IBM Security zSecure V2.4.0

Further Automation Of DISA STIG Resource Controls And Other Enhancements
IBM Security zSecure Messages Guide

IBM

Chapter 1. About this document

This document describes the documentation updates as a result of the Service Stream Enhancement (SSE; OA59004, OA59006). This SSE provides many new automatically determined sensitivity types.

The following DISA STIG RACF resource controls were automated:

Table 1. Further automated resource controls

Control	Description	Affected member
ZAIDR020	Protection of Compuware Abend-AID resources	CKAGAA20
ZCSLR020	Protection of Catalog Solution resources	CKAGCT20
ZCTDR020	Protection of BMC Contol-D resources	CKAGCD20
ZCTMR020	Protection of BMC Contol-M resources	CKAGCM20
ZCTOR020	Protection of BMC Contol-O resources	CKAGCO20
ZIOAR020	Protection of BMC INCONTROL IOA resources	CKAGOA20
ZISFR020	Protection of IBM System Display and Search Facility (SDSF) resources	CKAGSF20
ZMVZR020	Protection of BMC MainView resources	CKAGMV20
ZNETR020	Protection of IBM Z NetView resources	CKAGNV20
ZROSR020	Protection of CA Roscoe Interactive Environment resources	CKAGRS20
ZSMSR012	Protection of DFSMS program resources	CKAGSM12
ZVSSR020	Protection of Vanguard Security Solutions (VSS) resources	CKAGVS20

Note: Some of these resource controls require a SIMULATE SUBSYS command to be issued. For more information, see the following sections:

- *zSecure (Admin and) Audit User Reference Manuals*: section "Simulating an active subsystem".
- *zSecure CARLa Command Reference*, SUBSYS *security_options* in section "SIMULATE".

In addition, several other controls were also updated, corresponding with the following members:

Table 2. Updated controls	
Description	**Affected members**
Further automation	CKAGSM10 CKAGTM21
Support for non-default started task names in RACF and ACF2 controls that check configuration of started tasks of various products. To specify non-default started task names, use designated customization members. For more information about customization members, see Preparation for CKACUST members in the zSecure (Admin and) Audit User Reference Manual.	CKAGAA30 CKAGAA32 CKAGAD30 CKAGAD32 CKAGCD30 CKAGCD32 CKAGCM30 CKAGCM32 CKAGCO30 CKAGCO32 CKAGCS30 CKAGCS32 CKAGHC30 CKAGHC32 CKAGIC30 CKAGIC32 CKAGMI30 CKAGMI32 CKAGMT30 CKAGMT32 CKAGMV30 CKAGMV32 CKAGNC30 CKAGNC32 CKAGNV30 CKAGNV32 CKAGOA30 CKAGOA32 CKAGRS30 CKAGRS32 CKAGSF30 CKAGSF32 CKAGSS30 CKAGSS32 CKAGTM30 CKAGTM32 CKAGVA30 CKAGVA32 C2AGCD30 C2AGCM30 C2AGCO30 C2AGCS30 C2AGHC30 C2AGIC30 C2AGMI30 C2AGMT30 C2AGMV30 C2AGNC30 C2AGNV30 C2AGOA30 C2AGRS30 C2AGSF30 C2AGSS30 C2AGTM30 C2AGVA30

Table 2. Updated controls (continued)	
Support for DISA STIG version 6.43	CKAG@6 CKTG@6 C2AG@6 CKAGTM40 C2AGTM40
Minor updates	CKAGCT00 C2AGCT00 C2RGM060 C2RGTM60
Updated control imbed members	CKAIRZA0 CKAIRZN0 CKAIRZUI CKAIRZAI CKAIRZR2 CKAIRZRI C2RG@DEF C2RISYCT

Aside from the updated controls, the following enhancements were made for this zSecure V2.4.0 SSE:

- ACF2 access list processing has been revised to improve performance. This is most notable in the ACF2_SENSDSN_ACCESS report type, which is used in a fair number of ACF2 STIG data set controls. It also affects AS_DD, all DB2_* report types, and ACF2_SENSRESOURCE_ACCESS.
- The sensitive data sets reports now show more data set sensitivities; a few additional enhancements have also been made.
- Enhancements to the internal resource sensitivity knowledge bases result in more records being reported in report type RESOURCE. Even more additional records might be reported by TRUSTED processing, because of the recursive nature of this report type.
- More CA 1-specific settings are reported in the Tape protection reports.
- A WTO is issued with routing code 9 when real-time security event monitoring starts in CKQRADAR, at the time that message CKR0450 is written to SYSPRINT. The messages reporting on SMF cache processing have been improved and streamlined in connection with RESTART processing.
- New output format DEC$DIGITS enables printing decimal numbers with leading zeroes.
- Adjustable return code for CKR1322.
- Several enhancements to the DEBUG command for serviceability.

All the documentation updates apply to V2.4.0 zSecure Admin and Audit. The following publications are updated:

- *zSecure Admin and Audit for RACF User Reference Manual*
- *zSecure Audit for ACF2 User Reference Manual*
- *zSecure Audit for Top Secret User Reference Manual*
- *zSecure CARLa Command Reference*
- *zSecure Messages Guide*

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.
- The *zSecure (Admin and) Audit User Reference Manuals* and the *zSecure CARLa Command Reference* are available to licensed clients only. To access the zSecure V2.4.0 licensed documentation, you must sign in to the IBM Security zSecure Suite Library with your IBM ID and password. If you do not see the licensed documentation, your IBM ID is probably not yet registered. Send a mail to zDoc@nl.ibm.com to register your IBM ID.

Incompatibility warnings

BMC_MAINVIEW_STC removed
The BMC_MAINVIEW_STC variable in NEWLIST TYPE=REPORT_STC cannot be used anymore to specify which non-default BMC MainView started tasks are defined on a system. Instead, the CKAGMV30 and CKAGMV32 (for RACF), and C2AGMV30 (for ACF2) DISA STIG controls use the names of started tasks that are specified in a customization member; see Table 2 on page 1.

zSecure Audit for RACF and ACF2 automatically checks the following default BMC MainView started tasks:

BBIDLOG	MVALMGR	OSZ$EXEC
BBIILOG	MVCAS	OSZ$INIT
BBMCAS	MVLAS	OSZ$RTCS
BBMPAS	MVSPAS	OSZEXEC
MV$ALMGR	MV$CAS	OSZINIT
MV$LAS	MV$PAS	OSZRTCS
MVALARM	MV$MVS	

To specify further non-default BMC MainView started tasks, use the MVPROC customization member. For more information about customization members, see section "Preparation for CKACUST members" in the *zSecure (Admin and) Audit User Reference Manuals*.

Sensitivity types

DspSysCfg (with audit concern text "Can display system configuration information in SDSF") was changed to **SDSFAppInfo**:

Sensitivity	Priv_senstype	CLASS	Meaning
SDSFAppInfo		SDSF	In SDSF, can display regular operation information

For more information, see section "Predefined sensitivity types teared to newlists" in *zSecure CARLa Command Reference*.

Chapter 2. zSecure Messages Guide

The following messages were updated or added:

CKR0432 **Format *format* not supported for selection - field *field source***

Explanation

This message indicates that the indicated *field* was used for SELECT/EXCLUDE processing; the field can only be used for output in the current NEWLIST type. The NEWLIST types for which this error message may occur support the selection of strings, bitfields, and numbers. Some field types like time zones can only be used for output.

Severity

12

CKR0435 **Value *number* (decimal| hexadecimal) above maximum of *maximum***

Explanation:

Either a decimal or hexadecimal number was read that is too large to fit the field.

Severity

12

CKR0455 **SMFCACHE used *size* KB but had to skip *skipped-number* records and still had *cached-number* records cached for *number* out of *full-number* job tags**

Explanation

This message is printed to report statistics if the job tag system was turned on during SMF processing. It is suppressed when OPTION RESTART_INTERVAL is active, unless SMFCACHE VERBOSE is also in effect. The message prints the following values:

size
    The amount of memory that was used.

skipped-number
    The number of records that were skipped because the cache was full.

cached-number
    The number of records that were not completed after the last record was read.

number
    The number of incomplete job tags.

full-number
    The overall number of job tags.

The job tags persist across a RESTART; the cache does not. The records that were not completed and skipped were processed without RACF® information.

For more information, see section "SMFCACHE" in *zSecure CARLa Command Reference*.

Severity

00

CKR0456 **SMFCACHE incomplete job tag *job-tag* with *cached-num* records cached and *skipped-num* skipped**

Explanation:

This message is due to SMFCACHE VERBOSE. One of these messages is printed for each job tag that was incomplete at the end of SMF processing with any cached or skipped records during the last restart interval. It indicates the affected job, the amount of records that was cached at end-of-file, and the number of records that was skipped because the cache was full. (These records were processed without RACF information).

Severity

00

CKR1452 **Translation *translation1* overridden with *translation2 source***

Explanation

While parsing a LANGUAGE statement, more than one translation was found for the same string or value. The latest translation prevails. *source* is the location of *translation2*.

User response

Validate that the latest translation is what you want.

Severity

00

CKR1452 **Translation *translation* specified again *source***

Explanation:

While parsing a LANGUAGE statement, a translation that was already specified before was specified again at *source*.

Severity

00

CKR1322   Unsupported segment *segname* in complex *complex*

Explanation:
A new segment name was found in the RACF database templates that the current version of zSecure does not support. This typically happens when the RACF utility IRRMIN00 is run while relevant zSecure maintenance has not yet been applied. This message can be suppressed. The severity of this message can be set with OPTION MSGRC=(1322,*rc*).

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 Support to report the problem.

Severity

08 (unless changed by the MSGRC parameter of the OPTION statement)

CKR2062   SIM SUBSYS ROSCOE RESHLQ= must be equal to ROSID

Explanation:
In SIMULATE SUBSYS ROSCOE statements, the only allowed value of the RESHLQ parameter is ROSID. Refer to section "SIMULATE" in the *zSecure CARLa Command Reference* for a detailed description.

Severity

12

CKR2090   CA1 TMOSECxx result error - not found *string* in *ddname* system *system/version*

Explanation:
This suppressible message can be issued when an expected eye catcher string is not found in the in-storage CA 1 representation of the TMOSECxx member.

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 Support to report the problem.

Severity

16

CKR2091   SIMULATE CA1OPT PSWD=*Y-or-N* has overwritten actual PSWD=*Y-or-N* for system *system/version*

Explanation:
A SIMULATE CA1OPT PSWD= statement modified the CA 1 PSWD setting. If the CA 1 setting already matches what the SIMULATE command requests, this message is not issued.

Severity

00

CKR2094   Unexpected SMS MGMTCLAS name length *length* for *long-management-class-name* truncated to 8, system *system* [*version*] [- *generation*]

Explanation:
The CKFREEZE file DFSMS management class records contain an unexpected name length.

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 Support to report the problem.

Severity

08

CKR2095   Unexpected SMS STORCLAS name length *length* for *long-storage-class-name* truncated to 8, system *system* [*version*] [- *generation*]

Explanation:
The CKFREEZE file DFSMS storage class records contain an unexpected name length.

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 Support to report the problem.

Severity

08

CKR2096   Unexpected SMS storage group name length *length* for *long-storage-group-name* truncated to

8, system *system* **[***version***] [-***generation***]**

Explanation:
The CKFREEZE file DFSMS storage group records contain an unexpected name length.

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 Support to report the problem.

Severity

08

CKR2097   **Unexpected SMS volume definition length** *length* **for** *long-volume-serial* **truncated to 6, system** *system* **[***version***] [-***generation***]**

Explanation:
The CKFREEZE file DFSMS volume definition records contain an unexpected volume serial length.

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 Support to report the problem.

Severity

08

CKR2098   **Unexpected SMS storage group name length** *length* **for** *long-storage-group-name* **in VLD for** *volser* **truncated to 8, system** *system* **[***version***] [-** *generation***]**

Explanation:
The CKFREEZE file DFSMS volume definition contains an unexpected storage group name length.

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 Support to report the problem.

Severity

08

CKR2099   **Real time security event monitoring started**

Explanation:
This WTO message is issued with routing code 9 to help automated operations scripts keep track of the security event monitoring. This message is not present in the SYSPRINT but it is issued at the same time as the CKR0450 message in the SYSPRINT, when the monitoring task starts. It is not issued during the hourly RESTART; the SMF feed has no gap during a restart.

Severity

00

CKR2130   **Trigger format is nn+xx -** *token* **"***value***"** *source*

Explanation:
Specifying a trigger within a DEBUG TRIGGER(F(...)) clause must be done as *nn+xx* where *nn* (decimal) is an F-flag byte number and *xx* (hexadecimal) is a mask specification of bits to turn on within this byte.

Severity

12

CKR2233   **RETCONC: Audit concern contains variables, but none were found in the concern text**

Explanation:
This message flags an unsupported condition: an audit concern has associated variables, but they could not be substituted into the concern text. To understand the context, re-run the query with DEBUG NLS and examine the CKR1630 message right before this message.

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 Support to report the problem. Provide at least the associated information from the CKR1630 message referenced in the explanation.

Severity

08

CKR2487   **Duplicate SIM SUBSYS** *subsys-type* **before** *type* **"***value***" at** *ddname* **line** *number*

Explanation:
More than one SIMULATE SUBSYS *subsys-type* statement was detected for the same *subsys-type* subsystem. Only one set of options can be specified. The SYSPRINT file displays the CKR2487 message

directly after the duplicate SIMULATE command
specification.

Severity

12

IBM®