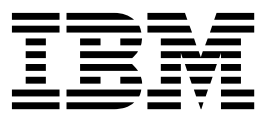


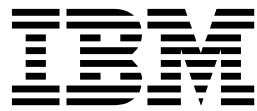
Security zSecure Audit for ACF2
Version 2.2.0

Getting Started



Security zSecure Audit for ACF2
Version 2.2.0

Getting Started



Note

Before using this information and the product it supports, read the information in “Notices” on page 147.

November 2015

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

© Copyright IBM Corporation 1998, 2015.

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

Contents

About this publication	v	Listing data set rule lines specific to a uid string ..	43
zSecure documentation	v	Displaying NEXTKEYs in data set rules	45
Obtain licensed documentation	vi	Specifying additional selection criteria	46
IBM Security zSecure Suite library	vi	Data set rule structure and NEXTKEYs	48
IBM Security zSecure Manager for RACF z/VM library	viii	Displaying rules lines in expanded NEXTKEY format	49
Related documentation.	ix	Using the expanded NEXTKEYs function	50
Accessibility	x	Reviewing the expanded NEXTKEY rule lines for each X line	54
Technical training.	x	Viewing individual data set rule lines	56
Support information.	x	Viewing a resource rule	58
Statement of Good Security Practices	x		
 Chapter 1. Overview	1	 Chapter 4. Infostorage records	61
Data sources	2	Infostorage record types and attributes	61
Remote data	3	Viewing scope records.	62
ACF2 terminology used in this guide	3	Viewing an individual Scope record	64
ACF2 scoping	5	Viewing cross-reference records.	65
Sample scope records	5	Viewing an individual cross-reference group record	66
Scoping by default	7		
LIST command	7	 Chapter 5. SETUP functions for data management	69
SELECT command	7	Inputting data	69
Screen navigation.	8	Inputting new files	69
Opening the Main menu	9	Refreshing and loading files	71
Trying out the options.	10	Selecting the input set	72
Viewing the Rules information	10	Specifying collections of input sets.	73
Viewing Audit information	10		
Masking characters	10	 Chapter 6. Security control analysis ..	75
Date fields.	11	Audit concerns	75
Summary of navigation characters.	11	Selecting the Audit function	75
		Viewing audit concerns detected by zSecure Audit for ACF2	76
 Chapter 2. Logon ID tasks	13	Reviewing audit concerns overview by priority	77
Accessing the Logon ID functions	13	Audit concern overview by priority	77
Displaying your Logon ID	14	Viewing GSO system settings	79
Displaying Logon IDs using SELECT.	16	Global System Options	82
Interpreting Logon ID settings	18	GSO Maintenance record	84
Displaying logonids using LIST.	19	GSO PDS record.	84
Displaying Logon IDs using a mask	20	Auditing user concerns	85
Displaying logon IDs with matching UID string ..	21	Reviewing the Overview report selection	86
Listing logon IDs with special privileges.	22	User audit concerns by priority.	87
Example: Find all logon IDs with SECURITY and ACCOUNT and not NON-CNCL:	23	Auditing password concerns.	88
Displaying all logon IDs with the same user name	24	Listing logon IDs without a password interval..	89
		Viewing information about the Logon ID	90
 Chapter 3. Rule analysis	27	Creating audit reports for resource concerns	92
Data set rules.	27	Sensitive Data report	93
Resource rules	27	Authorized Programs report.	93
Viewing data set rules.	27	Started Task Protection report	93
Viewing by rule set.	30	Globally Writable Files report	93
Displaying data set rules using LIST	33	Sensitive Data Trustees report	93
Displaying data set rules using SELECT.	34	Displaying the sensitive data trustees report	94
Audit concerns	38	Viewing more detail	94
Suggestions for rule reviews.	38	Selecting an entry	96
Displaying who last stored a rule	39	Viewing similar information for rules.	97
Listing rule lines for a specific data set	40		
Analyzing data set access.	42		

Chapter 7. Rule-based compliance evaluation	99
Reporting	100
STDRULES: Standard rule set compliance summary	102
STDYPES: Standard object type compliance summary	104
STDTESTS: Standard compliance test results ..	105
 Chapter 8. Resource-based reports for ACF2 resources	 111
CICS region and resource reports	111
DB2 region and resource reports	112
DB2 region reports	113
DB2 resource reports	114
IP stack reports	115
IMS region and resource reports	116
VTAM application reports	117
MQ region and resource reports	118
MQ region reports	119
MQ resource reports	119
UNIX file system reports	121
 Chapter 9. Event reporting.	 125
SMF data sources for input sets	125

Specifying a data set with SMF data.	126
Reviewing violation events	128
Viewing resource access violations in the Display Selection panel	130
Viewing ACF2 database maintenance activity. ..	131
Viewing user events	133
Selecting a logon ID for viewing user events . ..	133

Chapter 10. Report generation	137
Results panel	137
Creating an audit report.	137
Archiving reports	139
Printing reports	140

Appendix A. Frequently asked questions	143
---	------------

Appendix B. zSecure Collect memory requirements	145
--	------------

Notices	147
Trademarks	149

Index	151
------------------------	------------

About this publication

IBM® Security zSecure™ Audit for ACF2 Version 2.2.0 provides system auditing and monitoring utilities for ACF2. It collects and analyzes data from ACF2 systems and 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.

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.

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).

zSecure documentation

The IBM Security zSecure Suite and IBM Security zSecure Manager for RACF z/VM libraries consist of unlicensed and licensed publications. This section lists both libraries and instructions to access them.

Unlicensed zSecure publications are available at the IBM Knowledge Center for IBM Security zSecure Suite or IBM Security zSecure Manager for RACF z/VM. The IBM Knowledge Center is the home for IBM product documentation. You can customize IBM Knowledge Center, create your own collection of documents to design the experience that you want with the technology, products, and versions that you use. You can also interact with IBM and with your colleagues by adding comments to topics and by sharing through email, LinkedIn, or Twitter. For instructions to obtain the licensed publications, see “Obtain licensed documentation” on page vi.

IBM Knowledge Center for product	URL
IBM Security zSecure Suite	http://www.ibm.com/support/knowledgecenter/SS2RWS/welcome
IBM Security zSecure Manager for RACF z/VM	http://www.ibm.com/support/knowledgecenter/SSQQGJ/welcome

The IBM Terminology website consolidates terminology for product libraries in one location.

Obtain licensed documentation

All licensed and unlicensed publications for IBM Security zSecure Suite 2.2.0 and IBM Security zSecure Manager for RACF z/VM 1.11.2, except the Program Directories, are included on the *IBM Security zSecure Documentation CD, LCD7-5373*. Instructions for downloading the disk image (.iso) file for the zSecure Documentation CD directly are included with the product materials.

To obtain an extra copy of the .iso file of the *Documentation CD* or PDF files of individual publications, complete the following steps:

1. Go to the IBM Publications Center.
2. Select your country or region and click the **Go** icon.
3. On the **Welcome to the IBM Publications Center web** page, click **Customer Support** in the left navigation menu.
4. Complete the support form with the following information: your contact details, your customer number, and the numbers of the licensed publications you want to order.
5. Click **Submit** to send the form. The form is forwarded to an IBM Publications Center Customer Support representative who sends you details to fulfill your order.

Alternatively, you can send an email to tivzos@us.ibm.com requesting access to the .iso file of the *zSecure Documentation CD*. Include your company's IBM customer number and your preferred contact information. You will receive details to fulfill your order.

IBM Security zSecure Suite library

The IBM Security zSecure Suite library consists of unlicensed and licensed publications.

Unlicensed publications are available at the IBM Knowledge Center for IBM Security zSecure Suite. Licensed publications have a form number that starts with L; for example, LCD7-5373.

The IBM Security zSecure Suite library consists of the following publications:

- *About This Release* includes release-specific information as well as some more general information that is not zSecure-specific. The release-specific information includes the following:
 - *What's new*: Lists the new features and enhancements in zSecure V2.2.0.
 - *Release notes*: For each product release, the release notes provide important installation information, incompatibility warnings, limitations, and known problems for the IBM Security zSecure products.
 - *Documentation*: Lists and briefly describes the zSecure Suite and zSecure Manager for RACF z/VM libraries and includes instructions for obtaining the licensed publications.
- *IBM Security zSecure CARLa-Driven Components Installation and Deployment Guide, SC27-5638*

Provides information about installing and configuring the following IBM Security zSecure components:

- IBM Security zSecure Admin
- IBM Security zSecure Audit for RACF®, CA-ACF2, and CA-Top Secret
- IBM Security zSecure Alert for RACF and ACF2

- IBM Security zSecure Visual
- IBM Security zSecure Adapters for QRadar SIEM for RACF, CA-ACF2, and CA-Top Secret
- *IBM Security zSecure Admin and Audit for RACF Getting Started, GI13-2324*
Provides a hands-on guide introducing IBM Security zSecure Admin and IBM Security zSecure Audit product features and user instructions for performing standard tasks and procedures. This manual is intended to help new users develop both a working knowledge of the basic IBM Security zSecure Admin and Audit for RACF system functionality and the ability to explore the other product features that are available.
- *IBM Security zSecure Admin and Audit for RACF User Reference Manual, LC27-5639*
Describes the product features for IBM Security zSecure Admin and IBM Security zSecure Audit. Includes user instructions to run the admin and audit features from ISPF panels. This manual also provides troubleshooting resources and instructions for installing the zSecure Collect for z/OS® component. This publication is available to licensed users only.
- *IBM Security zSecure Admin and Audit for RACF Line Commands and Primary Commands Summary, SC27-6581*
Lists the line commands and primary (ISPF) commands with very brief explanations.
- *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, Global System Options, and running reports. The manual also includes a list of common terms for those not familiar with ACF2 terminology.
- *IBM Security zSecure Audit for ACF2 User Reference Manual, LC27-5640*
Explains how to use IBM Security zSecure Audit for ACF2 for mainframe security and monitoring. For new users, the guide provides an overview and conceptual information about using ACF2 and accessing functionality from the ISPF panels. For advanced users, the manual provides detailed reference information, troubleshooting tips, information about using zSecure Collect for z/OS, and details about user interface setup. This publication is available to licensed users only.
- *IBM Security zSecure Audit for Top Secret User Reference Manual, LC27-5641*
Describes the IBM Security zSecure Audit for Top Secret product features and provides user instructions for performing standard tasks and procedures. This publication is available to licensed users only.
- *IBM Security zSecure CARLa Command Reference, LC27-6533*
Provides both general and advanced user reference information about the CARLa Auditing and Reporting Language (CARLa). CARLa is a programming language that is used to create security administrative and audit reports with zSecure. The *CARLa Command Reference* also provides detailed information about the NEWLIST types and fields for selecting data and creating zSecure reports. This publication is available to licensed users only.
- *IBM Security zSecure Alert User Reference Manual, SC27-5642*
Explains how to configure, use, and troubleshoot IBM Security zSecure Alert, a real-time monitor for z/OS systems protected with the Security Server (RACF) or CA-ACF2.
- *IBM Security zSecure Command Verifier User Guide, SC27-5648*

Explains how to install and use IBM Security zSecure Command Verifier to protect RACF mainframe security by enforcing RACF policies as RACF commands are entered.

- *IBM Security zSecure CICS Toolkit User Guide*, SC27-5649

Explains how to install and use IBM Security zSecure CICS® Toolkit to provide RACF administration capabilities from the CICS environment.

- *IBM Security zSecure Messages Guide*, SC27-5643

Provides a message reference for all IBM Security zSecure components. This guide describes the message types associated with each product or feature, and lists all IBM Security zSecure product messages and errors along with their severity levels sorted by message type. This guide also provides an explanation and any additional support information for each message.

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

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

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

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

Program directories are provided with the product tapes. You can also download the latest copies from the IBM Knowledge Center for IBM Security zSecure Suite.

- *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 Security zSecure Adapters for QRadar SIEM.

- *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 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 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.

IBM Security zSecure Manager for RACF z/VM library

The IBM Security zSecure Manager for RACF z/VM library consists of unlicensed and licensed publications.

Unlicensed publications are available at the IBM Knowledge Center for IBM Security zSecure Manager for RACF z/VM. Licensed publications have a form number that starts with L; for example, LCD7-5373.

The IBM Security zSecure Manager for RACF z/VM library consists of the following publications:

- *IBM Security zSecure Manager for RACF z/VM Release Information*
For each product release, the Release Information topics provide information about new features and enhancements, incompatibility warnings, and documentation update information. You can obtain the most current version of the release information from the zSecure for z/VM® documentation website at the IBM Knowledge Center for IBM Security zSecure Manager for RACF z/VM.
- *IBM Security zSecure Manager for RACF z/VM: Installation and Deployment Guide, SC27-4363*
Provides information about installing, configuring, and deploying the product.
- *IBM Security zSecure Manager for RACF z/VM User Reference Manual, LC27-4364*
Describes how to use the product interface and the RACF administration and audit functions. The manual provides reference information for the CARLa command language and the SELECT/LIST fields. It also provides troubleshooting resources and instructions for using the zSecure Collect component. This publication is available to licensed users only.
- *IBM Security zSecure CARLa Command Reference, LC27-6533*
Provides both general and advanced user reference information about the CARLa Auditing and Reporting Language (CARLa). CARLa is a programming language that is used to create security administrative and audit reports with zSecure. The *zSecure CARLa Command Reference* also provides detailed information about the NEWLIST types and fields for selecting data and creating zSecure reports. This publication is available to licensed users only.
- *IBM Security zSecure Documentation CD, LCD7-5373*
Supplies the IBM Security zSecure Manager for RACF z/VM documentation, which contains the licensed and unlicensed product documentation.
- *Program Directory for IBM Security zSecure Manager for RACF z/VM, GI11-7865*
To use the information in this publication effectively, you must have some prerequisite knowledge that you can obtain from the program directory. The *Program Directory for IBM Security zSecure Manager for RACF z/VM* is intended for the systems programmer responsible for installing, configuring, and deploying the product. It contains information about the materials and procedures associated with installing the software. The Program Directory is provided with the product tape. You can also download the latest copies from the IBM Knowledge Center for IBM Security zSecure Manager for RACF z/VM.

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 IBM Education website at <http://www.ibm.com/training>.

For hands-on exercises to help you understand the basics of the CARLa command language, see zSecure CARLa Training at https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Wa6857722838e_491e_9968_c8157c8cf491/page/zSecure%20CARLa%20Training.

Support information

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

Statement of Good Security Practices

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

Chapter 1. Overview

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.

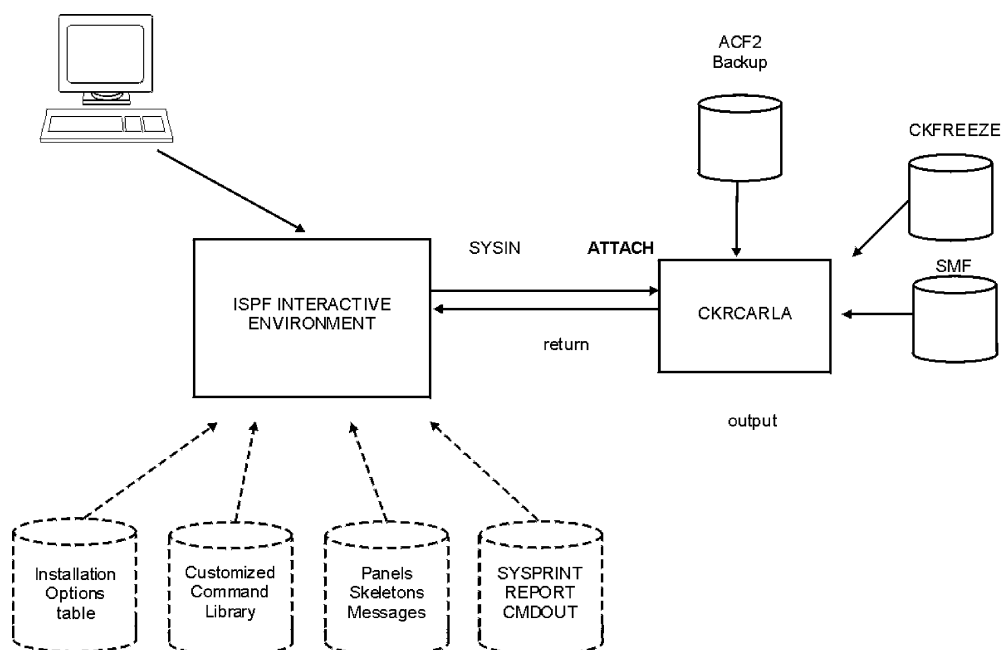


Figure 1. Conceptual data flow

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 is command-driven by using the CARLa Auditing and Reporting Language (CARLa). The commands are explained in the *IBM Security zSecure CARLa Command Reference*.

A typical user, using ISPF, does not need to be concerned with CARLa. The commands are generated automatically and sent to the application program. Except for the few comments here, this guide does not describe the CARLa command language, but concentrates on using the product interactively through ISPF.

The command language is generally used to generate customized reports and to use the product in batch mode. Because the standard reports are comprehensive, you might not ever need customized reports, but you can create them if necessary. Batch use is attractive as part of a security monitoring function. For example, you can use a scheduled batch job to automatically run monitoring checks and reports.

A comprehensive set of sample reports is available in a data set called the CARLa library. This library has a low-level qualifier of SCKRCARL and is often referred to with the default ddname CKRCARLA.

Data sources

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.

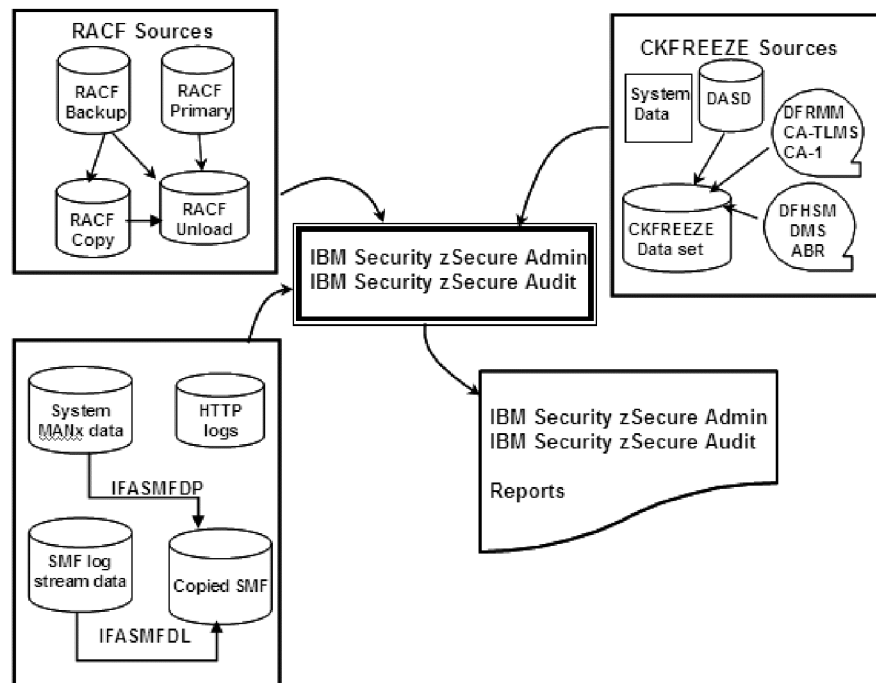


Figure 2. zSecure Audit for ACF2 Input Sources

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 IFASMFDL or IFASMFDL programs. These IBM programs unload SMF records as follows: the IFASMFDL 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

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

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.

GSO See Global System Options.

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

How Privileges influence Logon ID Capabilities											
Privilege	Security Administration Capabilities Allowed with Privileges						Type of Access ALLOWED with Privilege: even though Rule does NOT Permit				
	Create and Delete LIDs	List LIDs	Update LIDs	Data Studio Rules	Rsc Rules	GSO	Data READ any	Data WRITE any	Data ALLOC any	Use Any Resource	Audit Trail Log
Security		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Account	✓	✓	✓								
Audit		✓	List	List	List	List					

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

Field name	Description
DSN()	Data set name: partial or full or High Level Qualifier
LID()	LOGON ID records
UID()	User ID Strings
INF()	Infostorage records

Table 3. Class values

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

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 on page 7 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.

```
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

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

Figure 4. Scope definition for PAYROLL

Scoping by default

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.

```
ACF2 LIST OUTPUT                                     Line 1 of 13
Command ==> _____ Scroll==> CSR_
ACF02002 NOT AUTHORIZED FOR REQUEST

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

Figure 5. LIST Output panel - error message for access attempt outside of scope

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.

```

IBM Security zSecure Audit for ACF2  ACF2_LID display                               Line 1 of 58
Command ==> _____ Scroll==> CSR_
like JSMITH                               9 May 2005 00:09

Identification                                     DEMO
_ACF2 logonid                                     JSMITH
User name                                         JOHN SMITH

Full UID                                           Prefix
NSECMGR                                           JSMITH
Scope                               ScpList  DSNscope LIDscope UIDscope
Scope record names          SECDEPT

Application privileges                               Scopable privileges
Effective TSO setting                               Yes TSO  User has SECURITY privilege  Yes
User can sign on to CICS                               User has ACCOUNT privilege  Yes
User can sign on to IMS                               User has LEADER privilege
User can sign on to IDMS                               User has CONSULT privilege
Effective JOB setting                               Yes JOB  User has AUDIT privilege
Logonid for started tasks

```

Figure 6. SELECT Logon ID (LID) display

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. A good region size value to start with analyzing security is 256 MB. For analyzing compliance or large amounts of SMF, you will need more; start with 512 MB. For just displaying access rules in unrestricted mode, you need much less; 64 MB or even 32 MB might be enough, depending on the size of your security database and the amount of extra information included in the query.

- To open the Main menu, complete the steps in “Opening the Main menu” on page 9.

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.

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

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
      zSecure Audit for ACF2 - ACF2 - Logonid Selection
Option ==>_____ start panel

Show logonids that fit all of the following criteria
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

Output/run options
_ Summarize on UID group
_ Show differences
_ 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

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

The Main menu opens as shown in Figure 8 on page 10.

```

Menu  Options  Info  Commands  Setup
-----
                                zSecure Audit for ACF2 - Main menu
Option ==> _____ More:  +
SE  Setup      Options and input data sets
AA  ACF2       ACF2 Administration
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
LO  Local     Locally defined options
X   Exit      Exit this panel

Input complex:  Active backup ACF2 data base and live SMF data sets

Product/Release
5655-N17 IBM Security zSecure Audit for ACF2 2.2.0

```

Figure 8. IBM Security zSecure Audit for ACF2

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.

```
= 04JUL2004 (July 4, 2004)
< 04JUL2004 (any day before July 4, 2004)
= NEVER      (a date was never set)
= TODAY
= TODAY-3    (three days before today)
< TODAY-30   (more than thirty days ago)
> 01MAR2005  (any day after March 1, 2005)
```

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 4. zSecure Audit for ACF2 navigation characters

Navigation Character	Description
/	Option selection
S	Select for explanation of settings, view audit concerns
L	List to view the ACF2 record as stored on database
AND	Boolean logic – search for combination of attributes
OR	Boolean logic – search for any selected attributes
Y	Boolean logic – search for attribute
N	Boolean logic – do not search for attribute

Chapter 2. Logon ID tasks

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:

- View a Logon ID as stored in the ACF2 database.
- View a Logon ID with explanations of field settings and audit concerns.
- Search for Logon IDs with matching uid strings and display all user IDs that are grouped similarly.
- Find a Logon ID with a specific user name value.
- Display all Logon IDs that have a similar naming convention.
- Display all Logon IDs with powerful privileges.

You can search for any privilege combination by using Boolean logic with AND and OR criteria.

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.

Menu	Options	Info	Commands	Setup

zSecure Audit for ACF2 - Main menu				
Option ==>	AA	More: +		
SE	Setup	Options and input data sets		
AA	ACF2	ACF2 Administration		
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		
LO	Local	Locally defined options		
Input complex: Daily unload and ckfreeze				
Product/Release				
5655-N17 IBM Security zSecure Audit for ACF2 2.2.0				

Figure 10. Main menu

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 on page 14.

Menu	Options	Info	Commands	Setup

IBM Security zSecure – Main Menu				
Option ==>	L	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		
LO	Local	Locally defined options		
X	Exit	Exit this panel		
Input complex: *NONAME*				
Product/Release				
5655-N17 IBM Security zSecure Audit for ACF2 2.2.0				

Figure 11. Select Logon ID overview

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.

Menu	Options	Info	Commands	Setup

IBM Security zSecure Audit for ACF2- ACF2 - Logonid Selection				
Option ==>	_____ _ start panel			
Show logonids that fit all of the following criteria				
Logonid	JSMITH__	(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			
Output/run options				
_ Summarize on UID group				
- Print format	Customize title	Send as email		
Background run	Full page form	Sort differently	Narrow print	

Figure 12. Type your Logon ID

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.

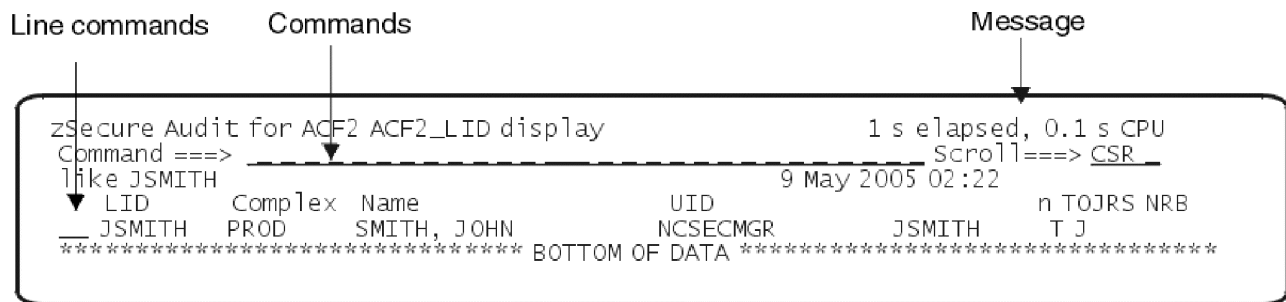


Figure 13. Overview display

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

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

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

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.

```

IBM Security zSecure Audit for ACF2  ACF2_LID display                               Line 1 of 2
Command ==> _____ Scroll==> CSR_
like JSMITH                               9 May 2005 00:09
  LID      Complex  Name                UID                n TOJRS NRB
S_ JSMITH  DEMO    JOHN SMITH          NSECMGR            T J
***** BOTTOM OF DATA *****

```

Figure 14. *SELECT* for more detail

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.

```

IBM Security zSecure Audit for ACF2  ACF2_LID display                               Line 1 of 59
Command ==> _____ Scroll==> CSR_
like JSMITH                               9 May 2005 23:08

  Identification                                     0290
  _ ACF2 logonid                                     JSMITH
  User name                                           JOHN SMITH

  Full UID                                           Prefix
  NSECMGR                                           JSMITH

  Scope          ScpList  DSNscope  LIDscope  UIDscope
  Scope record names  SECDEPT

  Application privileges                               Scopable privileges
  Effective TSO setting                               Yes TSO User has SECURITY privilege  Yes
  User can sign on to CICS                             User has ACCOUNT privilege  Yes
  User can sign on to IMS                             User has LEADER privilege
  User can sign on to IDMS                             User has CONSULT privilege
  Effective JOB setting                               Yes JOB User has AUDIT privilege
  Logonid for started tasks

  Systemwide privileges                               Multi-user privileges
  Allow all access                                     Logonid for MUSASS
  Read/Execute to all data set                         ACF2 updates under users auth
  Bypass tape Label Processing                         Can use /*JOBFROM

  Miscellaneous privileges                               Limitations
  Step-Must-Complete bypassed                         Resource rules validated
  ACF2 refresh allowed                               Data set rules validated
  User can always generate dump                       Can't store rule sets
  Limited BLP                                         Batch only via this program
  Bypass restricted cmd list                         Jobs w/LID through APF only
  Not bound to shifts                               Name of SHIFT record
  Logonid has MAINT privilege                       Source group for access
  User can execute PPGMs                           This LID cannot be inherited
  Dynamic logon privilege                           Barred from Unix Services
  Disable violation counter

  Audit trail                                           Password anomalies
  Write all logons to SMF                             Last invalid pswd attempt  04Dec2004
  Trace all data access                               Input source last invalid pwd  LCL901
  Trace all TSO commands                             # pswd violations on PSWD-DAT  1
  Warn security of all logons                         Pswd violations since logon  0
  # Kerberos key violations  0

  Password phrase anomalies                             Password forced to expire
  PwPhrase effectively allowed  YES                   Case-sensitive password
  # PwP violations on PWP-DATE                         RESTRICT - no password needed
  Last invalid PwP date

```

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
Command ==> _____ Scroll==> CSR
like JSMITH                               9 May 2005 00:09

Access
Logonid has been cancelled          Logonid has been suspended
Cancel/Suspend/Monitor by          since
Suspended: too many pswd vios No
Activation date
Expiration date
Date of last access                04Dec2004 03:17 from LCL900
Last LID record update             4Dec2004
Last password change date          26Oct2004
Maximum password lifetime          Minimum password lifetime

Audit concern
Scoped SECURITY and NORULEVLD, Scoped SECURITY and NORSRCVLD, Can change
password back to old value
***** BOTTOM OF DATA *****
```

Figure 16. End of selected Logon ID display

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 15 on page 17 and Figure 16 show 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 **Scorable 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:

```
SET SCOPE(SCP)
LIST SECDEPT
```

Figure 17. Native ACF2 command example

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.

```
IBM Security zSecure Audit for ACF2 ACF2_LID display          Line 1 of 2
Command ==> _____ Scroll==> CSR_
like JSMITH                      9 May 2005 23:36
  LID      Complex  Name      UID      n TOJRS NRB
L_ JSMITH  DEMO     JOHN SMITH NSECMGR      T J
***** BOTTOM OF DATA *****
```

Figure 18. LIST for more detail

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.

```
ACF2 LIST OUTPUT          Line 1 of 13
Command ==> _____ Scroll==> CSR_
                      DEMO 9 May 2005 23:36
JSMITH      NSECMGR      JOHN SMITH
PRIVILEGES   DEPT(SEC) JOBF(MGR) LOC(NC) JOB TSO
ACCESS       ACC-CNT(116) ACC-DATE(11/10/04) ACC-SRCE(LCL900)
              ACC-TIME(23:51) ENTRIES(116) EXCESS(11/10/04)
              XSTIME(23:51)
PASSWORD     KERB-VIO(0) KERBCURV() MAXDAYS(90) PSWD-DAT(11/08/04)
              PSWD-INV(0) PSWD-SRC(LCL901) PSWD-TIM(00:29)
              PSWD-TOD(10/30/04-17:58) PSWD-VIO(1)
TSO          DFT-PFX(JSMITH) DFT-SUBM(A) INTERCOM JCL LGN-PROC MAIL
              MODE MSGID NOTICES PAUSE PROMPT TSOPROC(TSOPROC2)
              TSORGN(32,000) WTP
STATISTICS   UPD-TOD(11/10/04-23:33)
RESTRICTIONS PREFIX(JSMITH)
***** BOTTOM OF DATA *****
```

Figure 19. Display of a Logon ID via LIST results

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

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

MenuOptionsInfoCommandsSetup

IBM Security zSecure Audit for ACF2 - ACF2 - Logonid Selection

Option ==> _ start panel

Show logonids that fit all of the following criteria

LogonidSYS- (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

Output/run options

_ Summarize on UID group

_ Print format Customize title Send as email

Background run Full page form Sort differently Narrow print

Figure 20. Select Logon IDs using a mask

- 2. Figure 21 displays all logon IDs that begin with SYS, if your organization uses this naming convention.

IBM Security zSecure Audit for ACF2 ACF2_LID display

Line 1 of 938

Command ==> _ Scroll==> CSR_

Like SYS- 9 May 2005 01:19

LID	Complex	Name	UID	n	TOJRS	NRB
- SYS001	DEMO	BENTLEY, JAN	NCSYSMGR	JBENTLE	T J	R
- SYS002	DEMO	CASPER, FRANK	NCSYSPGR	FCASPER	T J	N
- SYS003	DEMO	ABRAMS, MARK	NCSYSPGR	MABRAMS	T J	N
- SYS004	DEMO	WEBSTER, GLENDA	NCSYSANL	GWEBSTER	T J	
- SYS005	DEMO	NICHOLS, JIM	NCSYSADM	JNICHOL	T J	
- SYS006	DEMO	BERT SPECIAL USER	NLSYSPRG	SYS006	T J	B
- SYS007	DEMO	CLARKE, BERT	NLSYSPRG	SYS007	T J	B
- SYS008	DEMO	SNIDER, HANK	NLSYSPRG	SYS008	T J	

Figure 21. Display of logon IDs that match mask SYS-

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.

- 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

- 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-.

MenuOptionsInfoCommandsSetup

IBM Security zSecure Audit for ACF2- ACF2 - Logonid Selection

Option ==>> _ start panel

Show logonids that fit all of the following criteria

Logonid (user id or ACF2 mask)

User's name (name/part of name, no filter)

UID string NCSYS- (string or ACF2 mask)

Additional selection criteria

_ Date fields _ Attributes

Output/run options

_ Summarize on UID group

_ Print format Customize title Send as email

_ Background run Full page form Sort differently Narrow print

Figure 22. List logon IDs with matching uid string

- Press Enter to view the results.

This example, Figure 23, 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.

IBM Security zSecure Audit for ACF2 ACF2_LID display

Line 1 of 706

Command ==>> Scroll==> CSR_

9 May 2005 22:12

All logonids with UID NCSYS-

LID	Complex	Name	UID	n	TOJRS	NRB
JBENTLE	PROD	BENTLEY, JAN	NCSYSMGR	JBENTLE	T J	R
FCASPER	PROD	CASPER, FRANK	NCSYSPGR	FCASPER	T J	N
MABRAMS	PROD	ABRAMS, MARK	NCSYSPGR	MABRAMS	T J	N
GWEBSTER	PROD	WEBSTER, GLENDA	NCSYSANL	GWEBSTER	T J	
JNICHOL	PROD	NICHOLS, JIM	NCSYSADM	JNICHOL	T J	

Figure 23. Display of logon IDs with matching uid string

- Press PF3 to return to the Logon ID Selection panel.

Listing logon IDs with special privileges

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.

MenuOptionsInfoCommandsSetup

zSecure Audit for ACF2 - Logonid Selection

Option ===> _____ _ start panel

Show logonids that fit all of the following criteria

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

Output/run options

_ Summarize on UID group

_ Print format Customize title Send as email

_ Background run Full page form Sort differently Narrow print

Figure 24. Logon ID overview criteria screen

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.
 - 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 on page 23) 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.

MenuOptionsInfoCommandsSetup

zSecure Audit for ACF2 - Logonid Selection

Option ==>>>_____

like -

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 _ PPGM

Restrictions

OR_ _ Rsrcvld _ Rulevld _ Inactive

_ _ Scoped _ Scopelist _ (Only valid if scoped)

Scopable privileges

OR_ _ Security _ Account _ Leader _ Consult

_ _ Audit _

Figure 25. Overtypable 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:”

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. You might want to experiment with this selection logic to display various privilege assignments.

IBM Security zSecure Audit ACF2_LID display

Line 1 of 26

Command ==>>>_____

Scroll==>>> CSR_

like - with scopable privileges ACCOUNT AND SE 9 May 2005 00:21

LID	Complex	Name	UID	n	TOJRS	NRB
PRDBERT	DEMO	BERT SPECIAL USER	NLSYSPRG	PRDBERT	T J	B
BCLARKE	DEMO	CLARKE, BERT	NLSYSPRG	BCLARKE	T J	B
DHOGAN	DEMO	HOGAN, DIANE B	NLTECCON	DHOGAN	T J	B
EANDERS	DEMO	ANDERSON, ERIK	NLDEVPRG	EANDERS	T J	B
GBROWN	DEMO	BROWN, GARY	NLTECMGR	GBROWN	T J	B
HSINDER	DEMO	SNIDER, HANK	NLSYSPRG	HSNIDER	T J	B
MREYNOLD	DEMO	REYNOLDS, MARK	NLDEVPRG	MREYNOLD	TOJ	N B

Figure 26. ACF2_LID display - Scopable privileges report

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:

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.

Menu	Options	Info	Commands	Setup
IBM Security zSecure Audit for ACF2 - ACF2 - Logonid Selection				
Option	====>			
like	-			
Specify groups of criteria the logonids must meet:				
Application privileges				
OR	-	TSO	-	CICS
	-	Batch	-	Restrict
			-	IMS
			-	Started task
			-	IDMS
System privileges				
OR	-	Non-Cancel	-	Readall
	-	Use Jobfrom	-	Maint
			-	Use Tape BLP
			-	PPGM
			-	Lid for Musass
Restrictions				
OR	-	Rsrcvld	-	Rulevld
	-	Scoped	-	Scopelist
			-	Inactive
			-	(Only valid if scoped)
Scopable privileges				
AND	/	Security	/	Account
	-	Audit	-	Leader
			-	Consult

Figure 27. Using Boolean logic to tailor a search

3. Press Enter to view the results.

Displaying all logon IDs with the same user name

About this task

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 on page 25 uses Bert.

MenuOptionsInfoCommandsSetup

IBM Security zSecure Audit for ACF2- ACF2 - Logonid Selection

Option ==> _ start panel

Show logonids that fit all of the following criteria

Logonid (user id or ACF2 mask)

User's name Bert (name/part of name, no filter)

UID string (string or ACF2 mask)

Additional selection criteria

_ Date fields _ Attributes

Output/run options

_ Summarize on UID group

_ Print format Customize title Send as email

_ Background run Full page form Sort differently Narrow print

Figure 28. Search for all users with Bert in the Name field

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.

IBM Security zSecure Audit for ACF2 ACF2_LID display7 s elapsed, 2.4 s CPU

Command ==> Scroll==> CSR_

All logonids with name BERT9 May 2005 01:00

LID	Complex	Name	UID	n	TOJRS	NRB
PRDBERT	DEMO	BERT SPECIAL USER	NLSYSPRG	PRDBERT	T J	B
PRDBER2	DEMO	BERT L. HARRIS	NLDEVPRG	PRDBER2	T J	B
BERTJ01	DEMO	BERT, JOHN	CASALMGR	BERTJ01	T J	
BERTRAMJ	DEMO	BERTRAM, JOHN	CATECSUP	BERTRAMJ	T J	
SMITHA	DEMO	SMITH, ALBERT	NCTECSUP	SMITHA	T J	
SMITHJB	DEMO	J. BERT SMITH	CASECMGR	SMITHJB	T J	
SMITHB01	DEMO	SMITH, BERT	NCPAYCLK	SMITHB01	T J	
SMITHB02	DEMO	SMITH, BERTIE	NCPAYCLK	SMITHB02	T J	
BCLARKE	DEMO	SMITH, BERTIE	NCACCCLK	BCLARKE	T J	

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

Figure 29. Display of matching logon IDs with same Name

Chapter 3. Rule analysis

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

- 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

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		
LO	Local	Locally defines options		
X	Exit	Exit this panel		
Input complex: *NONAME*				
Product/Release				
5655-N17 IBM Security zSecure Audit for ACF2 2.1.1				

Figure 30. Select rules overview

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

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	_____	_____	_ Treat as ACF2 mask
Match data set.	. . .	_____	_____	(no mask)
Match UID string.	. .	_____	_____	(fully specified UID, no mask)
Match UID(s) of LID	_____	_____	_____	(logonid or ACF2 mask)
Additional selection criteria				
_ Other fields				
Output/run options				
/	Show rule lines	_____	By rule set	
	Expand nextkey	_____		
-	Print format	_____	Customize title	Send as email
	Background run	_____	Form oriented	Sort differently
				Narrow print

Figure 31. Rules Selection panel

6. Press Enter to open the ACF2_RULELINE display panel shown in Figure 32 on page 29.


```

IBM Security zSecure Audit ACF2_RULELINE display
Command ==>
All rule lines with HLQ CRM2
x DSN mask
  CRM2.ACCTNG.BACKUP
  CRM2.ACCTNG.MASTER
  CRM2.ACCTNG.MASTER
  CRM2.ACCTNG.-
  CRM2.APPL.CODE
  CRM2.CUSTOMER.MASTER
  CRM2.CUSTOMER.-
x CRM2.D-.-
  CRM2.HELP.FILES
x CRM2.M-.-
x CRM2.PROD.-
  CRM2.SEC.FILES
  CRM2.SEC.INFO
  CRM2.SOFTWARE.-
  CRM2.SYSTEM.LIB
  CRM2.S-.APPS
  CRM2.TEST.APPS
  CRM2.TRACK.USER
  CRM2.VENDOR.ACCTS
  CRM2.VENDOR.LIST
9 May 2011 22:10
UID mask
  **OPS-
  NEACCLK-
  NEACCMGR-
  NEACC-
  NEDEVPRG*****PBAKER-
  NEMKT-
  NEMKT-
  -
  NEHLP-
  -
  -
  NESEC-
  NESECMGR-
  NESYSPRG-
  NESYSPRG*****JSMITH-
  CRMB****CRMBTC1-
  CRMB****CRMBTC1-
  NESECMGR-
  **PUR-
  **PUR-
User

```

Figure 32. Default display when requesting a high-level qualifier or rule key

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 NEACCMGR-.

User column

Indicates whether this entry applies only to this user ID.

- 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.

```

IBM Security zSecure Audit ACF2_RULELINE display
Command ==>
All rule lines with HLQ CRM2
x DSN mask
  CRM2.ACCTNG.BACKUP
  CRM2.ACCTNG.MASTER
  CRM2.ACCTNG.MASTER
  CRM2.ACCTNG.-
  CRM2.APPL.CODE
  CRM2.CUSTOMER.MASTER
  CRM2.CUSTOMER.-
x CRM2.D-.-
  CRM2.HELP.FILES
x CRM2.M-.-
x CRM2.PROD.-
  CRM2.SEC.FILES
  CRM2.SEC.INFO
  CRM2.SOFTWARE.-
  CRM2.SYSTEM.LIB
  CRM2.S-.APPS
  CRM2.TEST.APPS
  CRM2.TRACK.USER
  CRM2.VENDOR.ACCTS
  CRM2.VENDOR.LIST

```

Figure 33. Display of permission parameter values

The rule set in Figure 32 on page 29 shows that any user with a matching uid string of `**0PS` can read and run the data set `CRM2.ACCTNG.BACKUP`. In this example, the uid (`**0PS`) 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

Permission Code	Description
R	Read
W	Write
A	Allocate - create, delete, rename, catalog, uncatalog
E	Execute - applies only to executable code, a program, and not data files

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 (Figure 35 on page 32). The rule lines of the NEXTKEY rule sets can be viewed from Figure 35 on page 32.

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

Menu	Options	Info	Commands	Setup

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	_____	-	Treat as ACF2 mask	
Match data set. . .	_____			(no mask)
Match UID string. .	_____			(fully specified UID, no mask)
Match UID(s) of LID	_____			(logonid or ACF2 mask)
Additional selection criteria				
- Other fields				
Output/run options				
/	Show rule lines	/	By rule set	
-	Expand nextkey			
-	Print format	Customize title	Send as email	
	Background run	Form oriented	Sort differently	Narrow print

Figure 34. The Output/run options

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.

```

Line 1 of 3
IBM Security zSecure ACF2_RULE display
Command ==> Scroll==> CSR_
All rules with HLQ CRM2 30 Aug 2011 04:25
$Key Rs $Prefix LastUpDat StoredBy
CRM2 9Nov2009 CRM2ADM
CRM2D No CRM2 26May2011 CRM2ADM
CRM2LAST No CRM2 26May2011 CRM2ADM
CRM2M No CRM2 26May2011 CRM2ADM
CRM2PROD No CRM2 26May2011 CRM2ADM
CRM2ENOR Yes CRM2 26May2011 CRM2ADM
***** Bottom of Data *****

```

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.

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

```

Line 1 of 3
IBM Security zSecure ACF2_RULE display
Command ==> Scroll==> CSR_
All rules with HLQ CRM2 30 Aug 2011 04:25
$Key Rs $Prefix LastUpDat StoredBy $N
CRM2 9Nov2009 CRM2ADM No
CRM2D No CRM2 26May2011 CRM2ADM No
CRM2LAST No CRM2 26May2011 CRM2ADM No
CRM2M No CRM2 26May2011 CRM2ADM No
CRM2PROD No CRM2 26May2011 CRM2ADM No
CRM2ENOR Yes CRM2 26May2011 CRM2ADM No

```

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

Field	Description
\$Key	\$KEY of the rule set
Rs	Indicates that this rule has ROLESET specified.
\$Prefix	\$PREFIX of the rule set.
LastUpDat	Day this rule record was last stored.
StoredBy	Logon ID that last stored this record.
\$N	The rule set has \$NOSORT specified.
Complex	Name for the ACF2 security database that contains this record.
\$Mode	The \$MODE specified for this rule record.
\$ResOwnr	The SMS default RESOWNER for the data sets protected by the rule set.
\$Owner	\$OWNER field of the rule record.
\$Member	The overriding name of the PDS member into which this rule set should be DECOMPiled.

Table 8. Rule set field descriptions (continued)

Field	Description
\$NR	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.
\$Userdata	\$USERDATA of the rule record.

Displaying data set rules using LIST

Procedure

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.

IBM Security zSecure ACF2_RULE display				Line 1 of 3	
Command ==>				Scroll==> CSR_	
All rules with HLQ CRM2				30 Aug 2011 04:25	
\$Key	Rs	\$Prefix		LastUpDat	StoredBy
L_ CRM2				9Nov2009	CRM2ADM
— CRM2D	No	CRM2		26May2011	CRM2ADM
— CRM2LAST	No	CRM2		26May2011	CRM2ADM
— CRM2M	No	CRM2		26May2011	CRM2ADM
— CRM2PROD	No	CRM2		26May2011	CRM2ADM

Figure 37. Rule overview – List the rule

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.

```

ACF2 DECOMP OUTPUT
Command ==>
Line 1 of 28
Scroll==> CSR_
DEMO 9 May 2005 23:36
ACF75052 ACCESS RULE CRM2 STORED BY DHOGAN ON 11/22/04-13:49
$KEY(CRM2)
ACCTNG.BACKUP UID(**OPS) READ(A) EXEC(A)
ACCTNG.MASTER UID(NEACCCLK) READ(A) WRITE(L) EXEC(A)
ACCTNG.MASTER UID(NEACCMGR) READ(A) WRITE(A) EXEC(A)
ACCTNG.- UID(NEACC) READ(A) EXEC(A)
APPL.CODE UID(NEDEVPRG*****PBAKER) READ(A) WRITE(A) EXEC(A)
CUSTOMER.MASTER UID(NEMKT) READ(A) WRITE(A) EXEC(A)
CUSTOMER.- UID(NEMKT) READ(A) EXEC(A)
D.- UID(*) NEXTKEY(CRM2D)
HELP.FILES UID(NEHLP) READ(A) WRITE(A) EXEC(A)
M.- UID(*) NEXTKEY(CRM2M)
PROD.- UID(*) NEXTKEY(CRM2PROD)
SEC.FILES UID(NESEC) READ(A) EXEC(A)
SEC.INFO UID(NESECMGR) READ(A) WRITE(A) EXEC(A)
SOFTWARE.- UID(NESYSPRG) READ(A) WRITE(A) EXEC(A)
SYSTEM.LIB UID(NESYSPRG*****JSMITH) READ(A) WRITE(A) ALLOC(A) EXEC(A)
S-.APPS UID(CRMB****CRMBTC1) READ(A) EXEC(A)
TEST.APPS UID(CRMB****CRMBTC1) READ(A) EXEC(A)
TRACK.USER UID(NESECMGR) READ(A) WRITE(A) EXEC(A)
VENDOR.ACCTS UID(**PUR) READ(A) WRITE(A) EXEC(A)
VENDOR.LIST UID(**PUR) READ(A) WRITE(A) EXEC(A)
VENDOR.PAYMENT UID(CAACC) READ(A) WRITE(A) EXEC(A)
VENDOR.REC UID(**PUR) READ(A) WRITE(A) EXEC(A)
VENDOR.- UID(**ACC) READ(A) EXEC(A)
XTRA.PROCLIB UID(NESYS) READ(A) WRITE(A) EXEC(A)
XTRA.****LIB UID(NEOPS) READ(A) EXEC(A)
- UID(*)
***** BOTTOM OF DATA *****

```

Figure 38. ACF2 decompiled output of a rule using LIST command

Displaying data set rules using SELECT

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

```

IBM Security zSecure ACF2_RULE display
Command ==>
Line 1 of 10
Scroll==> CSR_
30 Aug 2011 06:36
All rules with HLQ CRM2
$Key Rs $Prefix LastUpDat StoredBy $N
S_ CRM2 26May2011 CRM2ADM No
_ CRM2D No CRM2 26May2011 CRM2ADM No
_ CRM2LAST No CRM2 26May2011 CRM2ADM No
_ CRM2M No CRM2 26May2011 CRM2ADM No
_ CRM2PROD No CRM2 26May2011 CRM2ADM No

```

Figure 39. The Select character

3. Press Enter.

You see a panel similar to Figure 40 on page 35. This is the same rule displayed in Figure 38 and Figure 32 on page 29.

IBM Security zSecure		ACF2_RULE display		Line 1 of 42	
Command ==>				Scroll==> CSR_	
All rules with HLQ CRM2		9 May 2011 22:10			
DSN mask		UID mask		User	
CRM2.ACCTNG.BACKUP		**OPS-			
CRM2.ACCTNG.MASTER		NEACCCCLK-			
CRM2.ACCTNG.MASTER		NEACCMGR-			
CRM2.ACCTNG.-		NEACC-			
CRM2.APPL.CODE		NEDEVPRG*****PBAKER-			
CRM2.CUSTOMER.MASTER		NEMKT-			
CRM2.CUSTOMER.-		NEMKT-			
CRM2.D-.-		-			
CRM2.HELP.FILES		NEHLP-			
CRM2.M-.-		-			
CRM2.PROD.-		-			
CRM2.SEC.FILES		NESEC-			
CRM2.SEC.INFO		NESECMGR-			
CRM2.SOFTWARE.-		NESYSPRG-			
CRM2.SYSTEM.LIB		NESYSPRG*****JSMITH-			
CRM2.S-.APPS		CRMB****CRMBTC1-			
CRM2.TEST.APPS		CRMB****CRMBTC1-			
CRM2.TRACK.USER		NESECMGR-			
CRM2.VENDOR.ACCTS		**PUR-			
CRM2.VENDOR.LIST		**PUR-			

Figure 40. Rule display using Select

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.

```

IBM Security zSecure ACF2_RULE display
Command ==>
All rules with HLQ CRM2
User      Role      Perm N  NextKey  Volume Source  Shift  Library
          R  E
          R w E
          R w E
          R  E
          R w E
          R w E
          C
          C  CRM2D  NORMAL
          R w E
          C  CRM2M
          C  CRM2PROD

```

Figure 41. Display of additional 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

- To view more environmental parameters, press PF11.

```

IBM Security zSecure ACF2_RULE display
Command ==>
All rules with HLQ CRM2
Program DDname  Until    Active  Data
12/31/2011

```

Figure 43. Remaining environmental parameters

ACF2 rules provide date activation and expiration against data set access. Notice the date in Figure 43 under the **Until** column. Access is allowed for a data set until this date is reached. You can press PF10 to scroll left and view the data set name.

Table 9 lists the environmental parameter fields and description, including the fields that are visible on the right when you press PF11.

Table 9. Environmental parameter descriptions

Field	Description
DSN mask	Data sets specified in the rule set, under the high-level qualifier.
UID mask	UID strings specified in rule entries.

Table 9. Environmental parameter descriptions (continued)

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

- 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 DIANE B HOGAN	
SMS ResOwner of rule set		
\$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		
***** BOTTOM OF DATA *****		

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

Entry	Description
Name of this rule set	\$KEY of the rule set.
Roleset access rule	The rule has ROLESET specified.
HLQ(s) to which rules apply	The \$PREFIX of the rule set.
Date of the last rule set update	Day the rule record was last stored.
LID that stored rule set	The LID and NAME of the user that last stored the rule.
SMS ResOwner of rule set	\$RESOWNER field in the rule set. SMS uses this.
\$Owner of this rule set	\$OWNER field in the rule set. Documentation only.
Member in which to DECOMP rule	The overriding name of the PDS member into which this rule set should be decompiled.
Force use of old compiler	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.
Site info on this rule set	\$userdata field if one is present in the rule set.
Non-standard evaluation order	The rule has \$nosort specified.
Action when no entry matches	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.
UIDs that can change rule set	UIDs matching the %change statement if one is present in the rule set.
UIDs that can change entries	UIDs matching the %rchange statement if one is present in the rule set.

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

- Review \$NOSORT settings.
Bypassing ACF2 sorting capability is not recommended. The ACF2 GSO RULEOPTS default sort value is NO\$NOSORT (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.

```

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
L LID that stored rule set     DHOGAN  DIANE B HOGAN
SMS ResOwner of rule set
$Owner of this rule set
Member wherein to DECOMP rule
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
UIDs that can change entries
***** BOTTOM OF DATA *****

```

Figure 45. List logon ID that stored rule set

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.

```
ACF2 LIST OUTPUT                                     Line 1 of 13
Command ==> _____ Scroll==> CSR_
DEMO 9 May 2005 01:21

DHOGAN          NCTECCON  DIANE B HOGAN
                  DEPT(TEC) JOBF9CON) LOC(NC)
PRIVILEGES      ACCOUNT CICS JOB SECURITY TSO
ACCESS          ACC-CNT(120) ACC-DATE(12/17/04) ACC-SRCE(LCL900)
                  ACC-TIME(23:32) ENTRIES(120) EXCESS(12/17/04)
                  XSTIME(23:32)
PASSWORD        KERB-VIO(0) KERBCURV() MAXDAYS(90) PSWD-DAT(12/04/05)
                  PSWD-INV(0) PSWD-SRC(LCL901) PSWD-TIM(00:29)
                  PSWD-TOD(10/26/01-17:33) PSWD-VIO(1)
TSO             DFT-PFX(DHOGAN) DFT-SUBM(A) INTERCOM JCL LGN-PROC MAIL
                  MODE MSGID NOTICES PAUSE PROMPT TSOPROC(TSOPROC2)
                  TSORGN(32,000) WTP
STATISTICS      UPD-TOD(12/17/01-23:32)
RESTRICTIONS    PREFIX(DHOGAN)
***** BOTTOM OF DATA *****
```

Figure 46. ACF2 LIST OUTPUT panel

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**.

```
Menu  Options  Info  Commands  Setup
-----
zSecure Suite - ACF2 - Rules Selection
Command ==> _____ _ start panel

Show rules that fit all of the following criteria
Data set HLQ . . . _____ (qualifier or ACF2 mask)
UID string . . . _____ - Treat as ACF2 mask
Match data set. . . CRM2.VENDOR.ACCTS _____ (no mask)
Match UID string. . _____ (fully specified UID, no mask)
Match UID(s) of LID _____ (logonid or ACF2 mask)

Additional selection criteria
_ Other fields

Output/run options
/ Show rule lines _ By rule set
_ Expand nextkey
_ Print format Customize title Send as email
Background run Form oriented Sort differently Narrow print
```

Figure 47. Request specific data set name

To understand the next display in Figure 48 on page 41, notice the headings **DSN mask** and **UID mask**.

```

IBM Security zSecure ACF2_RULELINE display
Command ==> _____ Scroll==> CSR_
All rule lines with match dsn CRM2.VENDOR.ACCTS 9 May 2011 22:10
  x DSN mask                               UID mask                               User
  --- CRM2.VENDOR.ACCTS                    **PUR-
  --- CRM2.VENDOR.-                        **ACC-
  --- CRM2.-                               -
  --- CRM2.-                               CAACC-
  --- CRM2.-                               NCSUP-
  --- CRM2.-                               NEACC-
  --- CRM2.-                               NEMKT-
  --- CRM2.-                               NEOPS-
  --- CRM2.-                               **SYS-
***** BOTTOM OF DATA *****

```

Figure 48. Rule line entries that match data set name

6. Press PF11 to view the \$Key column heading (Figure 49).

```

IBM Security zSecure ACF2_RULELINE display
Command ==> _____ Scroll==> CSR_
All rule lines with match dsn 'CRM2.VENDOR.ACCT 9 May 2011 22:10
  DSN mask                               Role      Perm      NextKey  Complex  $Key
  --- CRM2.VENDOR.ACCTS                    RW E      DEMO      CRM2
  --- CRM2.VENDOR.-                        R E      DEMO      CRM2
  --- CRM2.-                               DEMO      CRM2
  --- CRM2.-                               R E      DEMO      CRM2LAST
  --- CRM2.-                               r E      DEMO      CRM2LAST
  --- CRM2.-                               R E      DEMO      CRM2LAST
  --- CRM2.-                               R E      DEMO      CRM2LAST
  --- CRM2.-                               r E      DEMO      CRM2LAST
***** BOTTOM OF DATA *****

```

Figure 49. Viewing additional column headings

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.

```

ACF2 DECOMP OUTPUT
Command ==> _____
Line 1 of 28
Scroll==> CSR_
DEMO 9 May 2005 23:36
ACF75052 ACCESS RULE CRM2 STORED BY DHOGAN ON 11/22/04-13:49
$KEY(CRM2)
ACCTNG.BACKUP UID(**OPS) READ(A) EXEC(A)
ACCTNG.MASTER UID(NEACCCLK) READ(A) WRITE(L) EXEC(A)
ACCTNG.MASTER UID(NEACCMGR) READ(A) WRITE(A) EXEC(A)
ACCTNG.- UID(NEACC) READ(A) EXEC(A)
APPL.CODE UID(NEDEVPRG*****PBAKER) READ(A) WRITE(A) EXEC(A)
CUSTOMER.MASTER UID(NEMKT) READ(A) WRITE(A) EXEC(A)
CUSTOMER.- UID(NEMKT) READ(A) EXEC(A)
D.- UID(*) NEXTKEY(CRM2D)
HELP.FILES UID(NEHLP) READ(A) WRITE(A) EXEC(A)
M.- UID(*) NEXTKEY(CRM2M)
PROD.- UID(*) NEXTKEY(CRM2PROD)
SEC.FILES UID(NESEC) READ(A) EXEC(A)
SEC.INFO UID(NESECMGR) READ(A) WRITE(A) EXEC(A)
SOFTWARE.- UID(NESYSPRG) READ(A) WRITE(A) EXEC(A)
SYSTEM.LIB UID(NESYSPRG*****JSMITH) READ(A) WRITE(A) ALLOC(A) EXEC(A)
S-.APPS UID(CRMB****CRMBTC1) READ(A) EXEC(A)
TEST.APPS UID(CRMB****CRMBTC1) READ(A) EXEC(A)
TRACK.USER UID(NESECMGR) READ(A) WRITE(A) EXEC(A)
VENDOR.ACCTS UID(**PUR) READ(A) WRITE(A) EXEC(A)
VENDOR.LIST UID(**PUR) READ(A) WRITE(A) EXEC(A)
VENDOR.PAYMENT UID(CAACC) READ(A) WRITE(A) EXEC(A)
VENDOR.REC UID(**PUR) READ(A) WRITE(A) EXEC(A)
VENDOR.- UID(**ACC) READ(A) EXEC(A)
XTRA.PROCLIB UID(NESYS) READ(A) WRITE(A) EXEC(A)
XTRA.***LIB UID(NEOPS) READ(A) EXEC(A)
- UID(*)
***** BOTTOM OF DATA *****

```

Figure 50. Display of entire CRM2 data set rule

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.

```
IBM Security zSecure ACF2_RULELINE display
Command ==> _____ Scroll==> CSR_
All rule lines with match dsn 'CRM2.VENDOR.ACCT 9 May 2011 22:10
  DSN mask                               UID mask                               User
  -- CRM2.VENDOR.ACCTS                    **PUR-
  -- CRM2.VENDOR.-                        **ACC-
  -- CRM2.-                               -
  -- CRM2.-                               CAACC-
  -- CRM2.-                               NCSUP-
  -- CRM2.-                               NEACC-
  -- CRM2.-                               NEMKT-
  -- CRM2.-                               NEOPS-
  -- CRM2.-                               **SYS-
***** BOTTOM OF DATA *****
```

Figure 51. Analyzing data set access

Follow the data set line to the UID mask column. Press PF11 to scroll and view the permissions (**Perm**) column.

```
IBM Security zSecure ACF2_RULELINE display
Command ==> _____ Line 1 of 18
All rule lines with match dsn 'CRM2.VENDOR.ACCT 9 May 2011 22:10
  DSN mask                               Role      Perm      NextKey  Complex  $Key
  -- CRM2.VENDOR.ACCTS                    RW E      DEMO      CRM2
  -- CRM2.VENDOR.-                        R E      DEMO      CRM2
  -- CRM2.-                               DEMO      CRM2
  -- CRM2.-                               R E      DEMO      CRM2LAST
  -- CRM2.-                               r E      DEMO      CRM2LAST
  -- CRM2.-                               R E      DEMO      CRM2LAST
  -- CRM2.-                               R E      DEMO      CRM2LAST
  -- CRM2.-                               r E      DEMO      CRM2LAST
***** BOTTOM OF DATA *****
```

Figure 52. Analyzing data set access - permissions

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 61 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 61 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.

Menu	Options	Info	Commands	Setup
IBM Security zSecure Audit for ACF2 – Rule				1.2 s CPU, RC=0
Command ==>				_ start panel
Show rules that fit all of the following criteria				
Data set HLQ	. . .		(qualifier or ACF2 mask)	
UID string	. . .	NEACC-	/	Treat as ACF2 mask
Match data set	. . .			(no mask)
Match UID string	. . .			(fully specified UID, no mask)
Match UID(s) of LID				(logonid or ACF2 mask)
Additional selection criteria				
_ Other fields				
Output/run options				
/	Show rule lines	_	By rule set	
	Expand nextkey			
_	Print format	Customize title	Send as email	
	Background run	Form oriented	Sort differently	Narrow print

Figure 53. Rule selection criteria, search by uid string

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.


```

IBM Security zSecure ACF2_RULELINE DISPLAY
Command ==> Scroll==> CSR_
All rule lines with uid NEACC-          9 May 2011 22:10
  DSN mask                               UID mask           User
  — CRM2.ACCTNG.MASTER                 NEACCCLK-
  — CRM2.ACCTNG.MASTER                 NEACCMGR-
  — CRM2.ACCTNG.MASTER                 NEACCMGR-
  — CRM2.ACCTNG.-                      NEACC-
  — CRM2.DAILY.MASTER                 NEACCCLK-
  — CRM2.DAILY.MASTER                 NEACCMGR-
  — CRM2.DAILY.-                      NEACC-
  — CRM2.-                            NEACC-
  — CRM2.MONTHLY.MASTER               NEACCCLK-
  — CRM2.MONTHLY.MASTER               NEACCMGR-
  — CRM2.MONTHLY.-                   NEACC-

```

Figure 54. Results of search for uid string matches in data set rules

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.

```

IBM Security zSecure ACF2_RULELINE DISPLAY
Command ==> Scroll==> CSR_
All rule lines with uid NEACC-          9 May 2011 22:10
  DSN mask          Role    Perm N    NextKey  Complex  $Key
  — CRM2.ACCTNG.MASTER      Rw E      DEMO
  — CRM2.ACCTNG.MASTER      RW E      DEMO
  — CRM2.ACCTNG.MASTER      RW E      DEMO
  — CRM2.ACCTNG.-          R E      DEMO
  — CRM2.DAILY.MASTER      Rw E
  — CRM2.DAILY.MASTER      Rw E
  — CRM2.DAILY.-          R E
  — CRM2.-                R E      DEMO
  — CRM2.MONTHLY.MASTER    Rw E      DEMO
  — CRM2.MONTHLY.MASTER    Rw E      DEMO
  — CRM2.MONTHLY.-        R E      DEMO
***** BOTTOM OF DATA *****

```

Figure 55. Results of search for uid string matches - additional fields

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.

```
Menu  Options  Info  Commands  Setup
-----
zSecure Suite - ACF2 - Rules Selection

Command ==> _____

Show rules that fit all of the following criteria
Data set HLQ . . . CRM2_____ (qualifier or ACF2 mask)
UID string . . . _____ - Treat as ACF2 mask
Match data set. . . _____ (no mask)
Match UID string. . _____ (fully specified UID, no mask)
Match UID(s) of LID _____ (logonid or ACF2 mask)

Additional selection criteria
/ Other fields

Output/run options
/ Show rule lines - By rule set
  Expand nextkey
- Print format      Customize title  Send as email
  Background run    Form oriented   Sort differently  Narrow print
```

Figure 56. Requesting NEXTKEYs for high-level qualifier

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

Menu	Options	Info	Commands	Setup

zSecure Suite - ACF2 - Rules Selection				
Command ==>				
All rule lines with HLQ CRM2				
Specify additional selection criteria:				
Other fields				
Complex	_____		(complex name or ACF2 mask)	
On volume	_____		(volume serial or ACF2 mask)	
Enter "/" to specify inclusion criteria				
/ Program pathing	/ Temporary access	/ Source	/ Shift	
/ No program pathing	/ No temporary access	/ No source	/ No shift	
Permissions (Yes, No, Allow, Log, Prevent; or blank for do not care)				
Read _____	Write _____	Alloc _____	Exec _____	/ NEXTKEY

Figure 57. Request NEXTKEYs for a rule key

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

Menu	Options	Info	Commands	Setup

zSecure Suite - ACF2 - Rules Selection				
Command ==>				
All rule lines with HLQ CRM2				
Specify additional selection criteria:				
Other fields				
Complex	_____		(complex name or ACF2 mask)	
On volume	_____		(volume serial or ACF2 mask)	
Enter "/" to specify inclusion criteria				
/ Program pathing	/ Temporary access	/ Source	/ Shift	
/ No program pathing	/ No temporary access	/ No source	/ No shift	
Permissions (Yes, No, Allow, Log, Prevent; or blank for do not care)				
Read _____	Write _____	Alloc _____	Exec _____	/ NEXTKEY

Figure 58. Initial display for NEXTKEYs chained to parent rule set

To view the **NEXTKEY** column, press PF11 to shift the screen to the right.

The **NextKey** column is displayed as shown in Figure 59 on page 48. This column indicates origination of the pointer from the rule set value in \$Key column.

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.

IBM Security zSecure - ACF2_RULELINE DISPLAY			Line 1 of 12
Command ==>			Scroll==> CSR_
All rule lines with HLQ CRM2, nextkey			9 May 2011 22:10
DSN mask	NextKey	Complex	\$Key
— CRM2.D-.-	CRM2D	DEMO	CRM2
— CRM2.M-.-	CRM2M	DEMO	CRM2
— CRM2.PROD.-	CRM2PROD	DEMO	CRM2
— CRM2.DAILY.-	CRM2LAST	DEMO	CRM2D
— CRM2.MONTHLY.-	CRM2LAST	DEMO	CRM2M
— CRM2.PROD.-	CRM2LAST	DEMO	CRM2PROD
***** BOTTOM OF DATA *****			

Figure 59. NEXTKEYs for requested high-level qualifier

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)

Figure 60. Example rule line

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

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.

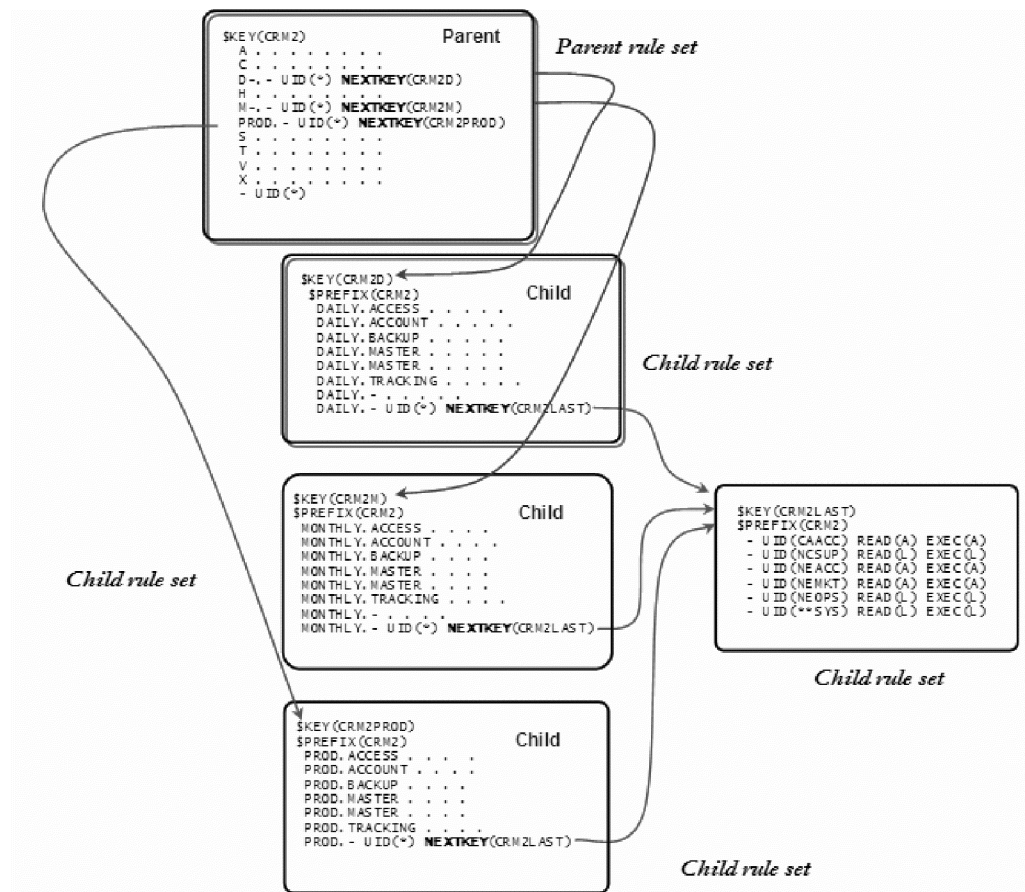


Figure 61. Data set rule structure and NEXTKEYs

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.

```

ACF2 DECOMP OUTPUT
Command ==> _____
Line 1 of 28
Scroll==> CSR
DEMO 9 May 2005 23:36
ACF75052 ACCESS RULE CRM2 STORED BY DHOGAN ON 11/22/04-13:49
$KEY(CRM2)
ACCTNG.BACKUP UID(**OPS) READ(A) EXEC(A)
ACCTNG.MASTER UID(NEACCCLK) READ(A) WRITE(L) EXEC(A)
ACCTNG.MASTER UID(NEACCMGR) READ(A) WRITE(A) EXEC(A)
ACCTNG.- UID(NEACC) READ(A) EXEC(A)
APPL.CODE UID(NEDEVPRG*****PBAKER) READ(A) WRITE(A) EXEC(A)
CUSTOMER.MASTER UID(NEMKT) READ(A) WRITE(A) EXEC(A)
CUSTOMER.- UID(NEMKT) READ(A) EXEC(A)
D-- UID(*) NEXTKEY(CRM2D)
HELP.FILES UID(NEHLP) READ(A) WRITE(A) EXEC(A)
M-- UID(*) NEXTKEY(CRM2M)
PROD.- UID(*) NEXTKEY(CRM2PROD)
SEC.FILES UID(NESEC) READ(A) EXEC(A)
SEC.INFO UID(NESECMGR) READ(A) WRITE(A) EXEC(A)
SOFTWARE.- UID(NESYSPRG) READ(A) WRITE(A) EXEC(A)
SYSTEM.LIB UID(NESYSPRG*****JSMITH) READ(A) WRITE(A) ALLOC(A) EXEC(A)
S-.APPS UID(CRMB****CRMBTC1) READ(A) EXEC(A)
TEST.APPS UID(CRMB****CRMBTC1) READ(A) EXEC(A)
TRACK.USER UID(NESECMGR) READ(A) WRITE(A) EXEC(A)
VENDOR.ACCTS UID(**PUR) READ(A) WRITE(A) EXEC(A)
VENDOR.LIST UID(**PUR) READ(A) WRITE(A) EXEC(A)
VENDOR.PAYMENT UID(CAACC) READ(A) WRITE(A) EXEC(A)
VENDOR.REC UID(**PUR) READ(A) WRITE(A) EXEC(A)
VENDOR.- UID(**ACC) READ(A) EXEC(A)
XTRA.PROCLIB UID(NESYS) READ(A) WRITE(A) EXEC(A)
XTRA.***LIB UID(NEOPS) READ(A) EXEC(A)
- UID(*)
***** BOTTOM OF DATA *****

```

Figure 62. ACF2 Rule List display

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.

Easy to find "How is SYS1.PARMLIB protected?"

```
Menu  Options  Info  Commands  Setup
-----
zSecure Suite - ACF2 - Rules Selection

Command ==> _____

Show rules that fit all of the following criteria
Data set HLQ . . . CRM2_____ (qualifier or ACF2 mask)
UID string . . . _____ - Treat as ACF2 mask
Match data set. . . _____ (no mask)
Match UID string. . _____ (fully specified UID, no mask)
Match UID(s) of LID _____ (logonid or ACF2 mask)

Additional selection criteria
_ Other fields

Output/run options
/ Show rule lines _ By rule set
/ Expand nextkey
_ Print format      Customize title  Send as email
```

Figure 63. Expanded NEXTKEY function

4. Press Enter to view the results as shown in Figure 64 on page 52.

```

IBM Security zSecure - ACF2_RULELINE DISPLAY                               Line 1 of 112
Command ==>                                                                Scroll==> CSR_
All rule lines with HLQ CRM2                                           9 May 2011 02:15
x DSN mask                                                                UID mask                                User
--- CRM2.ACCTNG.BACKUP                                                  **OPS-
--- CRM2.ACCTNG.MASTER                                                  NEACCCLK-
--- CRM2.ACCTNG.MASTER                                                  NEACCMGR-
--- CRM2.ACCTNG.-                                                       NEACC-
--- CRM2.APPL.CODE                                                       NEDEVPRG*****PBAKER-
--- CRM2.CUSTOMER.MASTER                                                NEMKT-
--- CRM2.CUSTOMER.-                                                    NEMKT-
--- x CRM2.D.-                                                           -
--- CRM2.HELP.FILES                                                    NEHLP-
--- x CRM2.M.-                                                           -
--- x CRM2.PROD.-                                                       -
--- CRM2.SEC.FILES                                                      NESEC-
--- CRM2.SEC.INFO                                                       NESECMGR-
--- CRM2.SOFTWARE.-                                                     NESYSPRG-
--- CRM2.SYSTEM.LIB                                                     NESYSPRG*****JSMITH-
--- CRM2.S-.APPS                                                         CRMB****CRMBTC1-
--- CRM2.TEST.APPS                                                       CRMB****CRMBTC1-
--- CRM2.TRACK.USER                                                      NESECMGR-
--- CRM2.VENDOR.ACCTS                                                    **PUR-
--- CRM2.VENDOR.LIST                                                    **PUR-
--- CRM2.VENDOR.PAYMENT                                                  CAACC-
--- CRM2.VENDOR.REC                                                      **PUR-
--- CRM2.VENDOR.-                                                       **ACC-
--- CRM2.XTRA.PROCLIB                                                    NESYS-
--- CRM2.XTRA.***LIB                                                     NEOPS-
--- CRM2.-                                                                -
--- CRM2.DAILY.ACCESS                                                    CAACC-
--- CRM2.DAILY.ACCOUNT                                                  NC-
--- CRM2.DAILY.BACKUP                                                  **OPS-
--- CRM2.DAILY.MASTER                                                  NEACCCLK-
--- CRM2.DAILY.MASTER                                                  NEACCMGR-
--- CRM2.DAILY.TRACKING                                                  NEMKT-
--- CRM2.DAILY.-                                                       NEACC-
--- x CRM2.DAILY.-                                                       -
--- CRM2.-                                                                CAACC-
--- CRM2.-                                                                NCSUP-
--- CRM2.-                                                                NEACC-
--- CRM2.-                                                                NEMKT-
--- CRM2.-                                                                NEOPS-
--- CRM2.-                                                                **SYS-
--- CRM2.MONTHLY.ACCESS                                                  CAACC-
--- CRM2.MONTHLY.ACCOUNT                                                  NC-
--- CRM2.MONTHLY.BACKUP                                                  **OPS-
--- CRM2.MONTHLY.MASTER                                                  NEACCCLK-
--- CRM2.MONTHLY.MASTER                                                  NEACCMGR-
--- CRM2.MONTHLY.TRACKING                                                  NEMKT-
--- CRM2.MONTHLY.-                                                       NEACC-
--- x CRM2.MONTHLY.-                                                       -
--- CRM2.PROD.ACCESS                                                    CAACC-
--- CRM2.PROD.ACCOUNT                                                  NC-
--- CRM2.PROD.BACKUP                                                  **OPS-
--- CRM2.PROD.MASTER                                                    NCACCMGR*****VROBERT
--- CRM2.PROD.MASTER                                                  NEACCCLK-
--- CRM2.PROD.TRACKING                                                  NEMKT-
--- CRM2.PROD.-                                                       NEACC-
--- x CRM2.PROD.-                                                       -
***** BOTTOM OF DATA *****

```

Figure 64. Rule display that shows status of expanded NEXTKEY function for each rule

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.

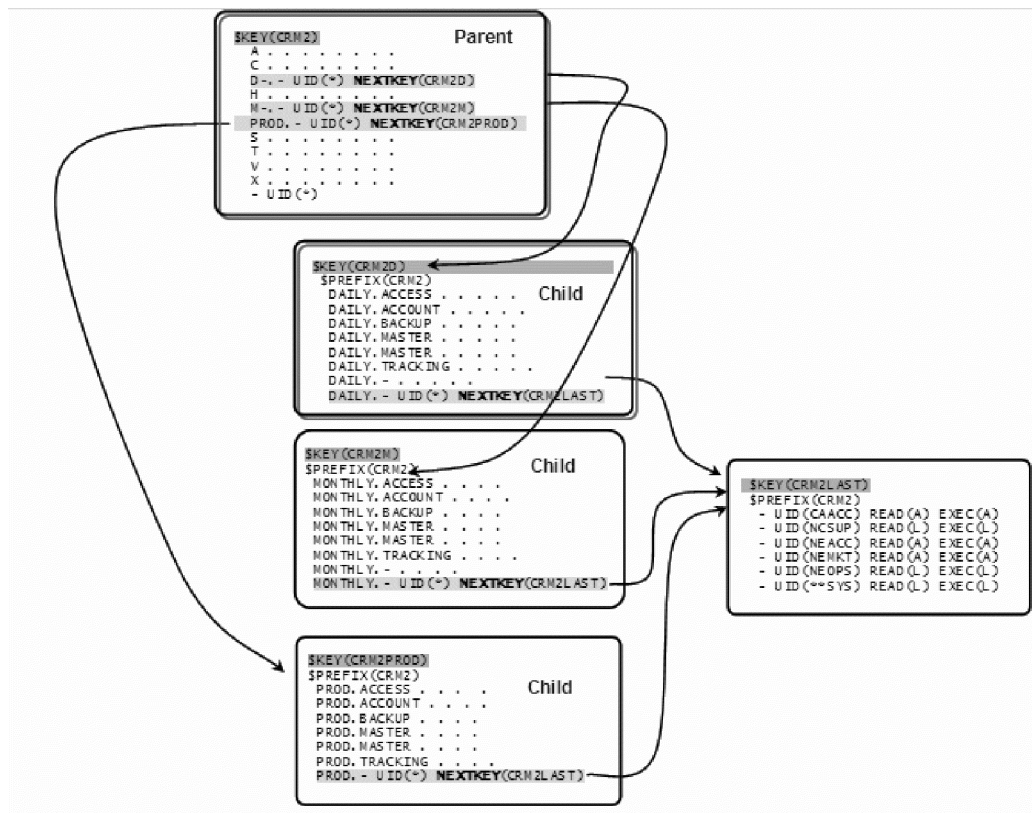


Figure 65. Rule structure

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.

```
IBM Security zSecure - ACF2_RULELINE DISPLAY                               Line 15 of 112
Command ==>                                                                Scroll==> CSR_
All rule lines with HLQ CRM2                                           9 May 2011 02:33
  x DSN mask                                                         NextKey Complex $Key
S_ x CRM2.D-.-                                                         CRM2D      DEMO      CRM2
. . .
. . .
  x CRM2.M-.-                                                         CRM2M      DEMO      CRM2
  x CRM2.PROD.-                                                       CRM2PROD   DEMO      CRM2
. . .
  x CRM2.DAILY.-                                                       CRM2LAST   DEMO      CRM2D
. . .
  x CRM2.MONTHLY.-                                                    CRM2LAST   DEMO      CRM2M
. . .
  x CRM2.PROD.-                                                       CRM2LAST   DEMO      CRM2PROD
. . .
. . .
```

Figure 66. Expanded NextKey function

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

```
IBM Security zSecure - ACF2_RULELINE DISPLAY                               Line 1 of 54
Command ==>                                                                Scroll==> CSR_
All rule lines with HLQ CRM2                                           9 May 2011 02:33
RuleEntry
D-.- UID(*) NEXTKEY(CRM2D)

Nextkey expansion
$Key      DSN mask      UID mask
CRM2      CRM2.D-.-     -
CRM2D     CRM2.DAILY.ACCESS  CAACC-
CRM2D     CRM2.DAILY.ACCOUNT  NC-
CRM2D     CRM2.DAILY.BACKUP   **OPS-
CRM2D     CRM2.DAILY.MASTER   NEACCCLK-
CRM2D     CRM2.DAILY.MASTER   NEACCMGR-
CRM2D     CRM2.DAILY.TRACKING  NEMKT-
CRM2D     CRM2.DAILY.-        NEACC-
CRM2D     CRM2.DAILY.-        -
CRM2LAST  CRM2.-           CAACC-
CRM2LAST  CRM2.-           NCSUP-
CRM2LAST  CRM2.-           NEACC-
CRM2LAST  CRM2.-           NEMKT-
CRM2LAST  CRM2.-           NEOPS-
CRM2LAST  CRM2.-           **SYS-
```

Figure 67. Expanded NEXTKEY function

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)

```

IBM Security zSecure - ACF2_RULELINE DISPLAY                               Line 21 of 54
Command ==> _____ Scroll==> CSR_
All rule lines with HLQ CRM2                                           9 May 2011 02:33

Evaluation order
Name of this rule set          CRM2
Roleset access rule           No
Sequence number                8
DSN to which rule applies
Entry valid for these volumes
UIDs for which entry is valid
Entry valid for this Source
Entry valid for this Shift
LIB in which PGM must reside
PGM to use for access
DD for which rule is valid
Last date this entry is valid
First day this entry is valid

Action on match
Types of access allowed
$Key for further evaluation
Site info on this entry

Rule attributes
Name of this rule set          CRM2
HLQ(s) to which rules apply
Date of last rule set update   22Nov2004
LID that stored rule set       RCCSLIN
SMS ResOwner of rule set
$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
UIDs that can change entries
***** BOTTOM OF DATA *****

```

Figure 68. Additional rule information

The expanded NEXTKEY provides a great visual for understanding rule structures. Without this capability, NEXTKEY branching is difficult to follow.

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.

Menu	Options	Info	Commands	Setup

IBM Security zSecure - ACF2 -			3.1 s CPU, RC=0	
Command ==>			_ start panel	
Show rules that fit all of the following criteria				
Data set HLQ . . .	CRM2		(qualifier or ACF2 mask)	
UID string			_ Treat as ACF2 mask	
Match data set. . .			(no mask)	
Match UID string. .			(fully specified UID, no mask)	
Match UID(s) of LID			(logonid or ACF2 mask)	
Additional selection criteria				
_ Other fields				
Output/run options				
/ Show rule lines	-	By rule set		
- Print format		Customize title	Send as email	
- Background run		Form oriented	Sort differently	Narrow print

Figure 69. Preparation for viewing individual rule line

4. Press Enter to open the Rule display panel shown in Figure 70.

IBM Security zSecure ACF2_RULELINE display		
Command ==>		Scroll==> CSR_
All rule lines with HLQ CRM2		9 May 2005 22:10
DSN mask	UID mask	User
CRM2.ACCTNG.BACKUP	**OPS-	
CRM2.ACCTNG.MASTER	NEACCCLK-	
CRM2.ACCTNG.-	NEACC-	
CRM2.APPL.CODE	NEDEVPRG*****PBAKER-	
CRM2.CUSTOMER.MASTER	NEMKT-	
CRM2.CUSTOMER.MASTER	NEMKT-	
CRM2.CUSTOMER.-	NEMKT-	
CRM2.D-.-	-	
S CRM2.HELP.FILES	NEHLP-	
CRM2.HELP.FILES	NEHLP-	
CRM2.M-.-		

Figure 70. Viewing rule lines for selected high-level qualifier

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.

```

IBM Security zSecure ACF2_RULELINE display                               Line 1 of 36
Command ==>                                                            Scroll==> CSR_
All rule lines with HLQ CRM2                                           9 May 2011 22:10

RuleEntry
CRM2.HELP.FILES UID(NEHLP) READ(A) WRITE(A) EXEC(A)

Evaluation order
Name of this rule set          CRM2
Roleset access rule           No
Sequence number                9
DSN to which rule applies     CRM2.HELP.FILES
Entry valid for these volumes
UIDs for which entry is valid NEHLP-
Entry valid for this Source
Entry valid for this Shift
LIB in which PGM must reside
PGM to use for access
DD for which rule is valid
Last date this entry is valid
First day this entry is valid

Action on match
Types of access allowed       READ(A) WRITE(A) EXEC(A)
$Key for further evaluation
Site info on this entry

Rule attributes
Name of this rule set          CRM2
HLQ(s) to which rules apply
Date of last rule set update  22Nov2004
LID that stored rule set      DHOGAN  DIANE HOGAN
- SMS ResOwner of rule set
$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
UIDs that can change entries
***** BOTTOM OF DATA *****

```

Figure 71. Additional rule line details

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

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.

```

Menu  Options  Info  Commands  Setup
-----
                                zSecure Audit for ACF2
Option ==>  I _____ 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
LO  Local      Locally defined options
X   Exit       Exit this panel

Input complex: *NONAME*

Product/Release
5655-N17 IBM Security zSecure Audit for ACF2 2.1.1

```

Figure 72. Select Resource rules overview

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.

```

Menu  Options  Info  Commands  Setup  StartPanel
-----
IBM Security zSecure - ACF2 - Resource
Command ==> _____

Show resource rules that fit all of the following criteria
Resource type . . . . . *** Resource class . . . . . _____
Resource key . . . . . _____ / ACF2 mask
UID string . . . . . _____ _ Treat as ACF2 mask
Match resource . . . . . _____
Match UID string . . . . . _____ (full UID, no mask)
Match UID(s) of LID . . . . . _____ (logonid or ACF2 mask)

Additional selection criteria
_ Other fields

Output/run options
_ Show rule lines / By rule set _ Prefix rule line _ No trunc.
_ Expand nextkey
_ Use resident dir
_ Print format Customize title Send as email
_ Background run Form oriented Sort differently Narrow print

```

Figure 73. Mask the resource type field to view all resource types

- b. Press Enter.

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).

IBM Security zSecure ACF2_INFORULE summary					Line 1 of 17
Command ==>					Scroll==> CSR_
All resource rules with type ***					9 May 2005 23:51
Type	#Rules	Max Len	Total Len		
— FAC	56	600	11286		
— HFS	144	4582	125626		
— IXC	2	309	618		
— OPR	3	1676	7012		
— PDS	6	194	1132		
— SAF	14	297	3382		
— SDF	20	1046	7128		
— SFP	4	363	1130		
— SPL	6	459	1750		
— SUR	14	255	3138		
— TCI	8	244	1952		
— TGR	4	202	792		
— TSQ	16	422	3854		
— TSS	14	284	3192		
— TST	3368	947	500216		
— TS3	4	250	894		
— VTA	2	236	472		
***** BOTTOM OF DATA *****					

Figure 74. List of resource rule type codes.

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. This selection criteria finds the users who have access to the MVS eight-character resource class name - OPERCMDS uid(.....) within the uid NESYSPRG.

Menu	Options	Info	Commands	Setup	StartPanel
IBM Security zSecure Audit for ACF2 - Resource					0.2 s CPU, RC=0
Command ==>					
Show resource rules that fit all of the following criteria					
Resource type	___	Resource class	OPERCMD5		
Resource key	_____ / ACF2 mask				
UID string	_____ _ Treat as ACF2 mask				
Match resource	_____				
Match UID string . . .	NESYSPRG (full UID, no mask)				
Match UID(s) of LID . .	_____ (logonid or ACF2 mask)				
Additional selection criteria					
_ Other fields					
Output/run options					
_ Show rule lines		/	By rule set	_ Prefix rule line	_ No trunc.
_ Expand nextkey					
_ Use resident dir					
_ Print format		Customize title	Send as email		
_ Background run		Form oriented	Sort differently		Narrow print

Figure 75. Display of resource rule JES* within the class OPERCMDS.

Chapter 4. Infostorage records

Scope and cross-reference 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 11. InfoStorage database class values and descriptions

ClassValues	Description
C	Control records
D	DB2 records
E	Entry records
F	Field records
I	Identity records
M	Mandatory Access Control
P	Profile records
R	Resource Rule records
S	Scope records SCP
T	Shift records
V	ACF2/VAX records
X	Cross-reference records SGP, RGP, ROL

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.
- 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 on page 63.

Menu	Options	Info	Commands	Setup

zSecure Audit for ACF2 – Main menu				
Option	====>	S	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		
LO	Local	Locally defined options		
X	Exit	Exit this panel		
Input complex: *NONAME*				
Product/Release				
5655-N17 IBM Security zSecure Audit for ACF2 2.2.0				

Figure 76. Select Infostorage record overview

- 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.

Menu	Options	Info	Commands	Setup	StartPanel

IBM Security zSecure Audit for ACF2 - ACF2 - Infostorage					
Command ==>					
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		Customize title		Send as email	
_ Background run		Form oriented		Sort differently Narrow print	

Figure 77. Infostorage record selection criteria.

- 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 78 on page 64.

```

IBM Security zSecure Audit for ACF2 ACF2_INFO display      0 s elapsed, 0.1 s CPU
Command ==> Scroll==> CSR_
All infostorage S-SCP records with key -                9 May 2005 22:10
  Rest Key                                             LastUpDat StoredBy Complex
  — SSCP ACCTSCP                                     28Sep2004 RCCPROD DEMO
  — SSCP CRM2SCP                                     13Jan2005 CRMBMRX DEMO
  — SSCP INVENTORY                                   13Jan2005 CRMBMRX DEMO
  — SSCP OPERATNS                                    13Jan2005 CRMBMRX DEMO
  — SSCP MARKETNG                                   13Jan2005 CRMBMRX DEMO
  — SSCP PAYROLL                                    10Mar2005 CRMBMRX DEMO
  — SSCP SECURITY                                    13Jan2005 JSMITH DEMO

```

Figure 78. Scope record key display

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.

```

IBM Security zSecure Audit for ACF2 ACF2_INFO display      0 s elapsed, 0.1 s CPU
Command ==> Scroll==> CSR_
All infostorage S-SCP records with key -                9 May 2005 22:10
  Rest Key                                             LastUpDat StoredBy Complex
  — SSCP ACCTSCP                                     28Sep2004 RCCPROD DEMO
  S_ SSCP COSTING                                    13Jan2005 CRMBMRX DEMO
  — SSCP INVENTORY                                   13Jan2005 CRMBMRX DEMO
  — SSCP OPERATNS                                    13Jan2005 CRMBMRX DEMO
  — SSCP MARKETNG                                   13Jan2005 CRMBMRX DEMO
  — SSCP PAYROLL                                    10Mar2005 CRMBMRX DEMO
  — SSCP SECURITY                                    13Jan2005 JSMITH DEMO

```

Figure 79. Selecting an individual scope record

2. Press Enter to open the display panel as shown in Figure 80 on page 65.

```

IBM Security zSecure Audit for ACF2 ACF2_INFO display          Line 1 of 19
Command ==> _____ Scroll==> CSR_
All infostorage S-SCP records with key -          9 May 2005 22:10

Record attributes
Id for resident record types      SSCP
Name of this InfoStg record      COSTING
Date of last rule set update      10Mar2005
- LID that stored rule set        SMITHINM   MARTIN SMITHEN
Key for further evaluation

LID records in scope
- CRM2-
UID strings in scope
COST-
Data set HLQs in scope
- COST-
InfoStorage scope

```

Figure 80. Detail display of a scope record.

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.

```

Menu  Options  Info  Commands  Setup          StartPanel
-----
IBM Security zSecure Audit for ACF2 - ACF2 - Infostorage
Command ==> _____

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

```

Figure 81. Infostorage record selection criteria – cross-reference record selection.

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.

```

IBM Security zSecure Audit for ACF2 ACF2_INFO display      0 s elapsed, 0.1 s CPU
Command ==> Scroll==> CSR
All infostorage X-RGP records with key -                9 May 2005 22:10
  Rest Key                                             LastUpDat StoredBy Complex
s_ XRGP ACCOUNTS                                     21Feb2005 CRMBNAP DEMO
  XRGP ACCTPAY                                       21Feb2005 CRMBNAP DEMO
  XRGP ACCTREV                                       21Feb2005 CRMBNAP DEMO
  XRGP BLLTXS                                       19Feb2005 CRMBNAP DEMO
  XRGP GR1                                          19Feb2005 CRMBNAP DEMO
  XRGP GR2                                          19Feb2005 CRMBNAP DEMO
  XRGP GR3                                          19Feb2005 CRMBNAP DEMO
  XRGP GR4                                          19Feb2005 CRMBNAP DEMO
  XRGP GR5                                          19Feb2005 CRMBNAP DEMO
  XRGP GR6                                          19Feb2005 CRMBNAP DEMO
  XRGP MULTITYPE                                    14Dec2005 CRMBNAP DEMO
  XRGP PWR                                          19Feb2005 CRMBNAP DEMO
  XRGP SG1                                          19Feb2005 CRMBNAP DEMO
  XRGP SG2                                          19Feb2005 CRMBNAP DEMO
  XRGP SG3                                          20Feb2005 CRMCPRP DEMO
  XRGP SG4                                          19Feb2005 CRMBNAP DEMO
  XRGP SG5                                          20Feb2005 CRMCPRP DEMO
  XRGP SG6                                          20Feb2005 CRMCPRP DEMO
  XRGP SMFTEST                                       25Jul2005 CRMBNAP DEMO
  XRGP WHATEVER                                       5Apr2005 CRMBNAP DEMO
  XRGP XCOLL                                         19Feb2005 CRMBNAP DEMO
  XRGP X001                                          7Nov2004 CRMBNAP DEMO
***** BOTTOM OF DATA *****

```

Figure 82. Infostorage record selection criteria

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, the XRGP ACCOUNTS record is selected.
2. Press Enter to open the display panel as shown in Figure 83.

```

IBM Security zSecure Audit for ACF2 ACF2_INFO display      Line 1 of 18
Command ==> Scroll==> CSR_
All infostorage X-RGP records with key -                9 May 2005 22:10

Record attributes
Id for resident record types  XRGP
Name of this InfoStg record   ACCOUNTS
Date of last rule set update  21Feb2005
_ LID that stored rule set     CRMBNA2  ERIK VAN DER NAT
_ Sysid                       TEST
_ Grouping record              Yes

Applicable $TYPES

Include
ACCTPAY
ACCTREV

Exclude

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

```

Figure 83. Detail display of a cross-reference group record.

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

Using SETUP functions, 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

zSecure Audit for ACF2 - Setup				
Command ==> _____				
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.

Menu	Options	Info	Commands

zSecure Audit for ACF2 - Setup - New files			
Command ==> _____			
Create new unload file from the ACF2 database and/or CKFREEZE file			
data set with unload from ACF2 database, use UNLOAD as last qualifier			
Unload _____			
I/O configuration file, use CKFREEZE as last qualifier			
Ckfreeze _____			
Description for this set of input files			
Description . . . _____			
Enter data set names and description and press ENTER			

Figure 85. New files panel

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.

Menu	Options	Info	Commands

zSecure Audit for ACF2 - Setup - New files			
Command ==> _____			
Create new unload file from the ACF2 database and CKFREEZE file			
Data set with unload from ACF2 database, use UNLOAD as last qualifier			
Unload _____			
I/O configuration file, use CKFREEZE as last qualifier			
Ckfreeze _____			
Description for this set of input files			
Description . . . _____			
Enter data set names and description and press ENTER			

Figure 86. Typical allocation panel

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 DASD volume, plus space for catalog and HSM information, as well as 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.

Menu	Options	Info	Commands

zSecure Audit for ACF2 - Setup - Input f Row 2 from 5			
Command ==> _____ Scroll ==> CSR_			
Description Your description for this set of input files _____			
Complex _____ Version _____			
Enter data set names and types. Type END or press F3 when complete.			
Enter dsname with .* to get a list Type SAVE to save set, CANCEL to quit.			
Valid line commands: E I R D Type REFRESH to submit unload job.			
Data set or DSNPREF= or UNIX file name _____ Type _____ NJE node _____			
- _____			

Figure 87. Input file panel to define data set definition

Refreshing and loading files

About this task

The data sets listed constitute one input set. An input set can contain multiple CKFREEZE data sets, multiple SMF files, and multiple HTTP log files. However, an input set can contain only one 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 LNKLIST, 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 145.

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.

Menu	Options	Info	Commands

zSecure Audit for ACF2 - Setup - Input file			I Row 1 from 4
Command ==> _____			Scroll ==> CSR_
(Un)select (U/S/C/M) set of input files or work with a set (B, E, R, I, D or F)			
Description			Complex
-	UNLOAD and CKFREEZE data sets created 8 Apr 2005		selected
-	Active backup ACF2 data base	DEMO	selected
-	Active primary ACF2 data base	DEMO	
-	Active backup ACF2 data base and live SMF data sets	DEMO	selected
***** Bottom of data *****			

Figure 88. Input set selection

In Figure 88, the input file sets marked as selected indicate that the product is now using these input sets for its input data. The other three input sets, such as active primary and backup ACF2 databases, are always present. You can switch to any input set defined in this display. For example, to switch between the unloaded files you created and the live ACF2 databases, go to this panel and select the appropriate input set.

Entering **S** before any choice in this panel causes the product to select this set for input. You can change input selections many times during a session, although this is not typical usage.

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

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.

Menu	Options	Info	Commands	Setup	Startpanel

zSecure Suite - Setup - Collections					
Command ==> _____					
Enter description for new collection of input sets					

Figure 89. Setup collections definition panel

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

Menu	Options	Info	Commands	Setup	Startpanel

zSecure Suite - Setup - Collections					
Row 1 from 2					
Command ==> _____ Scroll ==> CSR					
(Un)select (U/S) collection or work with a collection (E, R, I, or D)					
Description					
_ Collection for systems of SYSPLEX TEST selected					
_ Collection for systems of SYSPLEX PROD					
***** Bottom of data *****					

Figure 90. Setup collections display

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

zSecure Suite - Setup - Collections				Row 1 from 6
Command ==> _____				Scroll ==> CSR
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 then 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

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.

```

Menu  Options  Info  Commands  Setup
-----
                                zSecure Audit for ACF2 – Main menu
Option  ==> AU
More:    +

SE  Setup      Options and input data sets
AA  ACF2       ACF2 Administration
AU  Audit      Audit security and system resources
  C  Change track  Track changes to the system
  L  Libraries    Library status and update analysis
  R  Compliance   Rule-based compliance evaluation
  S  Status       Status auditing of security and system tables/options
RE  Resource    Resource reports
EV  Events      Event reporting from SMF and other logs
CO  Commands    Run commands from library
IN  Information  Information and documentation
LO  Local       Locally defined options
X   Exit        Exit this panel

Input complex: *NONAME*

Product/Release
5655-N17 IBM Security zSecure Audit for ACF2 2.2.0

```

Figure 92. Main menu - select AU option

4. To select status, type S in the command line as shown in Figure 93.

```

Menu  Options  Info  Commands  Setup
-----
                                zSecure Audit for ACF2 – Main menu
Option  ==> S
More:    +

SE  Setup      Options and input data sets
AA  ACF2       ACF2 Administration
AU  Audit      Audit security and system resources
  C  Change track  Track changes to the system
  L  Libraries    Library status and update analysis
  R  Compliance   Rule-based compliance evaluation
  S  Status       Status auditing of security and system tables/options
RE  Resource    Resource reports
EV  Events      Event reporting from SMF and other logs
CO  Commands    Run commands from library
IN  Information  Information and documentation
LO  Local       Locally defined options
X   Exit        Exit this panel

Input complex: *NONAME*

Product/Release
5655-N17 IBM Security zSecure Audit for ACF2 2.2.0

```

Figure 93. Select S for audit status

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.


```

Menu Options Info Commands Setup
-----
zSecure Audit for ACF2 - Audit - Status
Command ==>

Enter / to select report categories
- MVS tables           MVS oriented tables (reads first part of CKFREEZE)
- MVS extended         MVS oriented tables (reads whole CKFREEZE)
/ ACF2 control          ACF2 oriented tables
- ACF2 user            User oriented ACF2 tables and reports
- ACF2 resource        Resource oriented ACF2 tables and reports

Select options for reports:
- Select specific reports from selected categories
/ Include audit concern overview in overall prio order
/ Only show reports that may contain audit concerns
- Minimum audit priority for audit concerns (1-99)
- Show differences
- Print format
- Background run

Audit policy
/ zSecure
- C1
- C2
- B1
- Concise (short) report

```

Figure 94. Select ACF2 control

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.

```

IBM Security zSecure Audit for ACF2 Display Selection    11 s elapsed, 2.9 s CPU
Command ==> Scroll==> CSR_

Name      Summary Records Title
S OVERVIEW 10      0 Audit concern overview by priority (higher prioritie
- GSO      1      1 GSO system settings
- GSOAUDIT 1      10 GSO system settings - audit concerns
- CLASMAP  1      164 Effective CLASMAP settings
- FDE      2      621 ACF2 Field Definition Entries
***** BOTTOM OF DATA *****

```

Figure 95. Select Overview to display audit concerns

Reviewing audit concerns overview by priority

Procedure

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.

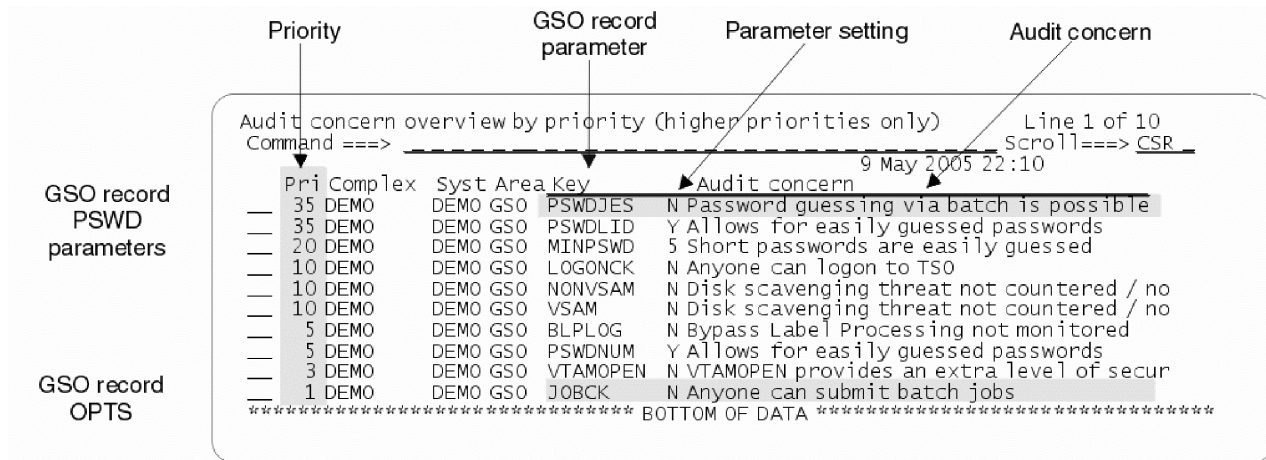


Figure 96. Audit concern overview panel

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

Value	Meaning
0-10	informational
10-20	desired
20-40	review required
40 and up	serious exposure

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 NPSWDJES 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, PSWDFRC, PASSLMT(3), MAXTRY(3), PSWDALPH, PSWDNMIC, PSWDMIN(1), PSWDPAIR(2), PSWDSIM(3), PSWDNAGE, PSWXHST, PSWXHST#(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 / PSWD LAST CHANGED BY JSMITH ON 11/26/00-14:31
  MAXTRY(2) MINPSWD(5) PASSLMT(4) PSWDALT PSWDFRC 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

Procedure

1. Press PF3 to the open the ACF2 Display Selection panel as shown in Figure 100 on page 80.

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.

```

IBM Security zSecure Audit for ACF2 Display Selection                               Line 1 of 5
Command ==>                                                                    Scroll==> CSR

  Name      Summary Records Title
- OVERVIEW    10      0 Audit concern overview by priority (higher prioritie
S GSO         1       1 GSO system settings
- GSOAUDIT    1      10 GSO system settings - audit concerns
- CLASMAP     1     164 Effective CLASMAP settings
- FDE         2     621 ACF2 Field Definition Entries
***** BOTTOM OF DATA *****

```

Figure 100. Select GSO system settings

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.

```

GSO system settings                                                              Line 1 of 75
Command ==>                                                                    Scroll==> CSR

  Complex  System  Collect time stamp
  0290     0290   current settings

Option settings (OPTS)
Mode
Reports are scoped  RPTSCOPE No      Records TSO cmd      CMDREC No
CPU Time           CPUTIME  LOCAL   Date format         DATE  MM/DD/YY
Batch default LID   DFTLID   Check for JOB priv   JOBCK  No
Show last logon time NOTIFY Yes    Protect Tape DSN     TAPEDSN No
Sess. violation limit MAXVIO 10     Logonid in SMF       STAMPSMF No
LID expiration # days WRNDAYS 5     Check VTAM ACBs     VTAMOPEN No
TSO UADS            UADS    No      Log all BLP usage    BLPLOG No
STC default LID     DFTSTC  ACFSTCID Can list any infost. records SeAu
Start only marked STCs STC    Yes    ACCESS subcommand enabled Yes
LDAP Directory Services LDS   No     Hide inaccessible ds NAMEHIDE No
Use ICSF for encryption ICSF No

Backup parameters (BACKUP)              TSO related settings (TSO)
Backup time                             TIME 06:00 Check for TSO priv LOGONCK No
Backup CPU id                           CPUID 0290 TSO logon supports a PWPHRASE No
Backup workunit                          WORKUNIT SYSALLDA
Backup command string STRING S ACFBKUP2

```

Figure 101. GSO system settings (Screen 1)

```

GSO system settings
Command ==>
Line 26 of 75
Scroll==> CSR

Password settings (PSWD)
Maximum tries          MAXTRY  2      Minimum length        MINPSWD  5
Daily pswd limit       PASSLMT  4      Warning days          WRNDAYS  5
Default MaxDays        PSWDMAX          Check pswd history    PSWDHST  Yes
Default MinDays        PSWDMIN          Effective pswd history # 4
JES updates Pswd-Vio   PSWDJES  No     Extended pswd hist    PSWXHIST No
Force pswd change      PSWDFRC  Yes    Extended pswd hist #  PSWXHST# 0
Change pswd at logon   PSWDALT  Yes    Similar char checking PSWDSIM  2
Volatile temp pswds    PSWNAGE  No     Extract password      PSWDXTR  No
Allow ACF CH pswd      PSWDCH  Yes    Pswd=LID allowed     NOPSWDLID Yes
New LIDs need pswd     PSWDREQ  Yes    Allow all-numeric     NOPSWDNUM No
Allow password verify   PSWDVFY  No     Use RESWORD table     PSWDRSV  Yes
# consecutive          PSWDPAIR  1     Req alphabetic char   PSWDALPH Yes
Allow vowels           PSWDVOWL  Yes    Req numeric char      PSWDNMIC  Yes
Case-sensitive pswds   PSWDMIXD  No     Req nat./special chr  PSWDSPLT No
Pswd needs uppercase   PSWDUC   No     LID in passwords      PSWDPLID  Yes
Pswd needs lowercase   PSWDLCL  No     Part of name in pswd  PSWDNAME
Logon ok: reset vio#   CLEARVIO No     Password encryption    PSWDENCT  XDES
Non-std chars allowed in pswd &!*%_ =

Password phrase settings (PWPHRASE)
PwP usage for all users ALLOW No      Max PwP length        MAXLEN 100
Age temporary PwPs     TEMP-AGE Yes   Min PwP length        MINLEN  9
Max PwP age (days)    MAXDAYS          Warning days for PwP  WARNDAYS  1
Min PwP age (days)    MINDAYS          PwP history size      HISTORY   0
Permit PwP change      CMD-CHG Yes   Min numerics in PwP    NUMERIC   0
EXTRACT calls for PwP  EXTRACT No     Min alphabetics in PwP ALPHA   0
Permit Logon ID in PwP LID Yes        Min spec. chr. in PwP SPECIAL  0
Min words in PwP       MINWORD  1     Max rep. chars in PwP REPCHAR
Special chars in PwP   SPECLIST

```

Figure 102. GSO system settings (Screen 2)

```

GSO system settings
Command ==>
Line 51 of 75
Scroll==> CSR

MLS related settings (MLSOPTS)
MLS active MLACTIVE No
MLS mode of operation MODE
MLS writedown allowed MLWRITE
Unix reqs seclabels MLFSOBJ
IPCobj reqs seclabel MLIPCOBJ
Seclabels SYS-depdt MLSECBYS
DSNs/rsrscs req label MLSLBLRQ No

Access rule settings (RULEOPTS)
Allow use of $NOSORT Yes
Allow %C and %R CHANGE Yes
Only Security can store rules No
SecVol rules: VOLUME.@volser No
Rules can be > 4K RULELONG Yes
Try small rule compiler first Yes
LIDs that can DECOMP any rule SeAu

UNIX options (UNIXOPTS)
SAF HFS Security enable No
Default user OMVSUSER
Default group OMVSDGRP

Erase settings (AUTOERAS)
Erase VSAM VSAM No
Erase everything ERASEALL No
EOS SecLevel-based SECLVL No
Erase volumes

Erase nonVSAM NON-VSAM No
EOS decided by: PROCESS
Threshold SecLvl SECLVL

Volumes protected by dataset (RESVOLS) Volumes protected by volser (SECVOLS)
-

Logged programs (LOGPGM)
AMASPPZAP IMASPPZAP

Protected programs (PPGM)
DRWD- FDR*** ICKDSF- IEHD-

Programs with tape-BLP (BLPPGM)

Maintenance programs and LIDs (MAINT)
CRMBMR1 ADDRSSU SYS1.LINKLIB
CRMBMR1 TESTJE TEST.LIBR

PDSes with member-level protection (PDS)
CRMBMR1.ISPF.CNTL PDS
TEST.LIBRARY COMMON PDJ
TEST.LIBRARY WORKPK PDJ
TEST.PDSALLOW VOL001 PDSALLOW
TEST.PDSALLOW PDSALLOW

Linklist libraries (LINKLST)
SYS1.LINKLIB SYS290
***** BOTTOM OF DATA *****

```

Figure 103. GSO system settings (Screen 3)

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.

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 13. Recommended password settings

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

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:

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

Figure 104. Global System Options – gso records

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.

```
GSO system settings                                     Line 1 of 69
Command ==> _____ Scroll==> CSR_
                                     9 May 2005 22:10

  Complex  System  Collect timestamp
  DEMO     DEMO    4 Dec 2001 22:10

Maintenance programs and LIDs (MAINT)
SMCLEAN  ADRDSSU  SYS1.LINKLIB
SMCLEAN  TESTJE   TEST.LIBR
```

Figure 105. MAINT records

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

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.

```
GSO system settings                                     Line 1 of 69
Command ==> _____ Scroll==> CSR_
                                     9 May 2005 22:10

  Complex  System  Collect timestamp
  DEMO     DEMO    4 May 2005 22:10

PDSES with member-level protection (PDS)

SMCLEAN.ISPF.CNTL                                PDS
TEST.LIBRARY                                       COMMON PDJ
TEST.LIBRARY                                       WORKPK PDJ
TEST.PDSALLOW                                     VOL001 PDSALLOW
TEST.PDSALLOW
```

Figure 106. Member-level protection through PDS record

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.

```
Menu  Options  Info  Commands  Setup
-----
                                zSecure Audit for ACF2 - Audit - Status
Command ==> _____

Enter / to select report categories
- MVS tables                MVS oriented tables (reads first part of CKFREEZE)
- MVS extended              MVS oriented tables (reads whole CKFREEZE)
- ACF2 control               ACF2 oriented tables
/ ACF2 user                  User oriented ACF2 tables and reports
- ACF2 resource              Resource oriented ACF2 tables and reports


Select options for reports:
- Select specific reports from selected categories
/ Include audit concern overview in overall prio order
- Only show reports that may contain audit concerns
- Minimum audit priority for audit concerns (1-99)
- Show differences
- Print format               - Concise (short) report
- Background run

Audit policy
/ zSecure
- C1
- C2
- B1
```

Figure 107. ACF2 user audit selection

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.

```

IBM Security zSecure Audit for ACF2 Display Selection 210 s elapsed, 155.2 s C
Command ==> Scroll==> CSR

Name      Summary Records Title
S OVERVIEW      227      0 Audit concern overview by priority (higher prioritie
- LIDAUDIT      2      227 ACF2 logonid audit concerns
- TRUS2USR      1    18457 Trusted logonids (may bypass security)
- UNSCPRIV      2      50 Users with unscoped SECURITY, ACCOUNT, LEADER, CONSU
- SCPDPRIV      2      30 Users with scoped SECURITY, ACCOUNT, LEADER, CONSULT
- SHRDPREF      2     825 Prefixes shared between logonids
- PWINNON2      2     148 Users without password interval
- PWINLNG2      2      55 Users with password interval > 60 days
- PWEXPIR2      2     153 Users with expired passwords
- PWAGSUM2      2     939 ACF2 password age overview
- PWAGALL2      2     219 User Password Age: All non-STC, non-Restrict users
- PWAGNEV2      2      2 User Password Age: No password set, no STC/Restrict
- PWAG5YR2      0      0 User Password Age: 5 years or more
- PWAG4YR2      2      6 User Password Age: 4..5 years
- PWAG3YR2      2     54 User Password Age: 3..4 years
- PWAG2YR2      2     28 User Password Age: 2..3 years
- PWAG1YR2      2     58 User Password Age: 1..2 years
- PWAG0YR2      2     71 User Password Age: Less than a year
- PWAG6MN2      2     24 User Password Age: 6..12 months
- PWAG5MN2      2      3 User Password Age: 5..6 months
- PWAG4MN2      2     15 User Password Age: 4..5 months
- PWAG3MN2      2      4 User Password Age: 3..4 months
- PWAG2MN2      2      7 User Password Age: 2..3 months
- PWAG1MN2      2      4 User Password Age: 1..2 months
- PWAG2WK2      2      7 User Password Age: 2..4 weeks
- PWAGREC2      2      7 User Password Age: Less than two weeks
- PWTRIES2      2     29 Users with logon failures
- PWMIN        2    224 Users without MinDays limit
- LGNEVER2      2    241 Users that have never been used
- LGAGSUM2      2     939 ACF2 last logon overview
- LGAGALL2      2     939 User Last Logon: All users
- LGAG5YR2      0      0 User Last Logon: 5 years or more ago
- LGAG4YR2      0      0 User Last Logon: 4..5 years ago
- LGAG3YR2      2    558 User Last Logon: 3..4 years ago
- LGAG2YR2      2     19 User Last Logon: 2..3 years ago
- LGAG1YR2      2     17 User Last Logon: 1..2 years ago
- LGAG0YR2      2    104 User Last Logon: Less than a year ago
- LGAG6MN2      2     35 User Last Logon: 6..12 months ago
- LGAG5MN2      1      1 User Last Logon: 5..6 months ago
- LGAG4MN2      2      2 User Last Logon: 4..5 months ago
- LGAG3MN2      2      3 User Last Logon: 3..4 months ago
- LGAG2MN2      1      2 User Last Logon: 2..3 months ago
- LGAG1MN2      1      2 User Last Logon: 1..2 months ago
- LGAG2WK2      2      7 User Last Logon: 2..4 weeks ago
- LGAGREC2      2     52 User Last Logon: Less than two weeks ago
***** BOTTOM OF DATA *****

```

Figure 108. User display selection

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.”

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.

Priority	JOBFROM	PREFIX	RESTRICT
Audit concern overview by priority (higher priorities only)			
Command ==>			Line 1 of 227
			Scroll==> CSR
9 May 2005 22:10			
Pri	Complex	Syst Area Key	Audit concern
35	DEMO	LID PRODLID	Probable hacking attempt
35	DEMO	LID SYSTLID	Probable hacking attempt
30	DEMO	LID JOHNTTEST	JOBFROM without MUSASS, Scoped SECURITY a
30	DEMO	LID RHORTON	Masked PREFIX, SECURITY and NORULEVLD, SE
30	DEMO	LID JLENNO	RESTRICT without any restraints
30	DEMO	LID CBELLE	Masked PREFIX, Password change not enforc
30	DEMO	LID PRODPAYR	RESTRICT without any restraints
30	DEMO	LID DHOGAN	RESTRICT without any restraints, PASSWORD
30	DEMO	LID BSMITH	JOBFROM without MUSASS, Scoped SECURITY a
30	DEMO	LID JRAYMOND	Masked PREFIX, SECURITY and NORULEVLD, SE
30	DEMO	LID DGUTHRIE	RESTRICT without any restraints
30	DEMO	LID SYSPGM1	Masked PREFIX, Password change not enforc
30	DEMO	LID TKERRY	RESTRICT without any restraints
30	DEMO	LID GSESSION	RESTRICT without any restraints, PASSWORD
22	DEMO	LID SZICHI	JOBFROM without MUSASS
22	DEMO	LID MMENDOZA	JOBFROM without MUSASS
20	DEMO	LID NLINLEY	Password change not enforced, Can change
20	DEMO	LID ELANSKI	Password change not enforced, Can change
20	DEMO	LID DBUSSEY	SECURITY and NORULEVLD, SECURITY and NORS
20	DEMO	LID GMCLEAN	Scoped SECURITY and NORULEVLD, Scoped SEC

Figure 109. User audit concerns by priority

Each line in the *Audit concern overview by priority* panel describes a single concern identified. The line contains the audit priority, complex and system name, problem area, key, that is, Logon ID, and the audit concern. Table 14 lists the audit priority values and the associated meaning.

Table 14. Audit Priority values

Value	Meaning
0 - 10	<i>informational</i>
10 - 20	<i>desired</i>
20 - 40	<i>review required</i>
40 and up	<i>serious exposure</i>

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.

IBM Security zSecure Audit for ACF2 Display Selection				55.2 s C
Command ===> _____				Scroll===> CSR_
Name	Summary	Records	Title	
_ OVERVIEW		227	0 Audit concern overview by priority (higher prioritie	
_ SCPDPRIV	2	30	Users with scoped SECURITY, ACCOUNT, LEADER, CONSULT	
_ SHRDPREF	2	825	Prefixes shared between logonids	
S PWINNON2	2	74	Users without password interval	
_ PWINLNG2	2	55	Users with password interval > 60 days	

Figure 110. Select a password audit report

- 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.

```

Users without password interval                                     Line 1 of 2
Command ==> _____ Scroll==> CSR_
                                     9 May 2005 02:24

Complex Timestamp      Users
DEMO      4May005 02:24    74
Inactivated Users
S_ No      57
_ Yes      17
***** BOTTOM OF DATA *****

```

Figure 111. Password interval summary

Listing logon IDs without a password interval Procedure

- 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*.
- Type S in the selection field for the **No** entry.
- Press Enter to view the list of active logon IDs without a password interval as shown in Figure 112.

```

Users without password interval                                     Line 1 of 57
Command ==> _____ Scroll==> CSR_
                                     9 May 2005 02:24

LID      Name      UID      MxD PW change Inv Vio
_ ASMITH SMITH, ALBERT NCADM ASMITH 28Mar2005 0 0
S_ BSMITH1 SMITH, BERT NCTST BSMITH1 28Mar2005 0 0
_ BSMITH2 SMITH, BERTIE NCTST BSMITH2 28Mar2005 0 0
_ JBERT BERT, JOHN NCTEC JBERT 28Mar2005 0 0
_ JBERTRAM BERTRAM, JOHN NLANL JBERTRAM 28Mar2005 0 0

```

Figure 112. Users without password interval

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.

```

Users without password interval
Command ==> _____
Line 1 of 57
Scroll==> CSR_
9 May 2005 23:37

Identification
ACF2 logonid BSMITH1
User name SMITH, BERT DEMO

Full UID
NCTST BSMITH1 Prefix BSMITH1

Scope ScpList DSNscope LIDscope UIDscope
Scope record names

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
Logonid for started tasks

Scopable privileges
User has SECURITY privilege
User has ACCOUNT privilege
User has LEADER privilege
User has CONSULT privilege
User has AUDIT privilege

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

Multi-user privileges
Logonid for MUSASS
ACF2 updates under users auth
Can use //*JOBFROM

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 PPGMs
Dynamic logon privilege
Disable violation counter

Limitations
Resource rules validated
Data set rules validated
Can't store rule sets
Batch only via this program
Jobs w/LID through APF only
Name of SHIFT record
Source group for access
This LID cannot be inherited
Barred from Unix Services
Restricted UNIX file access

Audit trail
Write all logons to SMF
Trace all data access
Trace all TSO commands
Warn security of all logons

Password anomalies
Last invalid pswd attempt
Input source last invalid pwd
# pswd violations on PSWD-DAT 0
Pswd violations since logon 0
# Kerberos key violations 0
Password forced to expire Yes
Case-sensitive password,
RESTRICT - no password needed

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

Audit concern
Password change not enforced, Can change password back to old value
***** BOTTOM OF DATA *****

```

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

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 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 CH
```

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

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.

```
Menu Options Info Commands Setup
-----
IBM Security zSecure Audit for ACF2 - Audit - Status
Command ==>

Enter / to select report categories
- MVS tables          MVS oriented tables (reads first part of CKFREEZE)
- MVS extended        MVS oriented tables (reads whole CKFREEZE)
- ACF2 control         ACF2 oriented tables
- ACF2 user            User oriented ACF2 tables and reports
/ ACF2 resource        Resource oriented ACF2 tables and reports

Select options for reports:
- Select specific reports from selected categories
/ Include audit concern overview, higher priorities only
- Minimum audit priority for audit concerns priorities (1-99)
- Print format          Concise (short) report
- Run in background

Audit policy
/ zSecure
C1
C2
B2
```

Figure 114. Select ACF2 resource

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.


```

Security zSecure Audit for ACF2 Display Selection                      elapsed, 94.6 s CP
Command ==> _____ Scroll==> CSR_

Name      Summary Records Title
- OVERVIEW      3474      0 Audit concern overview by priority (higher prioritie
- SEN2APF        1      103 APF data sets with full ACL
- SEN2LINK       1       39 Linklist data sets with full ACL
- SEN2LPA        1       14 LPA list data sets with full ACL
- SEN2ALL        1      192 All sensitive data sets by priority and type with fu
- SEN2TRUS       1     18457 Sensitive data trustees with full audit concerns / r
- SEN2RULE       1     18349 Rules protecting sensitive data with full audit conc
- TSOAUTH2       1        3 TSO authorized commands
- LPAPROT2       1      285 LPA module protection overview
- APFPROT2       1      285 APF module protection overview
- UNIXAPF2       0        0 UNIX files with APF authorization
- UNIXCTL2       0        0 UNIX files that are program controlled (daemons etc.
- UNIXSUI2       0        0 UNIX files with SETUID authorization
- UNIXSGI2       0        0 UNIX files with SETGID authorization
- STCPROT2       0        0 Started task overview
- GLB2UNIX       0        0 UNIX files vulnerable to trojan horse & back door at
***** BOTTOM OF DATA *****

```

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 SEN2*)
- 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

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

Started Task Protection report

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

Sensitive Data Trustees report

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” on page 94.

To see more detail, complete the following steps: “Viewing more detail” on page 94.

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.

IBM Security zSecure Audit for ACF2 Display Selection			elapsed, 94.6 s CP
Command ==> _____			Scroll==> CSR_
Name	Summary	Records	Title
OVERVIEW	3474	0	Audit concern overview by priority (higher prioritie
- SEN2APF	1	103	APF data sets with full ACL
- SEN2LINK	1	39	Linklist data sets with full ACL
- SEN2LPA	1	14	LPA list data sets with full ACL
- SEN2ALL	1	192	All sensitive data sets by priority and type with fu
/ SEN2TRUS	1	18457	Sensitive data trustees with full audit concerns / r
- SEN2RULE	1	18349	Rules protecting sensitive data with full audit conc
- TSOAUTH2	1	3	TSO authorized commands
- LPAPROT2	1	285	LPA module protection overview
- APFPROT2	1	285	APF module protection overview
- UNIXAPF2	0	0	UNIX files with APF authorization
- UNIXCTL2	0	0	UNIX files that are program controlled (daemons etc.
- UNIXSUI2	0	0	UNIX files with SETUID authorization
- UNIXSGI2	0	0	UNIX files with SETGID authorization
- STCPROT2	0	0	Started task overview
- GLB2UNIX	0	0	UNIX files vulnerable to trojan horse & back door at
***** BOTTOM OF DATA *****			

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 on page 95. Then, press Enter.

```

Sensitive data trustees with full audit concerns / reasons          Line 1 of 26
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
   9 ACF2 LID db DATASET 1 539
   9 APF library DATASET 33 823
   9 APF Linklst DATASET 24 1448
   9 APF LPAlst DATASET 3 195
   9 MSTR prmlib DATASET 3 195
   9 MSTR STClib DATASET 3 195
   8 ACF2 Infost DATASET 1 65
   8 ACF2 Rules DATASET 1 65
   7 JES2 Ckpt DATASET 1 938
   6 ACF2 MAINT DATASET 1 65
   4 ACF2 AltLid DATASET 5 2695
   4 ACF2 BkLid DATASET 1 539
   4 System Dump DATASET 1 474
   4 SMF dataset DATASET 1 40
   3 Active IODF DATASET 1 65
   2 ACF2 AltBkI DATASET 5 2695
   2 ACF2 AltBkL DATASET 5 2695
   2 ACF2 AltBkR DATASET 5 2695
   2 ACF2 BkInfo DATASET 1 539
   2 ACF2 BkRule DATASET 1 539
   2 SMS ACDS DATASET 1 65
   2 SMS COMMDS DATASET 1 65
   2 SMS SCDS DATASET 1 65
   1 ACF2 AltInf DATASET 5 325
   1 ACF2 AltRu1 DATASET 5 325
***** 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.

```

Sensitive data trustees with full audit concerns / reasons          Line 1 of 108
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
_ 10 PRODLID PROD BATCH LID DEMO Can submit for all others
_ 10 CRMASC2 SPECIAL JOB LID DEMO Can submit for all others
_ 10 SMCLEAN MCLEAN, SARAH DEMO Unscoped authority to change/defi
_ 10 PCRAM1 BERT SPECIAL USER DEMO Unscoped authority to change/defi
_ 10 LVOIGHT VOIGHT, LARRY DEMO Unscoped authority to change/defi
_ 10 RHORTON HORTON, RAY DEMO Unscoped authority to change/defi
_ 8 PRDSTCID PROD STC LID DEMO All data set access allowed
_ 4 PRODHFS PROD HFS LID DEMO All data set access allowed
_ 4 TAPEMGR TAPE MANAGER DEMO Can rea/write any tape includin
_ 1 PRODCICS CICS DEMO Can execute MAINT protected utili
_ 1 SYSPROG SYS PROG LID DEMO Can execute MAINT protected utili
_ 1 SYSPROG SYS PROG LID DEMO Can execute MAINT protected utili

```

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.

```

Sensitive data trustees with full audit concerns / reasons          Line 1 of 23
Command ==> _____ Scroll==> CSR_
                                     9 May 2005 22:10

Sensitive object
Complex that may be attacked DEMO
System that may be attacked DEMO
Type of sensitive resource Privilege
Resource class System
Resource name DEMO
- Volume serial for resource
Access level that is exposure

Security rule covering object
Complex used for the attack DEMO
ACF2 rule $KEY
ACF2 rule entry

User that may compromise security
- Trusted logonid SYSPROG MAINT
STC setting STC
UID string NLOPS SYSPROG
Privilege on user's complex MAINT

```

Figure 120. Shows the detail Logon ID attributes for the *SYSPROG* Logon ID

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.

Sensitive data trustees with full audit concerns / reasons					Line 1 of 26
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
—	9	ACF2 LID db	DATASET	1	539
—	9	APF library	DATASET	33	823
—	9	APF Linklst	DATASET	24	1448
—	9	APF LPAlist	DATASET	3	195
—	9	MSTR prmlib	DATASET	3	195
—	9	MSTR STClib	DATASET	3	195
—	8	ACF2 Infost	DATASET	1	65
S_	8	ACF2 Rules	DATASET	1	65
—	7	JES2 Ckpt	DATASET	1	938
—	6	ACF2 MAINT	DATASET	1	65
—	4	ACF2 AltLid	DATASET	5	2695
—	4	ACF2 BkLid	DATASET	1	539
—	4	System Dump	DATASET	1	474
—	4	SMF dataset	DATASET	1	40
—	3	Active IODF	DATASET	1	65
—	2	ACF2 AltBkI	DATASET	5	2695
—	2	ACF2 AltBkL	DATASET	5	2695

Figure 121. Detail Logon ID attributes for sensitive privileges

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.

Sensitive data trustees with full audit concerns / reasons					Line 1 of 65
Command ==>					Scroll==> CSR_
					9 May 2005 22:10
Pri	Complex	System	Trust relations		
10	DEMO	DEMO	18457		
Pri	Sensitivity	Class	Resources	Trust relations	
—	8	ACF2 Rules	DATASET	1	65
Pri	Resource			VolSer	Trust relations
—	8	SYS1.ACF2V64.PRIM.RULES		HFSPRD	65
Pri	Logonid	Name	From	Audit concern	
—	8	ACFBLID	PROD	Data set rules may be changed dir	
—	8	CICSPRD	PROD	Data set rules may be changed dir	
S_	8	SMITH7	BERT SPECIAL USER	PROD	Data set rules may be changed dir
—	8	RHORTON	HORTON, RAY	PROD	Data set rules may be changed dir

Figure 122. Show reasons that logon IDs have special access to sensitive data sets

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

Example

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

```
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
8 ACF2 Rules DATASET 1 65
Pri Resource VolSer Trust relations
8 SYS1.ACF2V64.PRIM.RULES HFSPRD 65
Pri Logonid Name From Audit concern
8 SMITH7 BERT SPECIAL USER PROD Data set rules may be changed dir
Pri Privilege Access $KEY Rule Entry
8 Rule UPDATE SYS1 - UID(SYSPROG) READ(A) WRITE(A) ALLOC(A) EXEC
***** BOTTOM OF DATA *****
```

Figure 123. View assigned privileges for logon IDs with access to sensitive data sets

Chapter 7. Rule-based compliance evaluation

Use these guidelines to understand how the zSecure Audit Compliance Testing Framework and rule-based compliance evaluation are implemented.

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 SYS1
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.
- CKTG* members are Top Secret STIG rules
- CKAO* members are GSD331 rules.

Reporting

Use this task to generate auditing compliance reports on STIG, GSD, PCI-DSS and other standards.

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

zSecure Suite - Audit - Compliance				
Command ==> _____				
Action				
_ 1. Run evaluation below 2. Select rules for ESM 3. Customization				
Compliance evaluation (action 1)				
/ STIG (subset)				
_ PCI-DSS (subset)				
_ Other standard member				
_ Test a single rule (set) member				
_____ ACF2 (RACF/ACF2/NONE)				
Compliance result selection				
_ Compliant _ Non-compliant _ Undecided				
Output/run options				
Print format _ Send as e-mail				
_ Background run _ Include test details _ Narrow print				

Figure 125. Audit Compliance menu

2. Select the action you want to perform in the **Action** section:

Select rules for ESM

Define your own subset of rules from the shipped compliance evaluations. See the section to define your own subset of rules from the shipped compliance evaluations in the *IBM Security zSecure Audit for ACF2 User Reference Manual*.

Run evaluation below

Run the compliance evaluation or evaluations selected on the top half of the panel. This is the default.

Customization

Edit/view the customization and population members. This is a concatenated display of the user CKACUST library and the site CKACUST library.

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

The **Compliance evaluation** selection refer to predefined subsets for these standards:

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

PCI-DSS

Payment Card Industry Data Security Standard.

The **Other standard member** selection can be used to run a compliance check against your own system-defined standard or an older version of STIG, GSD, or PCI-DSS. Specify the member name that contains standard statement in the field that is provided.

The **Test a single rule** selection is provided to assist in testing when developing a site standard. For a list of the controls available in zSecure, see IBM Security zSecure Audit controls. 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

Optionally, you can use the **Compliance result selection** section to restrict which results to include in the compliance report. By default, if no filter is selected, the reports contain compliant, noncompliant, and undecided results.

The compliance result selections determine what results are shown.

When you select **Print format**, two reports are produced. The first report shows the compliance rule set summary. The second report shows the compliance statistics for tested objects.

When you select **Print format** and **Include test details**, three reports are produced:

- a. The first report shows the compliance rule set summary.
- b. The second report shows the compliance statistics for tested objects.
- c. The third report shows each individual rule set on a separate page.

The objects affected by the rule set are ordered by their noncompliance, undecided, and compliance attributes, detailing the individual test results for the tests in the rules in the rule set.

When you select both **Print format** and **Narrow print**, the width of the page is limited to 79 characters, independently of the actual print file record length.

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 noncompliant objects per rule set
 - c. Object level
 - d. Individual test result overview level
 - e. Detail level
4. Select any of the standards in **Compliance evaluation** to evaluate against, for example, **STIG (subset)** or a subset of rules, and do not tag **Print format**. The Figure 126 on page 102 is displayed with three report options:

zSecure Suite Display Selection

3 s elapsed, 1.8 s CPU

Command ==>

Scroll==> PAGE

Name	Summary	Records	Title
- STDRULES	1	129	Standard rule set compliance summary
- STDTYPES	1	20	Standard object type compliance summary
- STDTESTS	1	17324	Standard compliance test
***** Bottom of Data *****			

Figure 126. zSecure Suite Display Selection panel

- “STDRULES: Standard rule set compliance summary”: Shows the compliance rule set summary. This management summary can help to determine rule set compliance status or improvement.
- “STDYPES: Standard object type compliance summary” on page 104: Shows the compliance statistics for tested objects. This management summary can help to determine object types compliance status or improvement.
- “STDTESTS: Standard compliance test results” on page 105: Shows the object test results sorted by rule set name. Noncompliant test results are sorted above compliant test results. These detailed compliance test results can help to determine what actions to take for which resources in order to improve compliance.

STDRULES: Standard rule set compliance summary

The management summary of rule set compliance test results can help determine the high level status or progress of rule set compliance.

When you select STDRULES on the zSecure Suite Display Selection panel (Figure 126), the Figure 127 is displayed. It does not contain the actual test result details but shows compliance results at a higher level instead. The STDRULES summary includes all supported rule sets, including those for which no objects are found that must be tested. If there are no objects found that must be tested, the rule set is reported to be compliant. There is one line for each rule set that zSecure Audit supports for the pertinent standard.

Standard rule set compliance summary											Line 1 of 129
Command ==>											Scroll==> PAGE
											2 Sep 2015 23:45
Complex	Ver	Pr	Standards								
NMPIPL87		30	1								
Standard		Pr	Rule sets								
RACF_STIG		30	129								
Rule set		Pr	Cm%	NS	TestPnt	Comply	NonCom	Unkn	Caption		
/ AAMV0030		20	0		1	0	1	0	LNKAUTH=APFTAB		
— AAMV0040		10	97		672	654	18	0	APF libraries exist		
— AAMV0050			100		14	14	0	0	APF libraries unique		
— AAMV0160		20	81		143	117	26	0	PPT programs exist		
— AAMV0380			100		288	288	0	0	SMF record (sub)types		
— ACP00010		30	33		12	4	8	0	PARMLIB protected		
— ACP00020		20	36		11	4	7	0	Update on SYS1.LINKLIB		
— ACP00030		30	36		11	4	7	0	Update on SYS1.SVCLIB		
— ACP00040		30	36		11	4	7	0	Update on SYS1.IMAGELIB		
— ACP00050		30	36		11	4	7	0	Update on SYS1.LPALIB		
— ACP00060		30	79		2827	2261	566	0	Update+alter on APF list		
— ACP00070		30	22		87	20	67	0	Update+alter on LPA list		
— ACP00080		30	36		11	4	7	0	Update+alter on Nucleus		
— ACP00110		20	36		193	70	123	0	Update+alter on Linklist		
— ACP00120		30	50		8	4	4	0	RACF db protected		

Figure 127. STDRULES: Standard rule set compliance summary panel

For each rule set, this summary includes the following columns:

Rule set

The rule set number from the documented standard.

Pr Noncompliant priority: 10 is low, 20 is medium, 30 is high. For each rule set that is reported as compliant, this column is blank.

Cm%

Compliance percentage. You can monitor this column to determine your progress on becoming compliant for the pertinent rule set.

NS NS is a concatenated column. The N stands for a rule set that contains a test that is evaluated as Not Applicable. An S is shown when a rule set is suppressed.

TestPnt

Number of tested objects within this rule set.

Comply

Number of compliant objects.

NonCom

Number of noncompliant objects.

Unkn

Number of tests with an undecided/unknown outcome.

Caption

Short description of what this rule set tests.

You can use the S or / line command to access the rule set details. This panel includes the full rule set description as well as the standard name and version against which you evaluated your system.

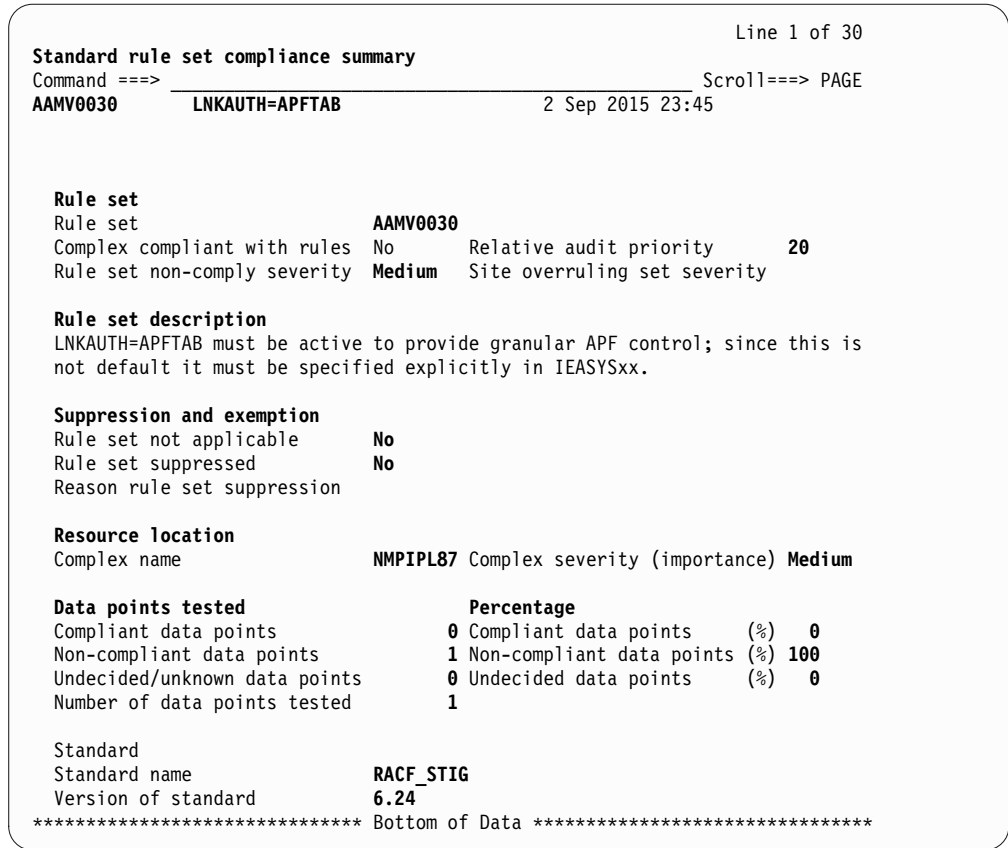


Figure 128. STDRULES: rule set details

A severity is assigned to each rule set or rule; see the **Rule set non-comply severity** field. You can overrule this severity with a SITE_SEVERITY statement that assigns a different severity value as it applies to your organization. Possible values are high, medium, and low.

STDYPES: Standard object type compliance summary

The management summary of object type compliance test results can help you to determine the status or progress of object type compliance.

When you select STDRULES on the zSecure Suite Display Selection panel (Figure 126 on page 102), the Standard object type compliance summary is displayed. It shows statistics about the newlist types that are used for the STIG compliance evaluation. For an explanation of the columns, see Figure 127 on page 102. In addition, the **Exempt** column shows the number of exempted objects that are found for which an exception is coded.

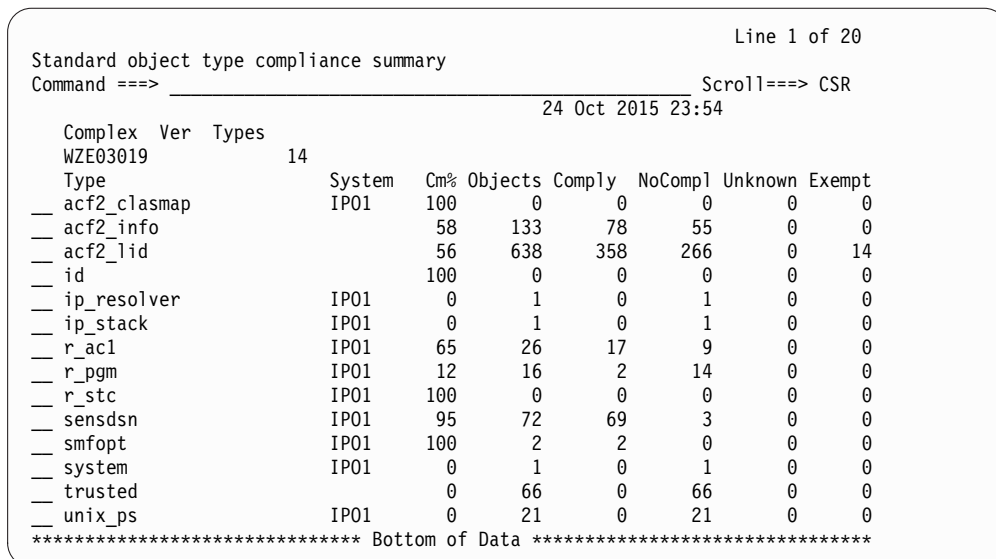


Figure 129. STDYPES: Standard object type compliance summary

You can use the S or / line command to see the STIG compliance evaluation for a specific newlist type. Figure 130 shows in which rule sets the pertinent newlist type is used and whether this rule set is compliant, noncompliant, undecided/unknown, or exempt.

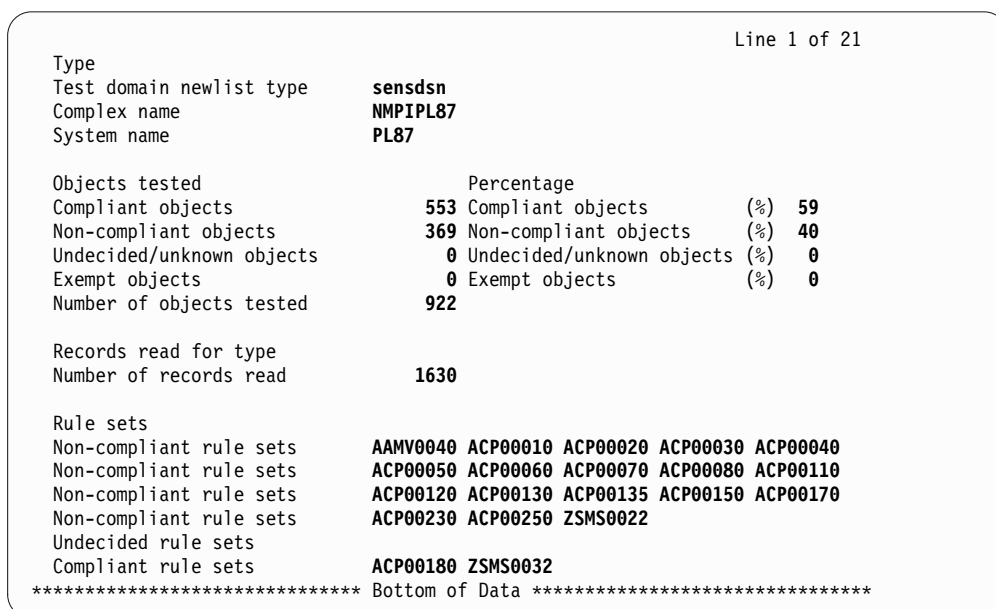


Figure 130. STDYPES: STIG compliance evaluation for newlist

STDTESTS: Standard compliance test results

The detailed compliance test results can help to determine what actions to take for which resources in order to improve compliance.

When you select STDTESTS on the zSecure Suite Display Selection panel (Figure 126 on page 102), Figure 131 on page 106 is displayed. Although the STRULES summary includes all supported rules sets, the STDTESTS summary contains only the rule sets that have test results. Rules sets without test results are ignored and not included in the STDTESTS report.

The screen and print output is sensitive to the screen width and line length. Narrow output shows rule-set captions, while wider output shows rule-set descriptions (see the **Narrow print** option in the AUR compliance menu in Figure 125 on page 100). Figure 131 shows an example of output for the rule set level on a screen with width 80.

For an explanation of the columns, see “STDRULES: Standard rule set compliance summary” on page 102.

Standard compliance test results							Line 1 of 58
Command ==>							Scroll==> CSR
13 Jun 2014 03:01							
Complex	Ver	Pr	Standards	NonComp	Unknown	Exm	Sup
ACF2AD2R	6.1	20	1	1	1	1	
Standard		Pr	Rule sets	NonComp	Unknown	Exm	Sup
ACF2_STIG		20	58	33	7	1	6.15
Rule set		Pr	Objects	NonComp	Unknown	Exm	Sup
AAMV0030		20	1	1			LNKAUTH=APFTAB
AAMV0040		10	269	4			APF libraries exist
AAMV0050			13				APF libraries unique
AAMV0160		20	27	4			PPT programs exist
AAMV0380			1				SMF record (sub)types
ACF0250			3		3		GSO APPLDEF needs doc
ACF0260		20	2	2			GSO AUTHEXIT OID exit
ACF0270			1				GSO AUTOERAS to ACF2
ACF0280		20	9	9			GSO BACKUP time set
ACF0290		20	4	4			GSO BLPPGM empty
ACF0300		20	2	1			GSO CLASMAP defined
ACF0310		20	8	8			GSO EXITS values set
ACF0330			19				GSO LINKLST defined
ACF0350		20	5	5			GSO MAINT defined

Figure 131. STDTESTS - Standard compliance test panel

Compliance by complex shows the number of standards and the results that are processed in this compliance evaluation run. This example shows that, for complex ACF2AD2R, compliance is checked against ACF2_STIG and that it is not fully compliant.

If only one standard is evaluated, the second summary level result is shown. If the complex is evaluated against more than one standard, a separate summary report is generated for each standard against which the system is evaluated.

The summary by standard shows the highest noncompliance priority, the total number of reported rule sets, and the number of noncompliant, unknown/undecided, and exempted rules within that standard.

The summary by rule set shows the number of affected objects by test or tests within a rule set, and the specific results for the pertinent rule set.

You can use the S or / line command to zoom in to the details of the report.

Standard compliance test results										Line 1 of 2	
Command ==>										Scroll==> PAGE	
10 Sep 2015 23:45											
Complex	Ver	Pr	Standards	NonComp	Unknown	Exm	Sup				
NMPIPL87	30		1	1	1	1					
Standard	Pr	Rule sets	NonComp	Unknown	Exm	Sup	Version				
RACF_STIG	30	107	69	3	4		6.20				
Rule set	Pr	Objects	NonComp	Unknown	Exm	Sup	Caption				
RACF0440	20	1	1				SETROPTS PASSW INT(60)				
Non	Unk	Exm	Class	System	Type	VolSer	Resource				
Non			System	PL87		PL87					
Cmp	Non	Unk	Ex	Test name	Member	Test description					
/	Non			b.1b.PWDInterval60	CKAGR440	PASSWORD(INTERVAL) must be					
—	Cmp			b.1a.PWDInterval0	CKAGR440	PASSWORD(INTERVAL) should					
***** Bottom of Data *****											

Figure 132. STDTESTS - Standard compliance test results panel

The example in Figure 132 shows that your system is not compliant to one of the two tests for rule set RACF0440. You can use the S or / line command to read the full details for this test.

```

Standard compliance test results
Command ==> _____ Line 1 of 59
                                Scroll==> PAGE
                                10 Sep 2015 23:45

Test description
PASSWORD(INTERVAL) must be set to less than or equal to 60.

Class      Resource
System     PL87

Test result
Test value is compliant      No      Test is true      No
Non-compliant audit finding  Yes      Relative audit priority  20
Lookup against
Actual value of test field   90

Test definition
Test name      b.1b.PWDInterval60
Test lookup base field name
Test field name      PWDINTERVAL
Relational operator  <=
Compliance comparison value  60

Suppression and exemption
Rule set not applicable
Exempt from rule      No
Rule suppressed
Reason for rule suppression

Domain
Domain name      System_options
Domain description

Rule
Rule set      RACF0440
Rule name      RACF0440
Rule non-compliance severity  Medium      Site overruling rule severity

Rule description
The PASSWORD(INTERVAL) SETROPTS value must be set to 60 days.

Rule set description
The PASSWORD(INTERVAL) SETROPTS value must be set to 60 days.

Resource location
Complex name      NMPIPL87      Complex severity (importance)  Medium
System name      PL87      Profile or data set type
Test domain newlist type  system

Standard
Standard name      RACF_STIG
Version of standard  6.24

Test origin
Test defined in CARLa member  CKAGR440
***** Bottom of Data *****

```

Figure 133. STDTESTS - Standard compliance test results for test b.1b.PWDInterval60 for RACF0440

In the example in Figure 133, the **Test description** shows that the password interval must be less or equal to 60 days. **Test results** shows that the actual value

found is 90. The **Test definition** shows the details of the pertinent test. It shows that the test must be reported to be noncompliant if the password interval is not shorter or equal to (\leq) 60.

Suppression and exemption shows that this rule is not exempt. It is possible to code an exempt definition in the CARLa code for this rule so that the test shows that this rule is exempted from the pertinent rule.

If a rule is part of a rule set, the pertinent rule description generally differs from the rule set description.

Test origin shows in which SCKRCARL member the CARLa code for this rule set is stored. You can review or customize this rule set for your system.

Chapter 8. Resource-based reports for ACF2 resources

The Resource reports option (**RE**) is available from the Main menu:

Menu	Options	Info	Commands	Setup

zSecure Audit for ACF2 - Main menu				
Option ==> -----				
SE	Setup	Options and input data sets		
AA	ACF2	ACF2 Administration		
AU	Audit	Audit security and system resources		
RE	Resource	Resource reports		
C	CICS	CICS region and resource reports		
D	DB2	DB2 region and resource reports		
I	IP stack	TCP/IP stack reports		
M	IMS	IMS control region and resource reports		
N	VTAM	VTAM reports		
Q	MQ	MQ region and resource reports		
U	Unix	Unix filesystem reports		
EV	Events	Event reporting from SMF and other log		
CO	Commands	Run commands from library		
IN	Information	Information and documentation		
LO	Local	Locally defined options		
X	Exit	Exit this panel		
Input complex: DAILY				
Product/Release				
5655-N17 IBM Security zSecure Audit for ACF2 2.2.0				

Figure 134. zSecure Audit for ACF2 Main menu

It provides access to display and reporting options for the following RACF resources:

- “CICS region and resource reports”
- “DB2 region and resource reports” on page 112
- “IP stack reports” on page 115
- “IMS region and resource reports” on page 116
- “VTAM application reports” on page 117
- “MQ region and resource reports” on page 118
- “UNIX file system reports” on page 121

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 data used for this CICS report 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 135 on page 112 is displayed.

Menu	Options	Info	Commands	Setup	Startpanel
zSecure Suite - Resource - CICS					
Option ===>					
R	Regions	CICS region reports			
T	Transactions	CICS CICS transactions selection and reports			
P	Programs	CICS programs selection and reports			

Figure 135. CICS Resource panel

In the CICS Resource panel in Figure 135, select the option of your choice. The corresponding selection panel is displayed. For example, the CICS Regions selection panel in Figure 136.

Menu	Options	Info	Commands	Setup
zSecure Suite - CICS - Regions				
Command ===>				
Show CICS regions that fit all of the following criteria:				
Jobname	_____	(jobname or filter)	
VTAM applid	_____	(applid or filter)	
SYSIDNT	_____	(identifier or filter)	
Complex	_____	(complex or filter)	
System	_____	(system or filter)	
Advanced selection criteria				
_ Region security settings _ Region attributes _ Classes				
Output/run options				
_ Show differences				
_ Print format		Customize title	Send as e-mail	
_ Background run		Full page form		

Figure 136. CICS Regions selection panel

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*.

DB2 region and resource reports

The DB2 Resource menu shown in Figure 137 on page 113 is displayed.

Menu	Options	Info	Commands	Setup	Startpanel

zSecure Suite - Resource - DB2					
Option ==> _____					
R	Regions	Region overview and system privileges (DSNADM, MDSNSM)			
BP	Buffer pools	Memory areas that can hold data pages			
CL	Collections	Groups of packages with the same qualifier			
DB	Databases	Sets of tables, indexes, and table spaces			
GV	Variables	Global variables (session scope named memory variables)			
JR	Java archives	Sets of files comprising Java applications			
PK	Packages	Packages (pre-bound SQL statements)			
PN	Plans	Plans (control structures created during BIND)			
SC	Schemas	Logical classifications of database objects			
SG	Storage groups	Sets of storage objects (volumes)			
SP	Stored procs	Stored procedure and user function routines			
SQ	Sequences	User defined objects defining a numerical sequence			
TB	Tables/views	Tables and views			
TS	Table spaces	Table spaces (data set name space for storing tables)			
UT	User data types	Distinct types			

Figure 137. DB2 Resource menu

DB2 region reports

On Figure 137, select the **R** menu option to display the DB2 Regions selection panel in Figure 138.

Menu	Options	Info	Commands	Setup

zSecure Suite - DB2 - Regions				
Command ==> _____				
Show DB2 regions that fit all of the following criteria:				
Jobname	_____			(jobname or filter)
Local LU name	_____			(luname or filter)
Local site name	_____			(name or filter)
DB2ID	_____			(identifier or filter)
Group attachment name	_____			(name 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 138. DB2 Regions selection panel

Use this selection panel to enter your selection criteria in one or more fields to limit the data. When you specify selection criteria, the output includes only those records that match all the selection criteria. Filters can be used in some of the selection fields. To find out whether a field supports filters, use the 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*.

DB2 resource reports

In the DB2 Resource panel in Figure 137 on page 113, select the menu option of your choice. The corresponding selection panel is then displayed. For example, for DB2 Bufferpools:

Menu	Options	Info	Commands	Setup
zSecure Suite - DB2 - Buffer pools				
Command ==> _____				
Show DB2 bufferpools that fit all of the following criteria:				
Bufferpool name . . .	_____	(name or filter)		
DB2ID	_____	(identifier or filter)		
Complex	_____	(complex or filter)		
System	_____	(system or filter)		
Advanced selection criteria				
		_ Further selection		
Output/run options				
_ 0. No summary	1. Summary by region	2. Summary by bufferpool		
_ Show differences				
_ Print format	_ Customize title	_ Send as e-mail		
_ Background run	_ Full page form			

Figure 139. DB2 bufferpools selection panel

Use this panel to enter your selection criteria in one or more fields to limit the data. To see detailed field information, press **F1** on any field. This field-sensitive help function also describes which fields on the selection panels support filters. You can also find descriptions of the field names in “SELECT/LIST Fields” in *IBM Security zSecureCARLa Command Reference*.

When you specify selection criteria, the output includes only those records that match all the selection criteria. Some selection panels include some advanced selection criteria:

Further selection

When you select Further selection, a further selection panel is displayed. For example, for DB2 Schemas:

DB2 schemas display		Line 1 of 16
Command ==>		Scroll==> CSR
All DB2 schema records	15 Oct 2013 13:22	
Identification		
System name	AHJB	complex ADCDPL
DB2 System identification	DBAG	
Schema name	ADM	
Usage		
Number of Datatypes	0	Number of Indexes 0
Number of JARs	0	Number of Routines 0
Number of Sequences	0	Number of Tables 1
Number of Triggers	0	Number of Views 0
***** Bottom of Data *****		

Figure 140. DB2 schema detail display report

Other settings

When you select Other settings, a next selection panel is displayed. For example, for DB2 Databases:

Menu	Options	Info	Commands	Setup

zSecure Suite - DB2 - Databases				
Command ==> _____				
Show DB2 databases that fit all of the following criteria:				
Authid of owner . . . _____				
Authid of creator . . . _____				
Creation date _____ (operator+yyyy-mm-dd or				
Alter date _____ ddMMMyyyy + hh:mm:ss or				
hh:mm)				
Select flag fields (Y/N/blank)				
_ Implicitly created				

Figure 141. DB2 databases security settings selection panel

You can select output and run options or select no options. Report data is processed as soon as you press **Enter**. The overview panel that is then displayed shows a summary of the records that match your selection criteria. For example, for DB2 Java archive records (JARs):

DB2 jars display						Line 1 of 5
Command ==> _____						Scroll==> CSR
All DB2 jar records						3 Jan 2013 07:18
JAR name	Complex	DB2I	Schema	Owner	0	Created
DS_20110622080035	ADCDPL	DBAG	DPACK	DPACK		22Jun2011 08:06
DS_20110801131621	ADCDPL	DBAG	DPACK	DPACK		1Aug2011 13:18
DS_20110822105345	ADCDPL	DBAG	DPACK	DPACK		22Aug2011 10:59
DS_20110822110830	ADCDPL	DBAG	DPACK	DPACK		22Aug2011 11:09
DS_20110920131946	ADCDPL	DBAG	DPACK	DPACK		20Sep2011 13:21
***** Bottom of Data *****						

Figure 142. DB2 JARs overview display report

This data can only be listed if a CKFREEZE file is created during an APF-authorized run of zSecure Collect (the CKFCOLL program). For information about creating such a CKFREEZE file, see “zSecure Collect for z/OS” in *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.

On this overview display panel, you can use action commands. For example:

- R** Shows region information.
- S** Shows additional information

For detailed information on resource reports and complete lists of available action command for each report type, see the online help (F1) and “Resource reports for z/OS” in *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.

IP stack reports

This data is obtained from a CKFREEZE data set created by running zSecure Collect APF-authorized with the **TCPIP=YES** parameter. You can also report on SMF events 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 143 is displayed.

MenuOptionsInfoCommandsSetup

zSecure Audit for ACF2 - Resource - IP stack Selection

Command ==> _ start panel

Show TCP/IP stack configuration data that fit all of the following criteria:

Stack name (name or filter)

System (system or filter)

Sysplex (sysplex or filter)

Output/run options

Ports

Interfaces

AUTOLOG

Telnet server/ports

Show differences

Output in print format

Run in background

/

Rules

Routes

Resolver

Customize title

VIPA

Netaccess

FTP daemon

Send as e-mail

Figure 143. IP stack Selection panel

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.

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 144 on page 117 is displayed.

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 144. IMS Resource panel

In the IMS Resource panel in Figure 144, select the option of your choice. The corresponding selection panel is displayed. For example, the IMS Regions selection panel in Figure 145.

Menu	Options	Info	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 145. 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*.

VTAM application reports

Select **RE.N** from the Main menu to display the VTAM Applications selection panel in Figure 146 on page 118.

Menu	Options	Info	Commands	Setup

zSecure Suite - VTAM - Applications				
Command ==> _____				
Show VTAM applications that fit all of the following criteria:				
Logical Unit name	_____	(name or filter)		
ACB name	_____	(name or filter)		
Current state . . .	_____	(code like ACTIV, CONCT, etc, or hex value)		
Conv.lvl.security	1. ALREADYV 2. PERSISTV 3. CONV 4. AVPV 5. NONE			
Complex	_____	(complex or filter)		
System	_____	(system or filter)		
Output/run options				
1. Summary by system	2. Summary by major node	3. Summary by jobname		
Show differences				
Print format	Customize title	Send as e-mail		
Background run	Full page form			

Figure 146. VTAM Applications selection panel

Use this panel to enter your selection criteria in one or more fields to limit the data. To see detailed field information, press **F1** on any field. This field-sensitive help function also describes which fields on the selection panels support filters. You can also find descriptions of the field names in “SELECT/LIST Fields” in *IBM Security zSecureCARLa Command Reference*.

You can select output and run options or select no options. Report data is processed as soon as you press **Enter**. The overview panel that is displayed shows a summary of the VTAM application records that match your selection criteria.

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

A sample overview display panel for the VTAM application display report is shown in Figure 147.

VTAM application display											
Command ==> _____											
All VTAM application records											
1 May 2014 23:42											
LName	ACBname	Major	System	CurSt	DesSt	VerifyLU	Pre	Acq	CPa	PP0	SPO
TS00149	TS00049	A01MVS	IP01	CONCT	CONCT	NONE			CPa		
TS00150	TS00050	A01MVS	IP01	CONCT	CONCT	NONE			CPa		
TVT5004	TVT5004	VTAMSEG	IP01	ACTIV	ACTIV	NONE		Acq			
WUINCM01	WUINCM01	A01CICS	IP01	CONCT	CONCT	NONE		Acq	CPa		
***** Bottom of Data *****											

Figure 147. VTAM application detail display

The data for this report is available only if a CKFREEZE file is created during an APF-authorized run of zSecure Collect (the CKFCOLL program). For details about creating a CKFREEZE file, see “zSecure Collect for z/OS” in *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.

MQ region and resource reports

The MQ Resource menu shown in Figure 148 on page 119 is then displayed.

Menu	Options	Info	Commands	Setup	Startpanel

zSecure Suite - Resource - MQ					
Option ==>					
R	Regions	MQ region level settings (MxADMIN)			
CH	Channels	Channel definitions			
CO	Connections	Applications connected to Queue Manager			
IN	Initiators	Channel initiator overview and settings			
NL	Namelists	Lists of names			
PR	Processes	Process definitions and settings			
QU	Queues	Queue definitions and settings			
TO	Topics	Topics for Publish/Subscribe usage			

Figure 148. MQ Resource menu

MQ region reports

In the MQ Resource panel in Figure 148, select the **R** menu option to display the MQ Regions selection panel in Figure 149.

Menu	Options	Info	Commands	Setup

zSecure Suite - MQ - Regions				
Command ==> _____				
Show MQ regions that fit all of the following criteria:				
Jobname		_____	(jobname or filter)	
Region userid		_____	(userid or filter)	
MQ QMGR name/subsystem		_____	(name or filter)	
Complex		_____	(complex or filter)	
System		_____	(system or filter)	
Output/run options				
<input type="checkbox"/> Show differences				
<input type="checkbox"/> Print format			Customize title	Send as e-mail
<input type="checkbox"/> Background run			Full page form	

Figure 149. MQ Regions selection panel

Use this panel to enter selection criteria in one or more fields to limit the MQ region configuration data. When you specify selection criteria, the output includes only those records that match all the selection criteria. You can use filters in some of the selection fields. To find out whether a field supports filters, use the field-sensitive help function (F1).

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

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

MQ resource reports

In the MQ Resource panel in Figure 148, select the menu option of your choice. The corresponding selection panel is then displayed. For example, for MQ Queues:

```

Menu           Options           Info           Commands       Setup
-----
                                zSecure Suite - MQ - Queues

Command ==> _____

Show MQ queues that fit all of the following criteria:
Queue name . . . . . _____
Queue type . . . . . _ 1. Alias    2. Local    3. Model    4. Remote
MQ QMGR name/subsystem _____ (name or filter)
Complex . . . . . _____ (complex or filter)
System . . . . . _____ (system or filter)

Advanced selection criteria
                                _ Further selection

Output/run options
_ 0. No summary                1. Summary by region    2. Summary by queue
_ Show differences
_ Print format                 _ Customize title          _ Send as e-mail
_ Background run               _ Full page form

```

Use this panel to enter your selection criteria in one or more fields to limit the data. To see detailed field information, press **F1** on any field. This field-sensitive help function also describes which fields on the selection panels support filters. You can also find descriptions of the field names in “SELECT/LIST Fields” in *IBM Security zSecureCARLa Command Reference*.

```

Menu      Options      Info      Commands      Setup
-----
                        zSecure Suite - MQ - Channels

Command ==> _____

Show MQ channels that fit all of the following criteria:
Transmit queue name _____
Userid for channel . . _____ (userid or filter)
Alter date . . . . . _____ (operator+yyyy-mm-dd)

Select flag fields (Y/N/blank)
OR      (AND or OR relationship)
_ Password set for channel      _ SSL Client auth required

```

You can select output and run options or select no options. Report data is processed as soon as you press **Enter**. The overview panel that is then displayed shows a summary of the records that match your selection criteria. For example, for MO Connections:

Figure 152. MQ connections display

This data can only be listed if a CKFREEZE file is created during an APF-authorized run of zSecure Collect (the CKFCOLL program). For information about creating such a CKFREEZE file, see “zSecure Collect for z/OS” in *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.

On this overview display panel, you can use action commands. For example:

- R** Shows region information.
- S** Shows additional information

For detailed information on resource reports and complete lists of available action command for each report type, see the online help (F1) and “Resource reports for z/OS” in *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.

UNIX file system reports

When you select option **RE.U**, the Resource - UNIX panel shown in Figure 153 opens.

Menu	Options	Info	Commands	Setup

zSecure Audit for ACF2 - Resource - Unix				
Option ==> _____				
F	Filesystem	Unix filesystem selection		
R	Reports	Unix audit reports		

Figure 153. 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 154 opens.

Menu	Options	Info	Commands	Setup

zSecure Audit for ACF2 - Resource - Unix Selection				
Command ==> _____ _ start panel				
Show Unix files that fit all of the following criteria:				
Path name . _____				
_____ (name or filter)				
File name . _____ (name or filter)				
Complex . _____ (complex or EGN mask)				
Advanced selection criteria				
<input type="checkbox"/> File attributes <input type="checkbox"/> File system <input type="checkbox"/> File ACL				
Output/run options				
<input type="checkbox"/> Show differences				
<input type="checkbox"/> Output in print format <input type="checkbox"/> Customize title <input type="checkbox"/> Send as e-mail				
<input type="checkbox"/> Run in background				

Figure 154. Resource UNIX selection panel

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 155.

zSecure Audit for ACF2 UNIX summary				Line 1 of 26
Command ==>				Scroll==> CSR_
All Unix files				7 Dec 2009 11:24
Complex	System	Count		
ACF2	ACF2	68117		
Count	FS mount point			
— 17	/			
— 52	/u			
— 2	/u/automount			
— 4	/u/automount/crmbert			
— 2	/u/automount/crmbhj1			
— 2	/u/automount/crmbpe1			
— 1	/u/automount/crmcss1			
— 219	/u/c2eaudit			
— 11	/ACF2			
— 23	/ACF2/dev			
— 467	/ACF2/etc			
— 3303	/ACF2/etc/WebSphere/V6R0M1			
— 4	/ACF2/tmp			
— 24	/ACF2/var			

Figure 155. UNIX summary display

Selecting any of the mount points listed in the UNIX summary panel (Figure 155) displays the list of UNIX files for that mount point as shown in Figure 156 on page 123.

```

zSecure Audit for ACF2 UNIX summary                                     Line 1 of 446
Command ==> _____ Scroll==> CSR_
All Unix files                                                         7 Dec 2009 11:24
Complex System Count
ACF2      ACF2      68117
Count FS mount point
      219 /u/c2eaudit
T FileMode + apsl AuF Relative pathname (within FS)
__ d          fff .
__ -          --s- fff .profile
__ -          --s- fff .sh_history
__ d          fff TCIM_8.5
__ l          fff TCIM_8.5/bin
__ d          fff TCIM_8.5/log
__ -          --s- fff TCIM_8.5/log/about-agent.log
__ -          --s- fff TCIM_8.5/log/actuator108.log
__ -          --s- fff TCIM_8.5/log/actuator108.log0
__ -          --s- fff TCIM_8.5/log/actuator108.log1
__ -          --s- fff TCIM_8.5/log/actuator108.log2
__ -          --s- fff TCIM_8.5/log/actuator109.log

```

Figure 156. UNIX summary panel - UNIX file list for selected mount point

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 156), the UNIX file detail display panel shown in Figure 157 on page 124 opens. To view the contents of a file in this panel, type **S** in front of the **Absolute pathname** field.

```

zSecure Audit for ACF2 UNIX summary                               Line 1 of 57
Command ==> _____ Scroll==> CSR_
All Unix files                                                  7 Dec 2009 11:24

System view of file
Complex name             ACF2
Sysplex name            ACF2AD2R
System name             ACF2
- Absolute pathname      /u/c2eaudit/.profile
FS mounted with SECURITY Yes
FS mounted with SETUID  No
FS mounted READ/WRITE   Yes
File access attributes
Extended file attributes +s -apl
Effective audit flags    =f
Device                  11
Relative audit priority
Audit concern

Physical file attributes
Complex that owns file system ACF2
System that owns file system ACF2
File system data set name    OMVS.C2EAUDIT.HFS
Volume serial for file system ACF2U1
File system DASD serial + id STK-02-000000006214-011B
Relative pathname within FS  .profile
File type                  -
Physical access attributes  o=u,rwx,g=r
Physical extended attributes +s -apl
User-requested audit flags  =f
Auditor-specified audit flags =
User id                    10002
Group id                   0
Inode number               16
File audit id              01C1C3C6F2E4F1001D20000000100000
Number of hard links        1
Link target

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

```

Figure 157. UNIX detail display

For more detailed information about these reports, see *IBM Security zSecure Audit for ACF2: User Reference Manual* and the online help.

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

```

zSecure Audit for ACF2 Display Selection                        3 s elapsed, 0.8 s CPU
Command ==> _____ Scroll==> PAGE

Name      Summary Records Title
- MOUNT      1      19 Effective UNIX mount points
- UNIXAPF2    1     303 UNIX files with APF authorization
- UNIXCTL2    1    3838 UNIX files that are program controlled (daemons etc.
- UNIXSUI2    0      0 UNIX files with SETUID authorization
- UNIXSGI2    0      0 UNIX files with SETGID authorization
- GLB2UNIX    0      0 UNIX files vulnerable to trojan horse & back door at
***** Bottom of Data *****

```

Figure 158. UNIX Reports listing

Chapter 9. Event reporting

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

Record type	Description
14	INPUT or RDBACK data set Activity
16	OUTPUT, UPDATE, INOUT, or OUTIN data set Activity
17	Scratch data set Status
18	Rename data set Status
30	Common Address Space Work
60	VSAM Volume data set Updated
61	ICF Define Activity
62	VSAM Component or Cluster Opened
63	VSAM Catalog Entry Defined
64	VSAM Component or Cluster Status

Table 15. SMF Record types that should not be filtered out of the SMF data (continued)

Record type	Description
65	ICF Delete Activity
66	ICF Alter Activity
67	VSAM Catalog Entry Delete
68	VSAM Catalog Entry Renamed
69	VSAM Data Space, Defined, Extended, or Deleted
83	Audit security event records from IBM Security Key Lifecycle Manager and WebSphere Application server.
90	System Status
92	UNIX Hierarchical file system
102	DB2 Performance and Audit
109	Firewall
110	CICS performance monitoring
118	TCP/IP Telnet and FTP
119	TCP UDP and IP
120	WebSphere Application Server
230	ACF2 Processing

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 159 on page 127 opens so you can assign a type to the file you are defining.

Menu	Options	Info	Commands	Setup
zSecure Audit for ACF2 - Setup - Input				Row 1 to 13 of 13
Command ==>				Scroll ==> CSR_
Select the type of data set or file				
-	ACF2INFO	The Infostorage component of an ACF2 database		
-	ACF2LID	The component of an ACF2 database that contains Logonids		
-	ACF2RULE	The component of an ACF2 database that contains Rules		
-	ACT.SMF	The live SMF data set(s)		
-	ACT.SYSTEM	Live settings		
-	ACT2.BACK	The backup ACF2 database of your active system		
-	CKFREEZE	System resource information data set		
-	INACT2.BACK	The inactive backup ACF2 database of your system		
-	SMF	VSAM or dumped SMF		
-	SMF.LOGSTR	SMF logstream		
-	UNLOAD	An unloaded ACF2 database		
-	WEBACCESS	IBM HTTP Server access log		
-	WEBERROR	IBM HTTP Server error log		
***** Bottom of data *****				

Figure 159. Assign file type

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 160.

Menu	Options	Info	Commands	StartPanel
zSecure Audit for ACF2 - Setup - Input file				I Row 1 from 5
Command ==>				Scroll ==> CSR_
(Un)select (U/S) set of input files or work with a set (B, E, R, I, D or F)				
	Description	Complex		
-	Filtered SMF data set			selected
-	Input set created 8 Apr 2005			selected
-	Active primary ACF2 data base	DEMO		
-	Active backup ACF2 data base	DEMO		
-	Active backup ACF2 data base and live SMF data sets	DEMO		
***** Bottom of data *****				

Figure 160. Input file settings

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 159 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

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.

Menu	Options	Info	Commands	Setup

zSecure Audit for ACF2 - Events				
Option	====>	More: +		
SE	Setup	Options and input data sets		
AA	ACF2	ACF2 Administration		
AU	Audit	Audit security and system resources		
RE	Resource	Resource reports		
EV	Events	Event reporting from SMF and other logs		
U	User	User events from SMF		
D	Data set	Data set events from SMF		
R	Resource	General resource events from SMF		
F	Filesystem	Unix filesystem events from SMF and other logs		
I	IP	IP events from SMF and other logs		
0	z/OS other	z/OS system level change events and ICSF		
1	SMF reports	Predefined analysis reports		
3	ACF2 events	ACF2 logging for specific events		
4	DB2	DB2 events from SMF		
5	CICS	CICS events from SMF		
6	Omegamon	Omegamon events from SMF		
C	Custom	Custom report		
CO	Commands	Run commands from library		
IN	Information	Information and documentation		
LO	Local	Locally defined options		
X	Exit	Exit this panel		
Input complex: *NONAME*				
Product/Release				
5655-N17 IBM Security zSecure Audit for ACF2 2.2.0				

Figure 161. Main menu - select Events option

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

Menu	Options	Info	Commands	Setup

zSecure Audit for ACF2 - Events - ACF2 events				
Command	====>			
Enter "/" to select report(s)				
- All	Overview of all ACF2 events			
- Logging	ACF2 logging except successful logon/job initiation			
- Not normal	ACF2 access not due to normal profile access			
- Warnings	ACF2 access due to rules in warn mode			
- Violations	ACF2 dataset/resource access violations			
- Maintenance	ACF2 logonid/rule/record updates (other than logon)			
- Logonfailure	ACF2 logon/job initiation failures			
- ACF2 events	ACF2 start/stop/modify/abend records			
Input complex: *NONAME*				
Product/Release				
5655-N17 IBM Security zSecure Audit for ACF2 2.1.1				

Figure 162. ACF2 Events panel

4. To select the SMF reports option, in the Events panel (Figure 161), type **1** in the **Option** field and press **Enter**. The SMF reports panel is displayed.

Menu	Options	Info	Commands	Setup

IBM Security zSecure Audit for ACF2 - Events - SMF reports				
Option ==> 1				
1	Exceptions	ACF2 exception report		
6	Stat hour	ACF2 statistics by hour (180 characters wide)		
7	Stat time	ACF2 statistics by time		
8	Stat day	ACF2 statistics by weekday		
9	Job viols	Dataset violations by batch jobs		
A	APPC conv	APPC conversation summary		

Figure 163. SMF reports - select Exceptions report

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 164. 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.

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

Menu	Options	Info	Commands	Setup

IBM Security zSecure Audit for ACF2 - Events - Options				
Command ==>				
Input and output specifications				
Max number of SMF records to read . . .		_____ (default is no limit)		
Max number of records per display group		_____ (default is no limit)		
Complete with SAF data 1 1. Yes 2. No 3. Minimal				
- Output in print format				
- Use CKFREEZE data				
- Show number of SMF records selected				
- Run in background				

Figure 164. SMF processing options - press ENTER and continue to next screen

- In the Options panel, press Enter to open the Display Selection panel as shown in Figure 165 on page 130.

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.

```

IBM Security zSecure Audit for ACF2 Display Selection 33 s elapsed, 14.2 s CPU
Command ==> _____ Scroll==> CSR_

Name      Summary Records Title
- LOGF_T_F 0      2 Logon failures per source - frequent
- LOGF_T_I 0      2 Logon failures by source - infrequent but more than
- LOGF_L_F 0      2 Logon failures per logonid - frequent
- LOGF_L_I 0      2 Logon failures per logonid - infrequent but more tha
- DVIO_D_F 0      0 Data set access violations by dataset - frequent
- DVIO_L_F 0      0 Data set access violations by logonid - frequent
- DVIO_L_I 3     40 Data set access violations by logonid - infrequent
S RVIO_R_F 1      2 Resource access violations by rule - overview
- RVIO_L_F 0      2 Resource access violations by logonid - frequent
- RVIO_L_I 1      2 Resource access violations by logonid - infrequent
- VIOLGSO 0      0 Invalid GSO
- ACF2MSG 12     12 ACF2 start/modify/stop events and messages - chronol
***** BOTTOM OF DATA *****

```

Figure 165. Overview of ACF2 events display

Figure 165 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

Exception event code	Definition
LOGF_x_x	Logon Failure, T=terminals or source, L=logon IDs, F=frequent, I=infrequent
DVIO_x_x	Data set violation, L=Logonid, F=frequent, I=infrequent
RVIO_x_x	Resource violation, L=Logonid, F=frequent, I=infrequent

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

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 165, 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 166.

```

Resource access violations by rule - overview Line 1 of 1
Command ==> _____ Scroll==> CSR_
27Apr05 00:09 to 8May05 00:01

Rulekey Count
R-PGM-PAYROLL 2
Logonid Full Name Sys Count
- JSMITH SMITH, JOHN DEMO 2
***** BOTTOM OF DATA *****

```

Figure 166. Display of resource access violations by rule - overview

In Figure 166 on page 130, 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 166 on page 130 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.

In the example shown in Figure 166 on page 130, the resource rule is a **PGM type - PROGRAM** rule.

- **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 111.

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

Viewing ACF2 database maintenance activity

About this task

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 167. Then, press Enter to open the ACF2 events panel as shown in Figure 168 on page 132.

Menu	Options	Info	Commands	Setup

zSecure Audit for ACF2 - Main menu				
Option	====>	EV		
SE	Setup	Options and input data sets		
AA	ACF2	ACF2 Administration		
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		
LO	Local	Locally defined options		
X	Exit	Exit this panel		
Input complex: *NONAME*				
Product/Release				
5655-N17 IBM Security zSecure Audit for ACF2 2.2.0				

Figure 167. Select ACF2 events

- Press Enter to open the ACF2 events panel as shown in Figure 168.
- In the ACF2 events panel, type / in the selection field for the **Maintenance** field as shown in Figure 168. Then, press Enter.

Menu	Options	Info	Commands	Setup

IBM Security zSecure Audit for ACF2 - Events - ACF2 events				
Option	====>			
Enter "/" to select report(s)				
_ All		Overview of all ACF2 events		
_ Logging		ACF2 logging except successful logon/job initiation		
_ Not normal		ACF2 access not due to normal profile access		
_ Warnings		ACF2 access due to rules in warn mode		
_ Violations		ACF2 dataset/resource access violations		
/ Maintenance		ACF2 logonid/rule/record updates (other than logon)		
_ Logonfailure		ACF2 logon/job initiation failures		
_ ACF2 events		ACF2 start/stop/modify/abend records		

Figure 168. Select the Maintenance report

The next screens do not necessarily require any data entry for our example.

- Press Enter on the next three screens that open until you reach the panel shown in Figure 169.

Figure 169 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.

SMF record ACF2 processing and audit records			38 s elapsed, 10.7 s CPU
Command ===>			Scroll====> CSR
			27Apr05 15:20 to 19May05 17:23
Date	Time	Description	
27Apr2005	15:20	56 ACF2 id MSTJCLEX delete resource C-TSO-CRMBNAT	
29Apr2005	10:41	ACF2 id JSMITH replace rule SYS1	
29Apr2005	11:12	ACF2 id JSMITH insert logonid SMCLEAN	
29Apr2005	11:16	ACF2 id JSMITH replace logonid SMCLEAN	
29Apr2005	11:27	ACF2 id JSMITH replace logonid SMCLEAN	
29Apr2005	11:28	ACF2 id JSMITH replace logonid SMCLEAN	
29Apr2005	11:28	ACF2 id JSMITH replace logonid SMCLEAN	
19May2005	11:30	ACF2 id SMCLEAN delete logonid PBAKER	
19May2005	11:30	ACF2 id SMCLEAN insert logonid GBROWN(model SMCLEAN)	
19May2005	11:40	ACF2 id SMCLEAN insert resource C-GSO--	MAINTMAINTDUMP
19May2005	11:41	ACF2 id SMCLEAN delete resource C-GSO--	MAINTMAINTDUMP
19May2005	11:41	ACF2 id SMCLEAN insert resource C-GSO--	MAINTDUMP
19May2005	11:43	ACF2 id SMCLEAN delete resource C-GSO--	MAINTDUMP
19May2005	11:44	ACF2 id SMCLEAN insert resource C-GSO-0261	MAINTDUMP
19May2005	11:51	ACF2 id SMCLEAN delete resource C-GSO-0261	MAINTDUMP
19May2005	11:52	ACF2 id SMCLEAN insert resource C-GSO-0261	MAINT
19May2005	12:13	ACF2 id SMCLEAN replace resource C-GSO-0261	INFODIR
19May2005	12:15	ACF2 id SMCLEAN insert resource C-GSO-0261	PDS.TEST
19May2005	14:41	ACF2 id SMCLEAN delete logonid TESTC00	
19May2005	14:41	ACF2 id SMCLEAN delete logonid TESTC10	
19May2005	14:41	ACF2 id SMCLEAN delete logonid TESTC20	
19May2005	14:41	ACF2 id SMCLEAN delete logonid TESTC30	
19May2005	14:41	ACF2 id SMCLEAN delete logonid TESTC40	
19May2005	14:41	ACF2 id SMCLEAN delete logonid TESTC50	
19May2005	14:41	ACF2 id SMCLEAN delete logonid TESTC60	
19May2005	14:41	ACF2 id SMCLEAN delete logonid TESTC70	
19May2005	14:41	ACF2 id SMCLEAN delete logonid TESTC80	
19May2005	14:41	ACF2 id SMCLEAN delete logonid TESTC90	
19May2005	14:41	ACF2 id DBHOGAN delete logonid TESTC99	
***** BOTTOM OF DATA *****			

Figure 169. Maintenance activity against the ACF2 databases

Viewing user events

Procedure

- 1. Press PF3 to return to the Main menu.
- 2. In the Main menu, type U in the command line to select the User option as shown in Figure 170.
- 3. Press Enter to open the User Selection panel shown in Figure 171 on page 134.

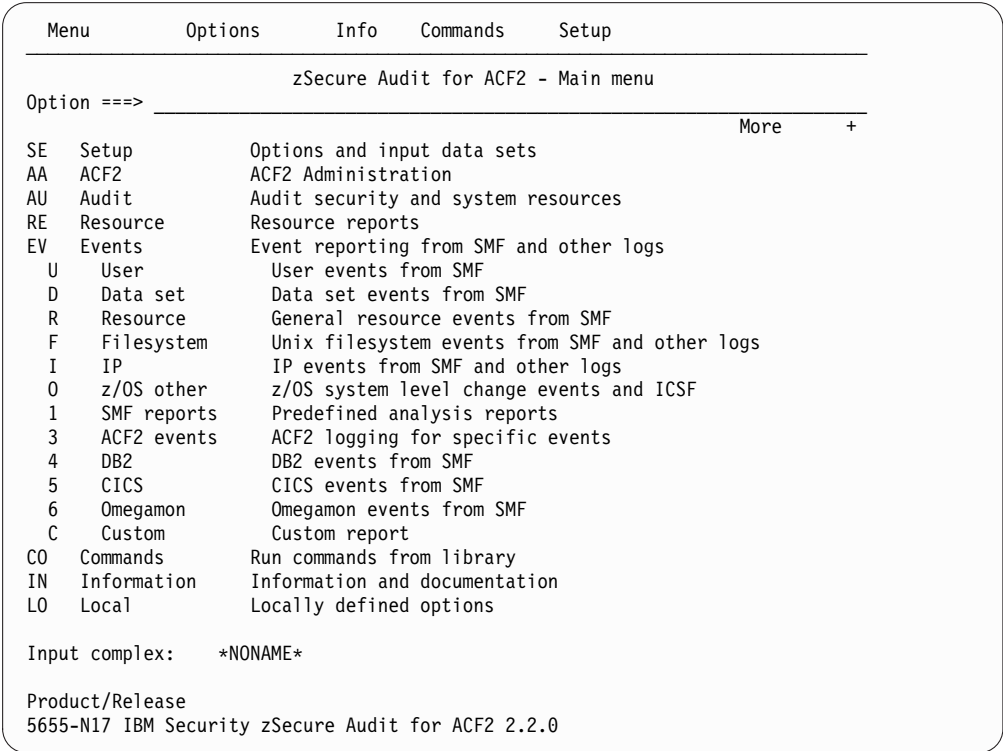


Figure 170. Select User events

- 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 171 on page 134 uses JSMITH.

Menu	Options	Info	Commands	Setup

zSecure Audit - Events - User Selection				
Command ==> _____ _ start panel				
Show records that fit all of the following criteria:				
Logonid JSMITH _____ (logonid or ACF2 mask)				
System _____ (system name or ACF2 mask)				
Name _____ (name/part of name, no filter)				
Jobname _____ (job name or ACF2 mask)				
Source _____ (Source id or ACF2 mask)				
Advanced selection criteria				
_ User actions		_ User attributes		_ Date and time
_ Data set selection		_ HFS selection		_ Resource selection
_ DB2 selection		_ CICS selection		_ Omegamon selection
_ IP selection				
Output/run options				
_ Include detail		_ Summarize		_ Specify scope
_ Output in print format		_ Customize title		_ Send as email
_ Run in background				

Figure 171. User selection panel - type your logon ID to view user events

3. Press Enter to view the events.

In this example, all events for JSMITH are shown in Figure 172 on page 135. 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.

SMF records for users like JSMITH 27Apr05 15:20 to 3May05 17:23

Date	Time	Description
29Apr2005	02:21:08.68	Start of job JSMITH (TSU01634) for user JSMITH
29Apr2005	02:21:08.68	Start of job JSMITH for user JSMITH
29Apr2005	02:22:26.95	Define data set JSMITH.CN1.S0290.CMDOUT in ICF catal
29Apr2005	02:22:32.94	Define data set JSMITH.CN1.D01363.T8550C.CMDOUT in I
29Apr2005	02:24:37.21	ACF2 id JSMITH READ access XFC CKR.READALL from LC
29Apr2005	02:31:03.72	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
29Apr2005	02:33:23.72	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
29Apr2005	02:34:58.54	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
29Apr2005	02:43:48.89	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
29Apr2005	03:02:01.80	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
29Apr2005	03:10:08.37	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
29Apr2005	03:17:47.34	Totals for step TSOPROC2 of job JSMITH for user JSMITH
29Apr2005	03:17:47.56	End of job JSMITH (TSU01634) for user JSMITH code S622
29Apr2005	03:17:47.63	TSO/E User Work Accounting for user JSMITH (commands fou
30Apr2005	22:59:55.28	Start of job JSMITH (TSU01660) for user JSMITH
30Apr2005	22:59:55.29	Start of job JSMITH for user JSMITH
30Apr2005	23:01:01.33	Define data set JSMITH.CN1.D01364.T82858C.CMDOUT in
30Apr2005	23:03:55.39	ACF2 id JSMITH READ access XFC CKR.READALL from LC
30Apr2005	23:20:52.52	ACF2 id JSMITH READ access XFC CKR.READALL from LC
30Apr2005	23:46:10.57	Totals for step TSOPROC2 of job JSMITH for user JSMITH
30Apr2005	23:46:10.82	End of job JSMITH (TSU01660) for user JSMITH code RC0
30Apr2005	23:46:10.83	TSO/E User Work Accounting for user JSMITH (commands fou
01May2005	23:30:36.97	Start of job JSMITH (TSU01668) for user JSMITH
01May2005	23:30:37.02	Start of job JSMITH for user JSMITH
01May2005	23:32:04.31	Define data set JSMITH.CN1.S0290.CMDOUT in ICF catal
01May2005	23:32:10.34	Define data set JSMITH.CN1.D01365.T84728C.CMDOUT in
01May2005	23:37:30.02	ACF2 id JSMITH READ access XFC CKR.READALL from LC
01May2005	23:50:25.35	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
01May2005	23:52:55.21	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
01May2005	23:55:01.15	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
01May2005	23:58:53.23	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
02May2005	00:53:21.13	Totals for step TSOPROC2 of job JSMITH for user JSMITH
02May2005	00:53:21.38	End of job JSMITH (TSU01668) for user JSMITH code RC0
02May2005	00:53:21.45	TSO/E User Work Accounting for user JSMITH (commands fou
02May2005	21:20:58.36	Start of job JSMITH (TSU01674) for user JSMITH
02May2005	21:20:58.36	Start of job JSMITH for user JSMITH
02May2005	21:22:23.21	Define data set JSMITH.CN1.S0290.CMDOUT in ICF catal
02May2005	21:22:30.91	Define data set JSMITH.CN1.D02001.T76948C.CMDOUT in
02May2005	21:28:30.19	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
02May2005	21:30:41.52	ACF2 id JSMITH READ access XFC CKR.READALL from LC
02May2005	21:42:45.32	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
02May2005	21:45:04.97	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
02May2005	21:48:38.77	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
02May2005	21:49:50.75	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
02May2005	21:51:45.59	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
02May2005	22:02:37.77	ACF2 id JSMITH READ access XFC CKR.READALL from LC
02May2005	22:18:01.24	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
02May2005	22:23:05.65	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
02May2005	22:29:39.84	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
02May2005	22:32:44.20	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
02May2005	22:34:51.55	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
02May2005	22:41:40.67	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
02May2005	22:43:47.22	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
02May2005	22:47:43.16	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
02May2005	22:50:16.51	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
02May2005	22:51:28.81	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
02May2005	22:52:48.60	ACF2 id JSMITH READ access XFC CKR.READALL from LC
02May2005	22:53:16.01	VVDS updated for data set SYS290.MAN1.DATA on volume SYS2
02May2005	22:53:58.19	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO
02May2005	22:56:52.31	Define data set JSMITH.ISPFCAP.RTF in ICF catalog CATALO

Figure 172. User events report

Chapter 10. Report generation

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

- “Creating an audit report”
- “Archiving reports” on page 139
- “Printing reports” on page 140

Creating an audit report

Procedure

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 173.

Menu	Options	Info	Commands	Setup

zSecure Audit for ACF2 - Audit				
Option	====> AU			More: +
SE	Setup	Options and input data sets		
AA	ACF2	ACF2 Administration		
AU	Audit	Audit security and system resources		
C	Change track	Track changes to the system		
L	Libraries	Library status and update analysis		
R	Compliance	Rule-based compliance evaluation		
S	Status	Status auditing of security and system tables/options		
RE	Resource	Resource reports		
EV	Events	Event reporting from SMF and other logs		
CO	Commands	Run commands from library		
IN	Information	Information and documentation		
LO	Local	Locally defined options		
X	Exit	Exit this panel		
Input complex: *NONAME*				
Product/Release				
5655-N17 IBM Security zSecure Audit for ACF2 2.1.1				

Figure 173. Main menu - select Audit option

2. After selecting the Audit option, type S in the Option command line to select the Audit Status option as shown in Figure 174 on page 138.

```

Menu  Options  Info  Commands  Setup
-----
                                zSecure Audit for ACF2 - Audit
Option ==> S
More:  +
SE  Setup      Options and input data sets
AA  ACF2       ACF2 Administration
AU  Audit      Audit security and system resources
  C  Change track  Track changes to the system
  L  Libraries    Library status and update analysis
  R  Compliance  Rule-based compliance evaluation
  S  Status      Status auditing of security and system tables/options
RE  Resource    Resource reports
EV  Events      Event reporting from SMF and other logs
CO  Commands   Run commands from library
IN  Information Information and documentation
LO  Local      Locally defined options
X   Exit       Exit this panel

Input complex:  *NONAME*

Product/Release
5655-N17 IBM Security zSecure Audit for ACF2 2.1.1

```

Figure 174. Select Audit Status option

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 175. The selections are shown in bold type.

```

Menu  Options  Info  Commands  Setup
-----
                                zSecure Audit for ACF2 - Audit -   Please choose one
Command ==>
Enter / to select report categories
- MVS tables      MVS oriented tables (reads first part of CKFREEZE)
- MVS extended    MVS oriented tables (reads whole CKFREEZE)
/ ACF2 control    ACF2 oriented tables
- ACF2 user       User oriented ACF2 tables and reports
- ACF2 resource   Resource oriented ACF2 tables and reports

Select options for reports:
- Select specific reports from selected categories
- Include audit concern overview, higher priorities only
/ Output in print format  - Concise (short) report
- Run in background
Audit policy
/ zSecure
- C1
- C2
- B1

```

Figure 175. Select Output in print format

- b. Press Enter. Figure 176 on page 139 shows the report generated after selecting report settings and pressing Enter. To review the entire report, scroll to the right and down.

```

BROWSE - CRMBDBH.CN1.S0290.REPORT ----- LINE 0000 0.3 s CPU, RC=0
COMMAND ==> _____ SCROLL ==> PAGE
***** Top of Data *****
S Y S T E M   S E T T I N G S   15 May 2005 22:10
GSO system settings

Complex System Collect timestamp
DEMO DEMO 15 May 2005 22:10

Option settings (OPTS)
-----
Mode MODE ABORT
Reports are scoped RPTSCOPE No Records TSO cmd CMDREC No CP
Date format DATE MM/DD/YY Batch default LID DFTLID Ch
Show last logon time NOTIFY Yes Protect Tape DSN TAPEDSN No Se
Logonid in SMF STAMPSMF No LID expiration # days WRNDAYS 5 Ch
TSO UADS UADS No Log all BLP usage BLPLOG No ST
Start only marked STCs STC Yes ACCESS subcommand enabled Yes LD
Can list any infost. records SeAu

Access rule settings (RULEOPTS) Backup parameters (BACKUP) TS
-----
Allow use of $NOSORT Yes Backup time TIME 06:00 Ch

```

Figure 176. Sample report output - ACF2 Control report

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 140.

Archiving reports

Procedure

1. Type W in the Report selection field as shown in Figure 177.

```

Menu Options Info Commands Setup
-----
IBM Security zSecure Audit for ACF2 - Results
Command ==> _____

The following selections are supported:
B Browse file S Default action (for each file)
E Edit file R Run commands
P Print file J Submit Job to execute commands
V View file W Write file into seq. or partitioned data set
M Email report

Enter a selection in front of a highlighted line below:
- SYSPRINT messages
W REPORT printable reports
- CKRTSPRT output from the last TSO commands
- CKRCMD queued TSO commands
- CKR2PASS queued commands for zSecure Audit for ACF2
- COMMANDS IBM Security zSecure Audit for ACF2 input commands from last query
- SPFLIST printable output from PRT primary command
- OPTIONS set print options

```

Figure 177. Write reports to data set from the Results panel

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 178 on page 140.

4. If the data set is partitioned (PDS), type the member name in the **Member** field as shown in Figure 178.

```

Menu  Options  Info  Commands  Setup
-----
IBM Security zSecure Audit for ACF2 - Results
Command ==> _____

Write the IBM Security zSecure Audit for ACF2 report file to the following dataset:

Data set name . . . . . 'JSMITH.ACF.AUDIT.REPORT'
Member . . . . . GSO
Disposition . . . . . 1 1. Append      2. Overwrite      3. Generate

Processing option after Write completed:
Go into Edit . . . . . N_          (Yes/No)

```

Figure 178. Specify the data set name for archiving reports

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

1. Type P beside the report selection as shown in Figure 179.
2. Press Enter.

```

Menu  Options  Info  Commands  Setup
-----
IBM Security zSecure Audit for ACF2 - Results
Command ==> _____

The following selections are supported:
B Browse file          S Default action (for each file)
E Edit file            R Run commands
P Print file           J Submit Job to execute commands
V View file            W Write file into seq. or partitioned data set
M Email report

Enter a selection in front of a highlighted line below:
- SYSPRINT messages
P REPORT printable reports
- CKRTSPRT output from the last TSO commands
- CKRCMD  queued TSO commands
- CKR2PASS queued commands for zSecure Audit for ACF2
- COMMANDS IBM Security zSecure Audit for ACF2 input commands from last query
- SPFLIST  printable output from PRT primary command
- OPTIONS  set print options

```

Figure 179. Printing reports from the Results panel

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 180 on page 141 shows an example of the print result message. **Output to Spool** indicates that your report is staged for hardcopy printing.


```
Menu  Options  Info  Commands  Setup
-----
      IBM Security zSecure Audit for ACF2 – Results      Output to Spool
Command ==>

The following selections are supported:
B Browse file          S Default action (for each file)
E Edit file            R Run commands
P Print file           J Submit Job to execute commands
V View file            W Write file into seq. or partitioned data set
M Email report

Enter a selection in front of a highlighted line below:
- SYSPRINT  messages
P REPORT    printable reports
- CKRTSPRT  output from the last TSO commands
- CKRCMD    queued TSO commands
- CKR2PASS  queued commands for zSecure Audit for ACF2
- COMMANDS  IBM Security zSecure Audit for ACF2 input commands from last query
- SPFLIST   printable output from PRT primary command
- OPTIONS   set print options
```

Figure 180. Printing reports - Print result message

Appendix A. Frequently asked questions

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=NO 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.

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?

Table 17. Frequently Asked Questions (continued)

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 an 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.

```
//SYSIN DD *  
PARALLEL=PATHGROUP (reduces parallel operation), or  
PARALLEL=NONE      (remove any parallel operation)  
CAT=MCAT            (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 181. 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 x
- ACF2
 - database maintenance 131
 - exception report 128
 - masking characters 10
 - override viewing scope 7
 - 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 128
- ACF2_LID display 7
- ACF2_LID display panel 16, 19
- analyze data set access 42
- archive a report 139
- AU.R 99
- AU.R - standard compliance test results (STDTESTS) 105
- AU.R - standard object type compliance summary (STDYPES) 104
- AU.R - standard rule set compliance summary (STD RULES) 102
- audit concern reports 92
- audit concerns
 - logon ID details 16
 - overview by priority 77
 - prioritize 77
 - use of 75
 - view 76
- audit function 75
- Audit panel 137
- audit priority values 77, 87
- Audit Selection panel 10
- Authorized Programs report 93

B

- Boolean operators 11
- Boolean operators for logon ID display 23

C

- CICS
 - region, transaction, and program data report 111
 - Resource panel 111
- Collections, SETUP 73
- compliance evaluation 99

D

- data flow 2

- data set
 - analyzing access 42
 - display NEXTKEYs 45
 - rule lines 40
 - rule structure 48
- 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 131
- date values 11
- DB2 reports
 - resource 114
- DB2 Resource panel 113
- default ACF2 scoping 7
- define input sets 125
- display Logon IDs 14
- Display Selection panel 92
- DUMPDATE date 11

E

- education x
- event report 125
- 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 x
 - Support Assistant x
- IMS
 - Resource panel 116
- IMS region, transaction, and program data reports 116
- individual scope record 64
- Infostorage
 - database 61
 - records 61
 - sample scope records 5
- input
 - data 69, 126
 - new files 69
- set
 - composition 71
 - selecting 72

- IP stack configuration report 115
- IP stack Selection panel 115
- ISPF 1

L

- LIST command 19, 33
- LIST Output error 7
- list rule lines
 - data set access 43
 - view for specific data set 40
- logon ID
 - access 13
 - display 14
 - display for same user name 24
 - display using a mask 20
 - display using Boolean operators 23
 - field descriptions 14
 - records 16
 - settings 18
 - special privileges to list 22
 - uid string to display 21
 - view user events 133
- Logon ID selection panel 8
- Logonid Selection panel 14

M

- Main menu panel 9, 13
- Maintenance report 131
- mask for logon IDs 20
- masking characters 10
- memory requirements for zSecure Collect 145
- MQ reports
 - Regions selection panel 119
 - selection panel 119
- 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, vi, viii
 - terminology v
- options
 - RE.C 111
 - RE.M 116

options (*continued*)
SE.B 73

P

panel
Rules Selection 10
panels
ACF2 Events 128
ACF2_LID display 16, 19
Audit 137
Audit Selection 10
CICS Resource 111
DB2 selection 114
Display Selection 92
IMS Resource 116
IP stack Selection 115
Logon ID selection 8
Logonid Selection 14
Main menu 9, 13
MQ Regions 119
MQ selection 119
New files 69
Resource DB2 112, 113
Resource VTAM 117
RULELINE display 42
Rules Selection 40
screen navigation 8
UNIX Selection 121
UNIX summary 121
password
audit concerns 88
settings 82
print report 137, 140
problem-determination x
product
overview 1
publications
accessing online v, vi, viii
list of for this product v, vi, viii
obtaining licensed v
obtaining licensed publications vi

R

RE.C option 111
RE.M option 116
recommended password settings 82
refresh and load files 71
remote data for reports 3
reports
ACF2 control settings 137
ACF2 exception 128
archiving 139
AU.R 100
audit concern 92
Authorized Programs 93
CICS region, transaction, and program
data report 111
creating an audit report 137
DB2 resource 114
Globally Writable Files 93
IP stack configuration 115
Maintenance 131
MQ regions 119
MQ resources 119

reports (*continued*)
printing 137, 140
resource-based 111
saving 137
security events 125
Sensitive Data 93
Sensitive Data Trustees 93
specifying input data 126
Started Task Protection 93
UNIX file system 121
resource access violations 130
Resource CICS panel 112
resource rules
tasks 27
view 58
Resource VTAM panel 117
results panel 137
rule lines 49
rule sets 48
rule-based compliance evaluation
overview 99
reporting 100, 102, 104, 105
RULELINE display panel 42
rules
ACF2 97
additional selection criteria 46
data set 27
resource 27
review guidelines 38
selection criteria 10
Rules Selection panel 40

S

sample scope records 5
save report 137
scope record 64
scoping 5
SE.B option 73
security controls 75
SELECT command 16
SELECT Logon ID display 7
selection criteria for IP stack report 115
Sensitive Data report 93
Sensitive Data Trustee report 93
SETUP - Collections 73
SETUP functions 69
SMF
data sources 125
specify data set 126
special privileges to list logon IDs 22
Started Task Protection report 93

T

TCP/IP configuration data 111
terminology v
training x
troubleshooting x

U

uid string 13, 21, 43
UID, last to store rule 39
UNIX file system 111
UNIX file system report 121

UNIX Selection panel 121
UNIX summary panel 121
user
concerns 85
events report 133

V

view
data set rules 27
Logon IDs 13
violation events report 128

W

write report to data set 139

X

X-RGP records 65

Z

zSecure Collect
memory requirements 145



Printed in USA

GI13-2325-02

