th>Sensitive data trustees with full audit concerns / reasons</th>
<th>Line 1 of 26</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command ===&gt; ___________________________________________</td>
<td>Scroll==&gt; CSR_</td>
</tr>
<tr>
<td>Pri Complex System Trust relations</td>
<td>9 May 2005 22:10</td>
</tr>
<tr>
<td>10 DEMO DEMO 18457</td>
<td></td>
</tr>
<tr>
<td>Pri Sensitivity Class Resources Trust relations</td>
<td></td>
</tr>
<tr>
<td>10 Privilege System</td>
<td>108</td>
</tr>
<tr>
<td>/_</td>
<td></td>
</tr>
<tr>
<td>9 ACF2 LID db DATASET 1</td>
<td>539</td>
</tr>
<tr>
<td>9 APF Library DATASET 33</td>
<td>823</td>
</tr>
<tr>
<td>9 APF Linklst DATASET 24</td>
<td>1448</td>
</tr>
<tr>
<td>9 APF LPAP1IST DATASET 3</td>
<td>195</td>
</tr>
<tr>
<td>9 MSTR pmplib DATASET 3</td>
<td>195</td>
</tr>
<tr>
<td>9 MSTR STClib DATASET 3</td>
<td>195</td>
</tr>
<tr>
<td>8 ACF2 Infost DATASET 1</td>
<td>65</td>
</tr>
<tr>
<td>8 ACF2 Rules DATASET 1</td>
<td>65</td>
</tr>
<tr>
<td>7 JES2 Ckpt DATASET 1</td>
<td>938</td>
</tr>
<tr>
<td>6 ACF2 MAINT DATASET 1</td>
<td>65</td>
</tr>
<tr>
<td>4 ACF2 AltLid DATASET 5</td>
<td>2695</td>
</tr>
<tr>
<td>4 ACF2 Bklid DATASET 1</td>
<td>539</td>
</tr>
<tr>
<td>4 System Dump DATASET 1</td>
<td>474</td>
</tr>
<tr>
<td>4 SMF Dataset DATASET 1</td>
<td>40</td>
</tr>
<tr>
<td>3 Active IODF DATASET 1</td>
<td>65</td>
</tr>
<tr>
<td>2 ACF2 AltBkl DATASET 5</td>
<td>2695</td>
</tr>
<tr>
<td>2 ACF2 AltBkl DATASET 5</td>
<td>2695</td>
</tr>
<tr>
<td>2 ACF2 AltBkR DATASET 5</td>
<td>2695</td>
</tr>
<tr>
<td>2 ACF2 BkInfo DATASET 1</td>
<td>539</td>
</tr>
<tr>
<td>2 ACF2 BkRule DATASET 1</td>
<td>539</td>
</tr>
<tr>
<td>2 SMS ACDS DATASET 1</td>
<td>65</td>
</tr>
<tr>
<td>2 SMS COMMDS DATASET 1</td>
<td>65</td>
</tr>
<tr>
<td>2 SMS SCDS DATASET 1</td>
<td>65</td>
</tr>
<tr>
<td>1 ACF2 AltInf DATASET 5</td>
<td>325</td>
</tr>
<tr>
<td>1 ACF2 AltRul DATASET 5</td>
<td>325</td>
</tr>
</tbody>
</table>
|**********************************************************************|************| Bottom of Data

Figure 117. Select a sensitivity group such as Privilege

Figure 118 shows the display of logon IDs within the sensitivity group of Privilege. These IDs have access due to a special privilege assigned to the Logon ID. The audit concern describes the threat.

<table>
<thead>
<tr>
<th>Sensitive data trustees with full audit concerns / reasons</th>
<th>Line 1 of 108</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command ===&gt; ___________________________________________</td>
<td>Scroll==&gt; CSR_</td>
</tr>
<tr>
<td>Pri Complex System Trust relations</td>
<td>9 May 2005 22:10</td>
</tr>
<tr>
<td>10 DEMO DEMO 18457</td>
<td></td>
</tr>
<tr>
<td>Pri Sensitivity Class Resources Trust relations</td>
<td></td>
</tr>
<tr>
<td>10 Privilege System</td>
<td>108</td>
</tr>
<tr>
<td>Pri Resource VolSer Trust relations</td>
<td>108</td>
</tr>
<tr>
<td>Pri Logonid Name From Audit concern</td>
<td></td>
</tr>
<tr>
<td>10 PRODLID PROD BACTCH LID DEMO</td>
<td>Can submit for all others</td>
</tr>
<tr>
<td>10 CMASC2 SPECIAL JOB LID DEMO</td>
<td>Can submit for all others</td>
</tr>
<tr>
<td>10 SMCLEAN MCLEAN, SARAH DEMO</td>
<td>Unscooped authority to change/defi</td>
</tr>
<tr>
<td>10 PCRAM1 BERT SPECIAL USER DEMO</td>
<td>Unscooped authority to change/defi</td>
</tr>
<tr>
<td>10 LVOIGHT VOIGHT, LARRY DEMO</td>
<td>Unscooped authority to change/defi</td>
</tr>
<tr>
<td>10 Rmorton HORTON, RAY DEMO</td>
<td>Unscooped authority to change/defi</td>
</tr>
<tr>
<td>8 PROCTCID PROD STC LID DEMO</td>
<td>All data set access allowed</td>
</tr>
<tr>
<td>4 PRODFHS PROD HFS LID DEMO</td>
<td>All data set access allowed</td>
</tr>
<tr>
<td>4 TAPEMGR TAPE MANAGER DEMO</td>
<td>Can rea/write any tape includin</td>
</tr>
<tr>
<td>1 PRODICICS CICS DEMO</td>
<td>Can execute MAINT protected utili</td>
</tr>
<tr>
<td>1 SYSPROG SYS PROG LID DEMO</td>
<td>Can execute MAINT protected utili</td>
</tr>
<tr>
<td>1 SYSPROG SYS PROG LID DEMO</td>
<td>Can execute MAINT protected utili</td>
</tr>
</tbody>
</table>

Figure 118. Sensitive data trustees with full audit concerns
Further information can be gathered by selecting an entry and viewing the user name and assigned privilege such as SECURITY, JOBFROM, or READALL.

**Selecting an entry**

**Procedure**

1. In the Sensitive data trustees with full audit concerns panel, move to a Logon ID entry. The example shown in Figure 118 on page 95 uses the SYSPROG Logon ID.

2. Type S in the selection field for the Logon ID entry as shown in Figure 118 on page 95.

3. Press Enter to view the record.

   Figure 119 shows the Logon ID SYSPROG with the MAINT privilege.

4. To view more detail, type S in the selection field for the MAINT privilege entry as shown in Figure 119.

   Sensitive data trustees with full audit concerns / reasons  Line 1 of 1
   Command ===> _________________________________________________ Scroll===> CSR_
   9 May 2005 22:10
   Pri Complex  System  Trust relations
   10 DEMO DEMO  18457
   Pri Sensitivity Class  Resources Trust relations
   10 Privilege  System  1  108
   Pri Resource  VolSer Trust relations
   10 DEMO  108
   Pri Logonid  Name  From  Audit concern
   1 SYSPROG MAINT PROD  Can execute MAINT protected utility
   Pri Privilege Access $KEY  Rule Entry
   S_  1 MAINT

   ******************************* BOTTOM OF DATA ********************************

   Figure 119. Select a Logon ID to view the assigned privilege

5. Press Enter to open the detailed view for the MAINT privilege entry as shown in Figure 120.
Viewing similar information for rules
Before you begin

Access the **Sensitive data trustees with full audit concerns / reasons** panel using the procedure in “Displaying the sensitive data trustees report” on page 94.

Procedure

1. Move to the **ACF2 Rules** field as shown in [Figure 121](#).

2. Press Enter to view the **ACF2 Rules** records as shown in [Figure 122](#). 

   [Figure 122](#) shows logon IDs that have special access to sensitive data sets. Select one to see the detail display.

   In this example, the Logon ID **SMITH7** is selected.

3. Press Enter to view the assigned privileges for the Logon ID, **SMITH7** in this example.

   [Figure 121](#). Detail Logon ID attributes for sensitive privileges

   [Figure 122](#). Show reasons that logon IDs have special access to sensitive data sets
Example

Figure 123 shows the reason why access is granted. In this example, the rule grants access to all **SYS1.ACF2V64.PRIM.RULES**.

---

**Figure 123. View assigned privileges for logon IDs with access to sensitive data sets**
Chapter 7. 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 ===> Scroll ===> CSR

****** ***************************** Top of Data *****************************
000001 * Systems Programmers or Systems Administrators *
000002 SYSPROG
000003 SYSPROG

****** ***************************** Bottom of Data *****************************
```

Figure 124. 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:

   Menu | Options | Info | Commands | Setup
   ----------------------------------------
   Command =AU.R  zSecure Suite - Audit - Compliance

   Compliance evaluation
   _ STIG (subset)
   _ GSD (subset)
   _ Other standard member
   _ Test a single rule (set) member _ RACF (RACF/ACF2/TSS/NONE)

   Compliance result selection
   _ Compliant _ Non-compliant _ Undecided

   Output/run options
   _ Print format _ Send as e-mail
   Background run

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:

   **STIG**  Security Technical Implementation Guide published by the US Defence Information Systems Agency (DISA-STIG)

   **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
Figure 125 shows an example of output for the rule set level:

<table>
<thead>
<tr>
<th>Complex Ver</th>
<th>Standards NonComp Unknown Exm Sup</th>
<th>Standard Rule sets NonComp Unknown Exm Sup Version</th>
<th>Rule set Objects NonComp Unknown Exm Sup Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACF2AD2R ACF2</td>
<td>1 1</td>
<td>ACF2_STIG 16 9 6.14</td>
<td>ACF0260 1 1 The AUTHEXIT GSO record value</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ACF0270 1 The AUTOERAS GSO record value</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ACF0280 9 9 The BACKUP GSO record value</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ACF0290 4 4 The BLPPSM GSO record value</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ACF0330 19 The LINKLST GSO record value</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ACF0350 5 5 The MAINT GSO record value</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ACF0390 1 1 The PSMD GSO record value</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ACF0410 8 1 The RESRULE GSO record value</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ACF0430 11 2 The RULEOPTS GSO record value</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ACF0480 1 The SECVOLS GSO record value</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ACF0760 40 28 There are LOGONIDs with t</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ZSMSA008 2 DFSMS resource class(es)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ZUSSA060 3 The CLASSMAP definitions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ZUSSA070 3 The INFODIR record does n</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ZUSS0041 1 1 Attributes of z/OS UNIX u</td>
</tr>
</tbody>
</table>

Figure 125. Standard compliance test results
Chapter 8. Resource-based reports for ACF2 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”
- “UNIX file system reports” on page 104
- “CICS region and resource reports” on page 108
- “IMS region and resource reports” on page 109
- “DB2 region and resource reports” on page 110

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 **TCP=NO** parameter. You can also report on SMF events related to IP configuration data by using the EV.I menu option.

When you select RE.I from the Main menu, the panel shown in Figure 127 on page 104 is displayed.
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 (F1).

You can also specify Output and run options on the Selection panel. You can use the run options to specify additional 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.

For a description of Show differences options, see the IBM Security zSecure Audit for ACF2: User Reference Manual.

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 that you specified.

See the IBM Security zSecure Audit for ACF2: User Reference Manual for more detailed information about these reports.

**UNIX file system reports**

When you select option RE.U, the Resource - UNIX panel shown in Figure 128 opens.

**Figure 128. Resource UNIX menu**

**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, additional information is displayed.

When you select option RE.U, the Resource - UNIX Selection panel shown in Figure 129 opens.

If the selection panel is left blank, all UNIX records are selected. You can limit the UNIX records 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 file system records. When you select a criteria, 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 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 Audit for ACF2: User Reference Manual and the online help.

After processing the CKFREEZE file by using the specified selection criteria, the UNIX summary panel opens to display the results as shown in Figure 130 on page 106.
Selecting any of the mount points listed in the UNIX summary panel (Figure 130) displays the list of UNIX files for that mount point as shown in Figure 131. 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 UNIX file list display panel (Figure 131), the UNIX file detail display panel shown in Figure 132 on page 107 opens. To view the contents of a file in this panel, type S in front of the Absolute pathname field.
Reports - running the predefined UNIX audit reports

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 133 For details about a specific report, position the cursor on the report selection field, then press F1 to view the online help.
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 134 is displayed.

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

In the CICS Resource panel in Figure 134, select the option of your choice. The corresponding selection panel is displayed. For example, the CICS Regions selection panel in Figure 135.

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).

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 online, field-sensitive help function (PF1). You can also select output and run options.
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 online help and the IBM Security zSecure Audit for ACF2: User Reference Manual.

**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 136 is displayed.

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

```
Menu Options Info Commands Setup Startpanel
------------------------------------------------------------------------------------
zSecure Suite - Resource - IMS
Option ===> __________________________________________________________________
R Regions IMS control region reports
T Transactions IMS transactions reports
P PSBs IMS program specification blocks
```

**Figure 136. IMS Resource panel**

In the IMS Resource panel in Figure 136, select the option of your choice. The corresponding selection panel is displayed. For example, the IMS Regions selection panel in Figure 137

```
Menu Commands Setup
----------------------
zSecure Suite - IMS - Regions
Command ===> __________________________________________________________________
Show IMS control regions that fit all of the following criteria:
  Jobname ........ ________ (jobname or filter)
  VTAM applid ..... ________ (applid or filter)
  IMSID ......... ________ (identifier or filter)
  Complex ......... ________ (complex or filter)
  System ......... _____ (system or filter)

Advanced selection criteria
  - Region security settings

Output/run options
  - Show differences
  - Print format Customize title Send as e-mail
  - Background run Full page form
```

**Figure 137. IMS 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 online, field-sensitive help function (PF1).
You can also select output and run options in the IMS Resource 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 online help and IBM Security zSecure Audit for ACF2: User Reference Manual.

### DB2 region and resource reports

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

When you select **RED**, the DB2 region and resource reports panel shown in Figure 138 is displayed.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>Regions Region overview and system privileges (DSNADM, MDSNSM)</td>
</tr>
<tr>
<td>DB</td>
<td>Databases Sets of tables, indexes, and table spaces</td>
</tr>
<tr>
<td>JR</td>
<td>Java archives Sets of files comprising Java applications</td>
</tr>
<tr>
<td>PK</td>
<td>Packages Packages (pre-bound SQL statements)</td>
</tr>
<tr>
<td>PN</td>
<td>Plans Plans (control structures created during BIND)</td>
</tr>
<tr>
<td>SG</td>
<td>Storage groups Sets of storage objects (volumes)</td>
</tr>
<tr>
<td>SP</td>
<td>Stored procs Stored procedure and user function routines</td>
</tr>
<tr>
<td>SQ</td>
<td>Sequences User defined objects defining a numerical sequence</td>
</tr>
<tr>
<td>TB</td>
<td>Tables/views Tables and views</td>
</tr>
<tr>
<td>TS</td>
<td>Table spaces Table spaces (data set name space for storing tables)</td>
</tr>
</tbody>
</table>

Figure 138. DB2 Resource panel

When you select the option of your choice, the corresponding selection panel is displayed. For example, the DB2 regions selection panel.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show DB2 regions that fit all of the following criteria:</td>
<td></td>
</tr>
<tr>
<td>Jobname . . . . . . ________ (jobname or filter)</td>
<td></td>
</tr>
<tr>
<td>Local LU name . . . ________ (luname or filter)</td>
<td></td>
</tr>
<tr>
<td>Local site name . . . ________ (name or filter)</td>
<td></td>
</tr>
<tr>
<td>DB2ID . . . . . . ________ (identifier or filter)</td>
<td></td>
</tr>
<tr>
<td>Group attachment name ________ (name or filter)</td>
<td></td>
</tr>
<tr>
<td>Complex . . . . . . ________ (complex or filter)</td>
<td></td>
</tr>
<tr>
<td>System . . . . . . ________ (system or filter)</td>
<td></td>
</tr>
</tbody>
</table>

Advanced selection criteria
- Region security settings

Output/run options
- Show differences
- Print format Customize title Send as e-mail
- Background run Full page form

Figure 139. DB2 Region 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 online, 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 Audit for ACF2: User Reference Manual."
Chapter 9. Event reporting

This chapter describes how to view security events extracted from SMF and formatted by IBM Security zSecure Audit for ACF2. Events are logged to SMF and extracted for reporting purposes. This information can be helpful when troubleshooting problems and investigating what happened during a particular time frame.

Use the Events functions to complete the following tasks:
- Trace user, job, terminal, and resource activity.
- Trace specific SMF events, including ACF2, DB2, CICS, Omegamon, and IP event types.
- Report on logon failures by source or Logon ID.
- Report on data set access violations by data set.
- Report on data set access violations by Logon ID.
- Report on resource access violations by rule.
- Report on resource access violations by Logon ID.
- Report on maintenance to the ACF2 databases.

SMF data sources for input sets

The SMF displays can work with the live SMF data sets, SMF log streams, or with sequential SMF data that is produced by the IBM IFASMFDP or IFASMFDL programs. While you are getting familiar and experimenting with IBM Security zSecure Audit for ACF2, 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 need to consider the SMF data you use with zSecure Audit. The amount of SMF data 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 Megabytes, for example, while in other cases, that allocation might hold only an hour of SMF data collection. For simple experimentation with the product, a set of SMF data in the 10-30 megabyte range would be reasonable. If you must apply filtering to reduce the size of the data set, make sure that the following record types are not filtered out.

Table 15. SMF Record types that should not be filtered 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>16</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>
</tbody>
</table>
Table 15. SMF Record types that should not be filtered out of the SMF data (continued)

<table>
<thead>
<tr>
<th>Record type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>83</td>
<td>Audit security event records from IBM Security Key Lifecycle Manager and WebSphere Application server.</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>110</td>
<td>CICS performance monitoring</td>
</tr>
<tr>
<td>118</td>
<td>TCP/IP Telnet and FTP</td>
</tr>
<tr>
<td>119</td>
<td>TCP UDP and IP</td>
</tr>
<tr>
<td>120</td>
<td>WebSphere Application Server</td>
</tr>
<tr>
<td>230</td>
<td>ACF2 Processing</td>
</tr>
</tbody>
</table>

When you opt to process SMF data, the data sets need to be defined to IBM Security zSecure Audit for ACF2. You can use live or log stream SMF data or obtain recent SMF data and copy it to a sequential data set. In both cases, you must change your input file settings.

You can also run zSecure Audit for ACF2 SMF analysis on a full SMF file with all record types present. The product supports about 100 different SMF record types.

To use a data set with SMF data, complete the steps in “Specifying a data set with SMF data.”

Specifying a data set with SMF data

Procedure
1. Select option SE from the Main menu.
2. Select 1 to open the Setup Input panel.
   For information in this panel, see “Selecting the input set” on page 72.
3. Move the cursor to the input field in 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 title 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 filled in. If it does not end with .SMF, a panel such as Figure 140 on page 115 opens so you can assign a
type to the file you are defining.

7. Press PF3.

This returns to the Input selection menu with the new input set you defined selected.

Tip: You can select multiple inputs sets at the same time. Reflect on the possibility to define a set for each file or couple of files. For example, a live SMF set and a most recent unload of the ACF2 database and CKFREEZE data set and select both sets as input.

Your input file settings look similar to those settings in Figure 141.

To use live SMF data you do not need to specify a data set. Type / in the Type field and press Enter. The panel from Figure 140 opens so you can select option ACT.SMF.

This form is the most basic form of SMF input. In a more complex situation, you might combine live SMF plus the most recent n generations (if you use GDGs) of archived SMF data by listing multiple lines within the set.

8. Select option SMF. Press Enter.

This generates a line that references the live SMF data.
Reviewing violation events

About this task

This task presents an overview for displaying violation events by using IBM Security zSecure Audit for ACF2.

Procedure

1. To return to the Main menu, press Enter.
2. In the command line, type EV and press Enter to select the Events options.

3. Type 3 in the Option field and press Enter to open the ACF2 Events panel.

4. To select the SMF reports option, in the Events panel (Figure 142), type 1 in the Option field and press Enter. The SMF reports panel is displayed.
Statistical reporting can be viewed by the hour, time, and day. Data set violations by batch job and APPC reports are additional reporting options.

In this example, no action is necessary in the Options panel shown in Figure 145. With this panel, you can set SMF processing options before processing the report. With these options, you can limit input and output specifications such as the number of SMF records to be read and processed.

5. To view the ACF2 exception report, type 1 in the Option field and press Enter to open the Options panel.

6. In the Options panel, press Enter to open the Display Selection panel as shown in Figure 146 on page 118.

The Display Selection panel presents the events grouped by logon failures, data set access violations, and resource violations. The Rows column indicates event data logged to SMF. Rows with zero indicate that no data was generated for this period.
Figure 146 shows three columns, Name, Records, and Title. The Name column uses abbreviations to indicate logon failures, data set violations, and resource violations. Interpret the Name column by using the following Table 16.

**Table 16. Exception Event codes and definitions**

<table>
<thead>
<tr>
<th>Exception event code</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOGF_x_x</td>
<td>Logon Failure, T=terminals or source, L=logon IDs, F=frequent, I=in frequent</td>
</tr>
<tr>
<td>DVIO_x_x</td>
<td>Data set violation, L=Logonid, F=frequent, I=in frequent</td>
</tr>
<tr>
<td>RVIO_x_x</td>
<td>Resource violation, L=Logonid, F=frequent, I=in frequent</td>
</tr>
</tbody>
</table>

To view the resource access violations shown in the Display Selection panel, complete the following steps: Viewing resource access violations in the Display Selection panel.

**Viewing resource access violations in the Display Selection panel**

**Procedure**

Follow these steps to view resource access violations:

1. In the Display Selection panel, move to an entry that has a number under the Records field.
2. In the selection field for the entry, type S.
   In the example shown in Figure 146, the Resource access violations by rule – overview entry is selected. This entry has one event to report as indicated in the Rows column.
3. Press Enter to open the overview panel for the exception record as shown in Figure 147 on page 119.
In Figure 147, note the Rule key and Count columns. There are two violations for PAYROLL protected by the ACF2 resource rule $KEY(PAYROLL) TYPE(PGM).

The Rulekey column in Figure 147 indicates the lookup rule set that was used during ACF2 resource rule processing when the access violation occurred. Interpret the column in the following manner:

- **R** = Resource rule class code
- **FAC, SAF, SFP, SUR, TGR, and PGM** represent ACF2 three character type codes for resource rules.
- **PAYROLL** is the $KEY value in this resource rule example.

To view the resource rules, use IBM Security zSecure Audit for ACF2 function AA.I. Additional information about TCP/IP configuration and statistics and the UNIX file system resources is available from the Resource menu option (RE). See Chapter 8, “Resource-based reports for ACF2 resources,” on page 103.

To view the data set rules, use IBM Security zSecure Audit for ACF2 function AA.R.

---

**Viewing ACF2 database maintenance activity**

**About this task**

With the Maintenance report, you can track database maintenance activity. This report shows inserts, replacements, and deletions for the following fields: Rule, Logon ID, and InfoStorage. Use this report to track changes, troubleshoot events, and to perform reviews of security administration activities.

**Procedure**

To view ACF2 database maintenance activity, complete the following steps:

1. To return to the Main menu, press Enter.
2. In the command line, type EV to select the ACF2 events option as shown in Figure 148 on page 120. Then, press Enter to open the ACF2 events panel as shown in Figure 149 on page 120.
3. Press Enter to open the ACF2 events panel as shown in Figure 149.

4. In the ACF2 events panel, type / in the selection field for the Maintenance field as shown in Figure 149. Then, press Enter.

5. Press Enter on the next three screens that open until you reach the panel shown in Figure 150 on page 121.

Figure 150 on page 121 shows the maintenance activity against the ACF2 databases. The reporting period is displayed at the top of the panel. Event information such as Logon ID inserts and deletions, and rule changes and the Logon ID of the security administrator is displayed in the Description column.
Viewing user events

Procedure

To view user events such as logon, job submission, data set access, and security violations and loggings, complete the following steps:

1. Press PF3 to return to the Main menu.
2. In the Main menu, type \texttt{U} in the command line to select the User option as shown in Figure 151 on page 122.
3. Press Enter to open the User Selection panel shown in Figure 152 on page 123.

---

SMF record ACF2 processing and audit records

Command \texttt{----- Command \texttt{----- Command \texttt{----- Command \texttt{----- Command \texttt{-----}}}}

Scroll\texttt{----- Scroll\texttt{----- Scroll\texttt{----- Scroll\texttt{----- Scroll\texttt{-----}}}}

- 27Apr05 15:20 to 19May05 17:23
- 38 s elapsed, 10.7 s CPU

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>27Apr2005</td>
<td>15:20</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>29Apr2005</td>
<td>10:41</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>29Apr2005</td>
<td>11:12</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>29Apr2005</td>
<td>11:16</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>29Apr2005</td>
<td>11:27</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>29Apr2005</td>
<td>11:28</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>29Apr2005</td>
<td>11:30</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>19May2005</td>
<td>11:40</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>19May2005</td>
<td>11:51</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>19May2005</td>
<td>11:52</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>19May2005</td>
<td>12:13</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>19May2005</td>
<td>12:15</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>19May2005</td>
<td>14:41</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>19May2005</td>
<td>14:41</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>19May2005</td>
<td>14:41</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>19May2005</td>
<td>14:41</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>19May2005</td>
<td>14:41</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>19May2005</td>
<td>14:41</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>19May2005</td>
<td>14:41</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>19May2005</td>
<td>14:41</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>19May2005</td>
<td>14:41</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
<tr>
<td>19May2005</td>
<td>14:41</td>
<td>SMF record ACF2 processing and audit records</td>
</tr>
</tbody>
</table>

Figure 150. Maintenance activity against the ACF2 databases

Chapter 9. Event reporting 121
4. To select a Logon ID, for example, your own Logon ID, for viewing user events, complete the steps in "Selecting a logon ID for viewing user events."

Selecting a logon ID for viewing user events

Procedure

To view user events for a specified logon ID, follow these steps:

1. Move to the Logon ID field.
2. Type your logon ID.

The example shown in Figure 152 on page 123 uses JSMITH.
3. Press Enter to view the events.

In this example, all events for JSMITH are shown in Figure 153 on page 124. This report shows activity for a date and time range as indicated in the third line of the panel. Each entry lists the date and description for an event. To view the entire display, press PF8 to scroll a few times.
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29Apr2005 02:21:08.68</td>
<td>Start of job JSMITH (TSU01634) for user JSMITH</td>
<td></td>
</tr>
<tr>
<td>29Apr2005 02:21:08.68</td>
<td>Start of job JSMITH for user JSMITH</td>
<td></td>
</tr>
<tr>
<td>29Apr2005 02:24:37.21</td>
<td>ACFS id JSMITH READ access XFC CKR.READALL from LC</td>
<td></td>
</tr>
<tr>
<td>29Apr2005 02:31:03.72</td>
<td>Define data set JSMITH.ISPFCAP.RTF in ICF catalog</td>
<td></td>
</tr>
<tr>
<td>29Apr2005 02:33:23.72</td>
<td>Define data set JSMITH.ISPFCAP.RTF in ICF catalog</td>
<td></td>
</tr>
<tr>
<td>29Apr2005 02:34:58.54</td>
<td>Define data set JSMITH.ISPFCAP.RTF in ICF catalog</td>
<td></td>
</tr>
<tr>
<td>29Apr2005 02:43:48.89</td>
<td>Define data set JSMITH.ISPFCAP.RTF in ICF catalog</td>
<td></td>
</tr>
<tr>
<td>29Apr2005 03:02:01.80</td>
<td>Define data set JSMITH.ISPFCAP.RTF in ICF catalog</td>
<td></td>
</tr>
<tr>
<td>29Apr2005 03:10:08.37</td>
<td>Define data set JSMITH.ISPFCAP.RTF in ICF catalog</td>
<td></td>
</tr>
<tr>
<td>29Apr2005 02:21:08.68</td>
<td>Start of job JSMITH for user JSMITH</td>
<td></td>
</tr>
<tr>
<td>29Apr2005 02:21:08.68</td>
<td>Start of job JSMITH (TSU01634) for user JSMITH</td>
<td></td>
</tr>
<tr>
<td>29Apr2005 02:24:37.21</td>
<td>ACFS id JSMITH READ access XFC CKR.READALL from LC</td>
<td></td>
</tr>
<tr>
<td>29Apr2005 02:31:03.72</td>
<td>Define data set JSMITH.ISPFCAP.RTF in ICF catalog</td>
<td></td>
</tr>
<tr>
<td>29Apr2005 02:33:23.72</td>
<td>Define data set JSMITH.ISPFCAP.RTF in ICF catalog</td>
<td></td>
</tr>
<tr>
<td>29Apr2005 02:34:58.54</td>
<td>Define data set JSMITH.ISPFCAP.RTF in ICF catalog</td>
<td></td>
</tr>
<tr>
<td>29Apr2005 02:43:48.89</td>
<td>Define data set JSMITH.ISPFCAP.RTF in ICF catalog</td>
<td></td>
</tr>
<tr>
<td>29Apr2005 03:02:01.80</td>
<td>Define data set JSMITH.ISPFCAP.RTF in ICF catalog</td>
<td></td>
</tr>
<tr>
<td>29Apr2005 03:10:08.37</td>
<td>Define data set JSMITH.ISPFCAP.RTF in ICF catalog</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 153. User events report**
Chapter 10. Report generation

This topic demonstrates how to save reports to a data set and how to print reports to hardcopy from the Results panel.

This information can be helpful when troubleshooting problems, preparing an audit report, and investigating what happened during a particular time frame.

Use the Results function to complete the following tasks:

- Browse a file.
- Edit a file.
- Print a file.
- View a file.
- Run commands.
- Submit jobs for command execution.
- Write a file to a sequential or partitioned data set.

Results panel

All reports generate the Results panel. The following procedures demonstrate how to create, archive, and print reports from the Results panel:

- “Creating an audit report”
- “Archiving reports” on page 127
- “Printing reports” on page 128

Creating an audit report

Procedure

Follow these steps to create an ACF2 control settings report:

1. From the IBM Security zSecure Audit for ACF2 Main menu, type AU in the Option command line to select the Audit option as shown in Figure 154 on page 126.
2. After selecting the Audit option, type $ in the Option command line to select the Audit Status option as shown in Figure 155.

3. Press Enter to open the panel to select report settings. This example procedure illustrates how to generate an ACF2 control settings report.

4. To select the ACF2 control report option, tab to the ACF2 control field. Then, type / in the selection field.
   a. To specify the report output setting, tab to the Output in print format field in the Select options for reports section. Then, type / in the selection field. The screen should look similar to the one shown in Figure 156 on page 127. The selections are shown in bold type.
b. Press Enter. Figure 157 shows the report generated after selecting report settings and pressing Enter. To review the entire report, scroll to the right and down.

To select the options for saving the report, press PF3 in the panel that shows the report output.

When you press PF3, the Results panel opens so you can archive or save the report. For details, see “Archiving reports” and “Printing reports” on page 128.

Archiving reports

Procedure

Follow these steps to save a specified data set for archiving:
1. Type W in the Report selection field as shown in Figure 158.

2. Press Enter to open a panel to specify the data set name for the reports.

3. In the Data set name field, type the data set name in which you want to save the report as shown in Figure 159.

4. If the data set is partitioned (PDS), type the member name in the Member field as shown in Figure 159.

5. After you specify the data set name information, press Enter. The report is saved to the specified data set for archiving and future reference.

**Printing reports**

**Procedure**

Follow these steps to print a report from the Results panel:

1. Type P beside the report selection as shown in Figure 160 on page 129.

2. Press Enter.
This action does not generate a new panel. Look in the upper right corner for a message that indicates the outcome of your print result.

Results

Figure 161 shows an example of the print result message. Output to Spool indicates that your report is staged for hardcopy printing.

Figure 160. Printing reports from the Results panel

Figure 161. Printing reports - Print result message
Appendix A. Frequently asked questions

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

Table 17. Frequently Asked Questions

Q: Why is the Main panel empty?
A: You need READ access to $KEY(CKR) rule in the XFACILIT class TYPE(XFC). CKR rules can allow or prohibit the use of IBM Security zSecure Audit for ACF2.

Q: Can I collect information (unloaded ACF2 and c data sets) on different systems and send this information to one system for display and analysis?
A: Yes. All the systems involved must be covered by your license framework. This is a common way to use IBM Security zSecure Audit for ACF2.

Q: How do I handle a shared JES2 spool environment, with one ACF2 database and several MVS images?
A: Run the ACF2 unload one time from any system, unless you want to work with live ACF2 data. Run multiple COLLECT jobs (one on each system). You can use the SHARED=N0 parameter with the second and additional COLLECT job to reduce the size of the resulting CKFREEZE data sets. Do this only if your UCBs are properly defined with SHARED options to exactly reflect the sharing environment, otherwise COLLECT everything. Create an INPUT SET for IBM Security zSecure Audit for ACF2 that has these multiple CKFREEZE data sets defined.

Q: When should I use my live ACF2 database with IBM Security zSecure Audit for ACF2, and when should I use unloaded data?
A: It is suggested when using the unloaded ACF2 database for all queries to prevent an enqueue failure on the ACF2 backup job.

Q: I used the SETUP.INPUT options to define my input sets. The next time I used IBM Security zSecure Audit for ACF2, my setup values were not saved. Why?
A: You probably used a different TSO user ID the second time. The setup information is remembered 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 Options menu to determine the setting of this option.

Q: I browsed the User Reference manual, and it talks about IBM Security zSecure Audit for ACF2 commands and the command language. Do I need this command language? Your evaluation guide seems to ignore it.
A: The interactive ISPF panels automatically generate the CARLA commands. For any IBM Security zSecure Audit for ACF2 functions that can be done through the ISPF panels, you can use the panels and ignore the command language.

However, if you want to do something unusual, such as produce a highly customized report, you might need to use the command language. You can enter IBM Security zSecure Audit for ACF2 commands through batch or by using Option CO (Command) in the IBM Security zSecure Audit for ACF2 primary menu.
Table 17. Frequently Asked Questions (continued)

Q: IBM Security zSecure Audit for ACF2 inspects many MVS controls, for various reports. When does it obtain these controls from MVS storage, and when should you use a CKFREEZE data set?

A: For full checking, IBM Security zSecure Audit for ACF2 uses MVS control blocks that were copied into the CKFREEZE data set. While this issue is more complex than using in-storage MVS data, it produces results that are much more consistent.

The results are meaningful for the time at which the CKFREEZE data was collected. For this reason, you might want to collect CKFREEZE data when your system is fully loaded and most active. This also means that you can perform IBM Security zSecure Audit for ACF2 studies for remote MVS systems, by using a CKFREEZE data set and ACF2 unloaded data created on the remote system. IBM Security zSecure Audit for ACF2 licenses are required for all systems involved.

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 have 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 to gather only part of the potential CKFREEZE data. Multiple CKFREEZE data sets are useful. For example, if you use IBM Security zSecure Audit for ACF2 freeze functions to detect changes in various libraries, or if your auditors want system snapshots at certain defined times.

Q: Does ACF2 Scoping work with IBM Security zSecure Audit for ACF2?

A: By default, ACF2 Scoping also applies to IBM Security zSecure Audit for ACF2. There is an override mechanism that enables someone to perform and evaluation and also for daily auditing.
Appendix B. zSecure Collect memory requirements

zSecure Collect is a component of IBM Security zSecure Audit for ACF2 that enables the product to collect the data from audited systems. It is designed to run as fast as possible and uses memory in return for speed. In a smaller z/OS installation, it might operate well in 6-8 MB, while it might grow to over 60 MB in a large installation. By default, zSecure Collect collects various information, which contributes to its memory requirements. If necessary, you can control memory usage by reducing the amount of parallel operation involved, and by not collecting certain types of data.

zSecure Collect is run as a batch job. The job is often submitted by using the REFRESH command while in the Input panels. When this is done, you have the opportunity to edit the job before it is submitted. You can add some or all of the following statements to the job. By default, there is no SYSIN DD statement. Do not add the comments in parentheses.

```plaintext
//SYSIN DD *
PARALLEL=PATHGROUP (reduces parallel operation), or
PARALLEL=NONE (remove any parallel operation)
CAT=MCA (do not read user catalogs)
DMS=NO (collect no SAMS:Disk data)
VMF=NO (collect no TLMS data)
RMM=NO (collect no RMM data)
MCD=NO (collect no primary HSM data)
BCD=NO (collect no backup HSM data)
TMC=NO (collect no CA-1 data)
ABR=NO (no FDR/ABR file data)
UNIX=NO (no UNIX file directories)
/*
```

Figure 162. Job statements to add to the zSecure Collect job to reduce memory requirements

Even if you have no memory constraints, you might want to consider using some of these restrictions. In particular, you might want to exclude HSM and tape catalog data. The MCD and BCD parameters refer to HSM data. This consideration is not related to product operation, but to your installation security policies. A policy discussion is not within the scope of this document.
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

A
accessibility viii
ACF2
database maintenance 119
exception report 116
masking characters 11
override viewing scope 8
record access criteria 7
rules 97
scoping
default 7
view cross-reference records 65
view scope records 62
scoping guidelines 5
terminology 3
types of rules 27
ACF2 Events panel 116
ACF2_LID display 8
ACF2_LID display panel 16, 19
analyze data set access 42
archive a report 127
AU.R 99
audit concern reports 92
audit concerns
logon ID details 16
overview by priority 77
prioritize 77
use of 76
view 76
audit function 75
Audit panel 125
audit priority values 77, 87
Audit Selection panel 10
Authorized Programs report 93

B
Boolean operators 11
Boolean operators for logon ID display 24

C
CICS
region, transaction, and program data report 108
Resource panel 108
Collections, SETUP 73
compliance evaluation 99

D
data flow 2
data set
analyzing access 42
display NEXTKEYs 45
rule lines 40
rule structure 48
data set (continued)
rules
tasks 27
view by rule set 30
view rule lines 56
view using LIST 33
view using SELECT 34
data set rules 27
data sources 2
database maintenance for ACF2 119
date values 11
default ACF2 scoping 7
define input sets 113
display Logon IDs 14
Display Selection panel 92
DUMPDATE date 11

E
education viii
event report 113
expanded nextkey option 49

G
Global System Options 82
Globally Writable Files report 93
GSO
Maintenance record 84
PDS record 84
system settings 79
GSO System Settings panel 77

I
IBM
Software Support viii
Support Assistant viii
IMS
Resource panel 109
IMS region, transaction, and program data reports 109
individual scope record 64
Infostorage
database 61
records 61
sample scope records 6
input
data 69, 114
new files 69
set
composition 71
selecting 72
IP stack configuration report 103
IP stack Selection panel 103
ISPF 1

L
LIST command 19, 33
LIST Output error 7
list rule lines
data set access 43
view logon ID for specific data set 40
logon ID
access 13
display 14
display for same user name 25
display using a mask 20
display using Boolean operators 24
field descriptions 14
records 16
settings 18
special privileges to list 22
uid string to display 21
view user events 122
Logon ID selection panel 8
Logonid Selection panel 14

M
Main menu panel 10, 13
Maintenance report 119
mask for logon IDs 20
masking characters 11
memory requirements for zSecure Collect 133
multisystem support, remote data 3

N
navigation characters 11
New files panel 69
new files to specify 69
NEXTKEY
display methods 45
expand function 50
expanded format 49
field 46

O
offline data sources 69
online
publications v
terminology v
options
RE.C 108
RE.M 109
SE.B 73

P
panel
Rules Selection 10
panels
ACF2 Events 116

© Copyright IBM Corp. 1998, 2013