# IBM Security zSecure Audit STIG Service Stream Enhancement

*Documentation updates*

# IBM Security zSecure Audit STIG Service Stream Enhancement

*Documentation updates*

# Contents

# Chapter 1. About this document

This document lists the updates for the zSecure™ V2.2.0 documentation as a result of the IBM® Security zSecure Audit STIG Service Stream Enhancement (SSE). The updates apply to the following publications:

- *IBM Security zSecure Admin and Audit for RACF® User Reference Manual*, LC27-5639-02
- *IBM Security zSecure Audit for ACF2 User Reference Manual*, LC27-5640-02
- *IBM Security zSecure Audit for Top Secret User Reference Manual*, LC27-5641-02
- *IBM Security zSecure CARLa Command Reference*, LC27-6533-01
- *IBM Security zSecure Messages Guide*, SC27-5643-02

**Note:** Referenced topics that have not changed are not included in this document. You can find them in the publication that the chapter applies to.

# Chapter 2. zSecure User Reference Manuals

This chapter lists the updates for the *IBM Security zSecure User Reference Manuals* for RACF, ACF2, and Top Secret as a result of the zSecure Audit version 2.2.0 STIG SSE.

In the System Audit Guide chapter, the **Preparation** section for "AU.R Rule-based compliance evaluation" was changed.

**Note:** Customization members CLASSIFY, PCIAUTH, and PCIPAN are not valid for Top Secret.

## Preparation

To use the **AU.R** option, you must first 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 about creating the CKACUST data set.

zSecure supports controls that require the presence of configuration member CICPAUDT in the CKACUST data set. Rule-based compliance auditing (AU.R) might fail with a syntax error if this member does not exist. It might also be necessary to update this member to contain the proper list to ensure proper functioning of the compliance checks.

Run the job CKAZCUST to create all members that AU.R expects that do not yet exist. Running this job does not impact members that do already exist. The members that are created contain empty lists; CICPAUDT contains an empty list of CICS production regions.

End users can configure their own CKACUST. Therefore, it might be necessary to repeat this task with different targets.

The CKACUST data set specifies the following members with just a comment line:

*Table 1. Customization members in CKACUST for standard compliance checking*

| Customization Member | Description |
|---|---|
| APPDAUDT | Application Development Programmers. Users that maintain and develop application programs for the customer base. |
| APPSAUDT | Application Production Support Team members. |
| AUDTAUDT | Auditors, whether they are System, Security, or other. This can be any user that performs any type of auditing on the system. These users can be actual persons, batch users, or STC. |
| AUTOAUDT | Automated Operation STCs/Batch Jobs. STC or Batch users that perform any type of automated operations control on the system. |
| BMCCADMIN | INCONTROL Admins/Owners of CONTROL-D/M/O. |
| BMCUSER | INCONTROL Users of CONTROL-D/M/O. |
| C2AG@INS | Site rules to extend ACF2 STIG rule sets. |
| C2AP@INS | Site rules to extend ACF2 PCI-DSS rule sets. |

*Table 1. Customization members in CKACUST for standard compliance checking (continued)*

| Customization Member | Description |
|---|---|
| CHGOWNER | Users authorized to issue the `chown` command in UNIX. |
| CICBAUDT | CICS Batch Programs. |
| CICDAUDT | CICS Developers. |
| CICPAUDT | CICS production region jobnames. |
| CICSAUDT | CICS Started Task. |
| CICSDEF | CICS regions default user IDs (DFLTUSER). |
| CICUAUDT | CICS Utils (CONTROLO, BatIDs via CONTROLM, MAINVIEW). |
| CKAG@IDF | Site DEFTYPEs and DEFINEs for extra population or classification for STIG. |
| CKAG@INS | Site rules to extend RACF STIG rule sets. |
| CKAO@IDF | Site DEFTYPEs and DEFINEs for extra population or classification for GSD/iSec. |
| CKAO@INS | Site rules to extend GSD/iSec rule sets. |
| CKAP@IDF | Site DEFTYPEs and DEFINEs for extra population or classification for PCI-DSS. |
| CKAP@INS | Site rules to extend RACF PCI-DSS rule sets. |
| CKTG@INS | Site rules to extend TSS STIG rule sets. |
| CLASSIFY | Member for PCI-DSS resources classification.<br>Use this member to include SIMULATE statements with a PCI-PAN, PCI-AUTH, or PCI-PAN-clr SENSITIVITY.<br>For example:<br>`SIMULATE CLASS=DATASET SENSITIVITY=PCI-AUTH RESOURCE=SYS1.MACLIB` |
| CONSOLES | The System Console user IDs. |
| DABAAUDT | Data Base Administrators. Users that maintain and administer the databases and the database product software on the system. These users also perform backup and recovery of the databases. |
| DAEMAUDT | Unix Daemon user IDs. |
| DASBAUDT | DASD batch, jobs that perform DASD Backups, Migrate. Batch or STC users that perform DASD maintenance functions. |
| DASDAUDT | DASD Administrators. Users that administer DASD functions on the entire operating system. These users can perform a complete backup and recovery of the DASD farm. |
| DUMPAUDT | STCs/Batch IDs that perform dump processing. STC or Batch users that generate system level dumps. |
| EMERAUDT | Emergency TSO logon IDs. |
| FTPUSERS | FTP only user IDs. |
| LONGTIME | User IDs with extended CICS timeout. |
| MQCIAUDT | CICS regions running MQ applications. |
| MQDEADQ | Automated applications that are used for DLQ. |
| MQIDMOD | User IDs that can set identity and origin data for a message. |
| MQSAAUDT | MQ Series Administrators. Users that define and administer the IBM MQ for z/OS environment on the system. |

*Table 1. Customization members in CKACUST for standard compliance checking (continued)*

| Customization Member | Description |
|---|---|
| MQSDAUDT | Decentralized MQ Series Administrators. |
| OMVSAUDT | The OMVS started task kernel. |
| OPERAUDT | Operations personnel. Users that have direct access to the hardware components of the operating system. |
| PARMSTC | Users that have READ access justification via IAO. These users are STCs or batch jobs that obtain their configuration settings from the logical parmlib concatenation. |
| PCIAUTH | Users allowed to access resources containing payment card Sensitive Authentication data, such as full track data (magnetic-stripe data or equivalent on a chip), security codes, or PINs. (Only used by credit card providers/issuers.) |
| PCIPAN | Users allowed to access resources containing payment card Primary Account Numbers. |
| PCSPAUDT | Production control and scheduling personnel. Users that have domain level control of all scheduling of batch processes on the system. Not users that schedule specific application batch jobs. |
| PCIPANCL | Users and groups who have access to resources containing the clear text PAN (credit card Primary Account Number). |
| PRODAUDT | Production started tasks and batch logon IDs. |
| SECAAUDT | Security Administrators. Domain level security administrators; these users have total control over the administration of the ACP. |
| SECBAUDT | Security batch, jobs that perform ACP maintenance. Batch or STC users that perform security maintenance. |
| SECDAUDT | Decentralized security administrators. |
| SENSAPFU | Users and groups who are authorized to UPDATE APF data sets without generating an alert. |
| SENSMEMB | Specify UPDATE-sensitive members and the data sets they reside in. Filters are allowed. |
| SENSREAD | Users and groups for Alert who have access to site READ sensitive resources. |
| SENSRSRC | Member for `SIMULATE SENSITIVE` statements for site sensitive resources. |
| SENSUPDT | Users and groups for Alert who have access to site UPDATE sensitive resources. |
| SERVAUDT | Unix server user IDs. |
| SMFBAUDT | STC/BATCH IDs that perform SMF dump processing. |
| STCGAUDT | STC IDs that perform GTF processing. |
| SUPRAUDT | User IDs that require BPX.SUPERUSER. |
| SYSCAUDT | CICS Systems Programmers. |
| SYSPAUDT | Systems Programmers or Systems Administrators. Users that perform installation and maintenance on the operating system and vendor software. |
| TAPEAUDT | Tape Librarians, CA1 Prod Batch Jobs, and CA1 STCs. Users that perform control, initialization, and maintenance of a systems tape library. |
| TSTCAUDT | Trusted started tasks users. See list in TRUSTED STARTED TASKS in the z/OS STIG Addendum. |

*Table 1. Customization members in CKACUST for standard compliance checking (continued)*

| Customization Member | Description |
|---|---|
| WEBAAUDT | Web Server Administrators. |

The members should be populated with an ID in column 1-8. An asterisk in column 1 causes the line to be ignored (comment). The ID can be a user, a group, or a job name. Some standards imply that you must list user IDs or logon IDs here, but because it costs less maintenance to use group IDs instead, zSecure Audit supports both.

By default, the CKACUST data set specified in the zSecure configuration that is used to start the product is used. You can also specify a CKACUST data set in CO.1, which overrides the default. (Note: 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.

In the **CO.1** panel, you can specify action **E** to edit the data set, as shown in the following example.

```
  Menu   options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - Setup - Command file Row 24 from 1290
Command ===>                                                 Scroll ===> CSR

Select CARLa script library or work with a library (S, E, R, I, or D)

   CARLa script library                            Type      Status
E  'CRMASCH.MY.CKACUST'_____________________       CKACUST__ concatenated
****************************** Bottom of data ********************************
```

Placeholder members have been defined per standard to allow site customization to extend the rule sets with modified rules (with a slightly modified name) while suppressing the shipped rules with a SUPPRESS command. There are also three separate customization members (STIG, PCI-DSS, and GSD) to add DEFTYPEs for site-specific population members.

The C%%%@INS members are placeholders (templates) for site customization for addition of rules to the various standards, as implied by the 4-character member name prefix. Edit a copy of the C%%%@INS member in a site CKACUST data set. You can add new rule sets or extend existing rule sets (for example, to declare the set `N/A` for some specific reason), or replace a rule by adding a SUPPRESS for the standard RULE and add a new RULE with a slightly different name (the suggested suffix is `_site`) and add it to the existing rule set with the SET() keyword. The appropriate C%%%@IDF and C%%%@INS members for each standard category and standard are automatically included from the **AU.R** standard options.

# Chapter 3. zSecure CARLa Command Reference

This chapter lists the updates for the *IBM Security zSecure CARLa Command Reference* as a result of the zSecure Audit version 2.2.0 STIG SSE:

- CARLa command language chapter:

  SIMULATE: a sentence was added to the introduction.

  STANDARD: the syntax was changed and a new section was added: "Simulate sensitive resources".

- SELECT/LIST Fields chapter:

  NEWLIST TYPE=AS: the field description for SUBSYS_TYPE was changed.

  NEWLIST TYPE=ID: field descriptions were added for new fields ID_STC_SUBSYS_TYPE and STCPROC_NAME.

  NEWLIST TYPE=MOUNT: the field description was added for new field AUTOMOUNTED.

  NEWLIST TYPE=RESOURCE: a new table with sensitivity types and descriptions was added to the introduction.

## CARLa Command Language - SIMULATE

The following sentence was added to the introduction:

The SIMULATE command can be used as a stand alone command or within STANDARD or ENDSTANDARD.

## CARLa Command Language - STANDARD - Syntax

The STANDARD command syntax was changed:

```
STANDARD standardname
 [DESCRIPTION('description')]
 VERSION(version)
 [ESM({RACF|ACF2|TSS|NONE})]

DEFINE TYPE=type ...
/* optional DEFINE statements can be present */
...
INCLUDE ...
/* optional INCLUDE statements can be present */
...
DOMAIN domainname
   [OPTION(type(option ...) ...),]
          /* type must be same as on SELECT */
   SELECT(type[(selclause)] ... ),
          /* automatic object merge, max 1/type */
   [DESCRIPTION('desc'),]
   [SUMMARY(type(field ...))]
          /* type must be same as on SELECT */
...
RULE_SET set [DESCRIPTION(description)]
   [CAPTION(caption)]
   [SORTKEY(sortkey)]
   [SEVERITY({1 | 2 | 3 | HIGH | MEDIUM | LOW})]...
RULE rulename DOMAIN(name),
   [DESCRIPTION('desc'),]
   [SET(set)]
   [CAPTION(caption)]
```

```
   [SEVERITY({1 | 2 | 3 | HIGH | MEDIUM | LOW})]   [EXEMPT(type(selclause)) ]
          /* exempt types must be present in the DOMAIN SELECT */

   TEST testname
          type{=count | (fieldname reloper compliantvalue)}
          [DESCRIPTION(description)]
          [NONCOMPLIANT | N/A]
          [OTHERWISE(UNDECIDED | nested TEST ...)]
...
ENDRULE [rulename]

...     /* more RULEs, DOMAINs and DEFINEs */
/* Optional SUPPRESS and SIMULATE statements */
SUPPRESS STANDARD=name { RULE_SET=name | RULE=name } REASON='description'
SIMULATE CLASS=DATASET SENSITIVITY=sensitivity RESOURCE=creditcardsset

ENDSTANDARD [standardname]

/* Other optional statements */
SUPPRESS STANDARD=name RULE=name REASON='description'
SITE_SEVERITY severity STANDARD(standard)
   {RULE(set) | RULE_SET(set)}
SITE_SEVERITY severity  COMPLEX(complex)
```

## CARLa Command Language - STANDARD - Simulate sensitive resources

You can use the SIMULATE command within a STANDARD/ENDSTANDARD block to define sensitive data sets or resources, to test them in newlists SENSDSN, R_SENSITIVE, TRUSTED, RACF_ACCESS, and RESOURCE.

NEWLIST TYPE=RESOURCE is not automatically populated with all resources since that uses too much storage. But sensitive resources are included. Therefore, adding a SIMULATE SENSITIVE command will cause the resource to appear in TYPE=RESOURCE.

If a RULE, for example, must test security access on a certain data set that is not automatically considered sensitive, it might be required to define it as sensitive. To define a data set as sensitive, use SIMULATE SENSITIVE {READ,UPDATE} DATASET *datasetname*. Another way to define data sets and resources as sensitive is to use SIMULATE CLASS=*name* SENSITIVITY=*type* RESOURCE=*name*. Sensitivity types such as PCI-PAN and PCI-AUTH can be used to mark data sets or resources sensitive to the PCI-DSS standard. This is commonly done using the CLASSIFY CKACUST member. For more information about the SIMULATE statement, see SIMULATE.

## SELECT/LIST Fields - AS: Address space information

The field description for SUBSYS_TYPE was changed as follows:

**SUBSYS_TYPE**
The address space is a specific type of subsystem. (It might also be an MVS subsystem, but that is not the meaning here.) It can show the following values if the CKFREEZE file contains sufficient information:

*Table 2. SUBSYS_TYPE values*

| | |
|---|---|
| ABR | Innovation Data Processing: Automatic Backup and Restore. |
| ACCMON | zSecure Admin Access Monitor |
| APPC | Advanced Program to Program Communication. |
| ASCH | APPC Transaction Scheduler. |

*Table 2. SUBSYS_TYPE values (continued)*

| | |
|---|---|
| CICS | The address space is a Customer Information Control System region. |
| CSSMTP | Communications Server Simple Mail Transfer Protocol. |
| DB2 | The address space is a DB2 control region. |
| FTPD | The address space runs the FTP daemon process. |
| HEALTHCK | Health Checker. |
| HSM | DFSMS Hierarchical Storage Manager. |
| HTTPSERV | HTTP Server product. |
| ICSF | Integrated Cryptographic Service Facility. |
| IDMS | CA: Integrated Database Management System for z/OS |
| IMS | The address space is an Information Management System control region. |
| IPSTACK | Communications Server TCP/IP stack. |
| JES2 | The address space is a JES2 Job Entry Subsystem. It can be primary or secondary. This can be seen in the SUBSYS newlist. |
| JES3 | The address space is a JES3 Job Entry Subsystem. It can be primary or secondary. This can be seen in the SUBSYS newlist. |
| MIM | CA MIM Multi-Image Manager Resource Sharing. |
| MQ | The address space is an MQ Management Region (also known as QMGR). |
| MQCI | The address space is an MQ Channel Initiator Region. |
| MSTR | The master address space. |
| NETVIEW | NetView for z/OS address space. |
| NVAS | NetView Access Services address space. |
| RACF | The address space is the system's RACF address space (possibly running RACF Remote Sharing Facility, but that is not implied). |
| RMFGAT | RMF Monitor III Data Gatherer address space. |
| RMM | Removable Media Manager. |
| ROSCOE | CA Roscoe address space. |
| SDSF | System Display and Search Facility. |
| SMF | MVS System Management Facilities. |
| SYSREXX | System REXX (APF authorized REXX processor). |
| TCAS | TSO Control Address Space. |
| TLMS | CA TLMS Tape Management address space. |
| TN3270 | Telnet 3270 server region. |
| VTAM | The address space is the system's Virtual Telecommunications Access Method region. |
| ZALERT | zSecure Alert. |
| ZFS | ZFS UNIX File System or colony address space. |
| ZSECURE | zSecure server address space. |

## SELECT/LIST Fields - ID: User IDs and groups

The following field descriptions were added or changed:

**ID_STC_SUBSYS_TYPE**
Similar to ID_SUBSYS_TYPE, this repeated field returns the subsystem types running under a certain ID, but only those subsystems started with a started task procedure. Possible values for the fields are those as documented for the field SUBSYS_TYPE in AS: Address space information.

**STCPROC_NAME**
This repeated field returns the started task procedure names associated with the ID found in any actively running started task and the member names found in any procedure library in any subsystem in any system in the complex. The default length is 8 characters.

## SELECT/LIST Fields - MOUNT: UNIX Mount Points

The following field description was added:

**AUTOMOUNTED**
Flag field that indicates whether the automount facility manages the file system, that is, if the file system is mounted at the time it is accessed, and also unmounted later.

## SELECT/LIST Fields - RESOURCE

The following sensitivity types and descriptions table was added:

*Table 3. RESOURCE: Sensitivity types, classes, and descriptions*

| Sensitivity | CLASS | Meaning |
|---|---|---|
| MQ command | MQCMDS | IBM MQ for z/OS command security resource. |
| MQconn CHIN | MQCONN | IBM MQ for z/OS connection resource which applies to access by the channel initiator. |
| MQconn CICS | MQCONN | MQ connection resource which controls access from a CICS address space. |
| MQconn IMS | MQCONN | IBM MQ for z/OS connection resource which is checked for access from IMS control and application processing regions. |
| MQconn Job | MQCONN | IBM MQ for z/OS connection resource which controls access from batch jobs, TSO applications, DB2 stored procedures, and Unix System Services (USS). |
| MQcontext | MxADMIN | Grant access to the message context information for a specific queue. |
| MQreslevel | MxADMIN | Can bypass security checks in MQ. |

# Chapter 4. zSecure Messages Guide

This chapter provides the update for the *IBM Security zSecure Messages Guide* as a result of the IBM Security zSecure Audit STIG Service Stream Enhancement (SSE).

Message CKR1520 was added.

---

**CKR1520** **Buffer** *name* **too small for** *profile*

**Explanation:** The named buffer is used for line command processing. It is too small to contain one profile name.

**User response:** See the Electronic Support Web site for possible maintenance associated with this message.

If you cannot find applicable maintenance, follow the procedures described in Contacting IBM Software Support to report the problem.

**Severity:** 24

Printed in USA