IBM Security zSecure V2.4.0
Service Stream Enhancement (SSE)

MQ auditing, Command Audit Trail, compliance automation, and other enhancements
IBM Security zSecure CARLa-Driven Components Installation And Deployment Guide

Chapter 1. About this document

This document describes the documentation updates as a result of the Service Stream Enhancement (SSE) for MQ auditing, Command Audit Trail, compliance automation, and other enhancements (APAR numbers OA59807, OA59823, OA59861, and OA59862).

The following enhancements were made for this zSecure V2.4.0 SSE:

- MQ auditing:
  - New report types:
    - MQ_AUTHINFO to report on MQ authentication information objects.
    - MQ_CHLAUTH to report on MQ channel authentication records.
  - The MQ_REGION reports show the following:
    - Authentication information object for user ID and password authentication.
    - Certificates that the queue manager and queue sharing group use.
    - Presence of various switch profiles.
  - The MQ_CHANNEL report type identifies the security exit and the user data that is passed to it, as well as the channel's certification label.
  - The disposition of inbound transmissions has been added to the MQ_INIT reports.
- STIG controls:
  - Automation of more STIG controls: 17 for RACF, 8 for ACF2, and 8 for Top Secret.
  - Equivalents of STIG controls RACF0570 and RACF0580 that allow for password phrases in addition to passwords are provided in the zSecure Extra standard.
  - General improvements for checking general access and logging requirements.
- Command Verifier:
  - Various enhancements have been made to the Command Audit Trail.
  - Multiple commands can now be specified in a pre-command or post-command policy profile.
- Selection on audit and global audit settings are added to the RA.D and RA.R menu options.
- Db2 102 IFCid 106 events (Security parameters at start-up/reload) are now sent to IBM QRadar SIEM and Micro Focus ArcSight.
- Performance improvements are made for ACF2 TRUSTED reporting.
- ICSF settings are added to the IPL parameters report.
- Automatic sensitivities are added, for example, for inaccessible LPA or linklist libraries.
- New fields FALLBACK_DATASET are added to the SENSDSN report type to identify secondary, duplex, or backup RACF data sets.

The documentation updates apply to zSecure V2.4.0. Each of the following links includes a PDF file with the updates for the subject publication: :

- *zSecure CARLa-Driven Components Installation and Deployment Guide*
- *zSecure Messages Guide*
- *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 Command Verifier User Guide*

Note:

- The revision bars in the margin indicate updates since publication of Further Automation Of DISA STIG Resource Controls And Other Enhancements (OA59004, OA59006) on April 11, 2020.
- Referenced or linked 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

STIG members renamed for controls AAMV0410 and AAMV0420

Table 1. SCKRCARL generic member names renamed for RACF, ACF2, and Top Secret systems

Original member name	Renamed - for RACF system	Renamed - for ACF2 systems	Renamed - for Top Secret systems
C2RGM410	CKAGM410	C2AGM410	CKTGM410
C2RGM420	CKAGM420	C2AGM420	CKTGM420

Multiline mixed SBCS/DBCS strings

With previous versions of CARLa and CKGRACF, within a string literal crossing a line boundary, if a line ended with a shift-in (SI) character and an optional space, and if the next line started with a shift-out (SO) character, the SI character, optional space, and SO character were trimmed away by the parser. This trimming behavior has been extended as follows.

Within a string literal crossing a line boundary, if a continuation line starts with an SO character, optionally preceded by Single-byte Character Set (SBCS) space characters, lines immediately preceding this line are trimmed away if they entirely consist of SBCS spaces. Trailing SBCS spaces in the line before these blank lines, if any, are trimmed away as well. If the trimmed line ends with an SI character and the continuation line starts with an SO character, these SI and SO characters are trimmed away, too.

Double-byte Character Set (DBCS) space characters are typically used for non-Roman character languages, like Japanese.

For more information, see "Syntax rules" in *zSecure CARLa Command Reference*.

Chapter 2. Data preparation for SIEM

The following section was updated:

Generating the SMF records

Db2® IFCid 106 was added to the following bullet:

- Selected subtypes of 102 that zSecure forwards to SIEM are Db2 IFCids 4, 5, 6, 7, 8, 9, 10, 22, 23, 24, 25, 55, 83, 87, 90, 92, 104, 105, 106, 107, 140, 141, 142, 143, 144, 145, 169, 177, 219, 220, 258, 270, 314, 319, 343, 361, 362, 370, 371, 373, and 404; see section "Procedure".

Security setup for zSecure

In section "Resources that configure which line commands are allowed", the overview-type/entity combinations were updated:

```
AD.F: ACF2_RULE
AI.I: ACF2_INFOLINE
AK.F: ACF2_RULELINE
AL.L: ACF2_LID
AR.I: ACF2_INFORULE
CL.$: RACF CLASS
CP.$: CICS_PROGRAM
CR.$: CICS_REGION
CS.$: CICS_TRANSACTION
DA.$: DB2_TABLESPACE
DB.$: DB2_BUFFERPOOL
DC.$: DB2_COLLECTION
DD.$: DB2_DATABASE
DE.$: DB2_VARIABLE
DG.$: DB2_STOGROUP
DH.$: DB2_SCHEMA
DJ.$: DB2_JAR
DK.$: DB2_PACKAGE
DN.$: DB2_PLAN
DO.$: DB2_ROUTINE
DQ.$: DB2_SEQUENCE
DR.$: DB2_REGION
DS.$: DSN
DT.$: DB2_TABLE
DY.$: DB2_DATATYPE
EF.$: RUN_DD
FL.$: FIELD
IC.$: SETROPTS_CLASS
MB.$: MEMBER
MC.$: IMS_REGION
MP.$: IMS_PSB
MQ.$: MQ_REGION
MT.$: IMS_TRANSACTION
QA.$: MQ_CHLAUTH
QC.$: MQ_CONNECT
QH.$: MQ_CHANNEL
QI.$: MQ_INIT
QN.$: MQ_NAMELIST
QO.$: MQ_AUTHINFO
QP.$: MQ_PROCESS
QQ.$: MQ_QUEUE
QT.$: MQ_TOPIC
R1.$: REPORT_AC1
RA.$: RACF_ACCESS
RA.C: RACF_ACCESS (Custom display)
RA.D: RACF_ACCESS (Data set profiles)
RA.G: RACF_ACCESS (Group information)
RA.R: RACF_ACCESS (Resources)
RA.U: RACF_ACCESS (User information)
RC.D: RACF (DATASET entities)
RC.G: RACF (GROUP entities)
RC.M: RACF (User ID summary)
RC.R: RACF (RESOURCE entities)
RC.U: RACF (USER entities)
RD.D: REPORT_NONDEFAULT
RN.D: REPORT_REDUNDANCY
RO.D: REPORT_OUTOFGROUP
RP.$: REPORT_PADS
RR.D: REPORT_PROFILE
RR.R: REPORT_PROFILE
RS.D: REPORT_SENSITIVE
SC.D: RACF REPORT_SCOPE (DATASET entities)
SC.R: RACF REPORT_SCOPE (RESOURCE entities)
SD.$: SENSDSN
SM.D: SMF (DATASET entities)
SM.G: SMF (GROUP entities)
SM.L: SMF (LOGONID entities)
SM.R: SMF (RESOURCE entities)
SM.U: SMF (USER entities)
SP.$: SPT
ST.$: REPORT_STC
TK.$: ICSF_TOKEN
TR.D: TRUSTED (data sets)
TR.R: TRUSTED (Resources)
TR.U: TRUSTED (Users)
UN.$: UNIX
ZA.B: Alert (Category selection)
ZA.C: Alert (Configuration selection)
ZA.D: Alert (Destinations)
ZA.R: Alert (Selection)
```