IBM Security zSecure V2.4.0

Enhancements for compliance automation and usability 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 zSecure enhancements for compliance automation and usability (for APAR numbers OA60419, OA60420, and OA60459 - December 2020).

The following enhancements were made:

- More control automation for RACF, and some for ACF2 and Top Secret.
- Upgrade to STIG Version 6 Release 47 (6.47).
- New library: SCKACUST
  In previous zSecure versions, following a PTF, customers had to run job CKAZCUST to create new CKACUST members in the customer's Site and User CKACUST data sets.
  Starting with this SSE, the new SCKACUST library is added to the concatenation for DDname CKACUST. New CKACUST members that are introduced in compliance controls are now automatically provided in SCKACUST. Following specification of the relevant zSecure configuration information, these new members are automatically copied from SCKACUST to the customer's Site or User CKACUST data sets.
- New library: SCKACUSV
  The CKACUST data set has records that are limited to 80 characters. The CKACUSV data set allows specifying longer values. The issuer name of a digital certificate is an example of a value that can be much longer. Your zSecure configuration (by default, C2R$PARM) must define which data set is to be used as the CKACUSV data set, or it must be set up manually through option Setup Command files (SE.8).
- Additional VM events for SIEM.
- Background run capabilities for RA.3.2, AM.8, and AM.9.
- Support for SMF relocate section 443 and ID token extensions.
- New report types:

  CERTIFICATE
  A record in the TYPE=CERTIFICATE report type describes a digital certificate as it is present on a particular system.

  IOAENV
  The IOAENV report type shows the security settings of active BMC INCONTROL IOA environments, and it includes information on the IOA, Control-D, Control-M, and Control-O products.

  IP_INETD
  The IP_INETD report type shows configuration of network services that the inetd daemon manages.

  JES_DEVICE
  The JES_DEVICE report shows the available JES2 devices and the information that is used to secure them.

  JES_REMOTE
  The JES_REMOTE report shows the available remote JES2 workstations, and the information that is used to secure them.

  SSH_DAEMON
  The SSH_DAEMON report shows the configuration of the z/OS OpenSSH SSH daemons that run in the UNIX address spaces in the system.

  SUPSESS_REGION_CP
  The SUPSESS_REGION_CP newlist type can be used to report about IBM CL/SuperSession. Each record in the TYPE=SUPSESS_REGION_CP report describes a Network Access Manager Control Point.

  For details, see the documentation updates for the *zSecure CARLa Command Reference*.

- New ACF2_SENSDSN_ACCESS fields link logonids with started task to better determine their authorization.
- Enhancements for parsing parameter members.
- zSecure Alert enhancements:
  - zSecure Alert provides an option to exploit a CKRCARLA internal restart to refresh environment information while retaining job information.
  - Batch jobs are now provided to ease upgrade, maintenance, test, and roll-out of zSecure Alert configuration changes.
- The ability to run CKXLOGID authorized.

The documentation updates apply to V2.4.0 zSecure Admin, zSecure Audit, and zSecure Alert. The following publications were updated:

- *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 Alert User Reference Manual*

The following product name and terminology changes were applied throughout the zSecure documentation:

- "CA Roscoe Interactive Environment" to "Advantage CA-Roscoe"
- "Tivoli NetView" to "Z NetView"
- "Whitelist" to "allowlist".

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.

Installation requirement

HOLD data in SMPE

APAR OA60419 is fixed by UJ04501, which includes a pre-installation job (in cover letter and ++HOLD(ACTION)). Change this job to meet your site's installation standards and then run it prior to installation.

Migration considerations

New SCKACUST and SCKACUSV libraries

- New SCKACUST and SCKACUSV libraries are distributed as part of the PTF package.
- CKACUST and CKACUSV data sets can be created through new job SCKRSAMP(CKAZSITE) for usage by a particular user. This new construction eliminates the need for maintaining Site (or customized) CKACUST instances through the CKAZCUST job for every PTF.
- For this update (only), a Site CKACUSV data set must be created and a reference to it must be added to the zSecure configuration (C2R$PARM).
- For a new installation, Site (or customized), CKACUST and CKACUSV data sets are created by using CKRZPOST; the zSecure configuration (C2R$PARM) includes provisions for both.

Chapter 2. *zSecure CARLA-Driven Components Installation and Deployment Guide*

Several sections were updated for SCKACUST and SCKACUSV libraries and “Alert / C2POLICE” on page 4.

The following sections were also updated:

- “TSO and ISPF command tables for zSecure Admin” on page 6
- Optional installation step for CKXLOGID

SCKACUST and SCKACUSV libraries

The following sections were updated:

- Section "About zSecure configuration data sets"
  The CKACUST description was updated and CKACUSV was added in table "zSecure configuration data sets".

Data set name	Description
*your.prefix.*CKRPARM	This data set contains the main configuration member C2R$PARM. You can create other configuration members as well. The CKRPARM data set also contains the REXX CKR (adapted to your naming convention). Copy and adapt this member to a SYSPROC or SYSEXEC data set. See "Making the software avaialble to TSO/ISPF users".
*your.prefix.*CKACUST	This data set contains the 'compliant authorized ID population' members used for option AU.R - Rule-based compliance evaluation. This option is only available for zSecure Audit. This dataset must be a fixed blocked 80 formatted PDS or PDSE. C2R$PARM must define which data set is to be used as the CKACUST data set, or it must be set up manually through zSecure option Setup Command files (SE.8).
*your.prefix.*CKACUSV	This data set contains the 'compliant authorized ID population' members used for option AU.R - Rule-based compliance evaluation. This option is only available for zSecure Audit. This dataset must be a variable blocked formatted PDS or PDSE. The advice is to use a logical record length of 32752. C2R$PARM must define which data set is to be used as the CKACUSV data set, or it must be set up manually through zSecure option Setup Command files (SE.8).

  The following sentence was removed:

  > The CKACUST data set is created and filled with job CKAZCUST available in the the CKRINST library or the SCKRSAMP library.

- Section "Customization of zSecure configuration data sets"
  The last bullet was updated:
  - For zSecure Audit users that use option AU.R - Rule-based compliance evaluation: Remove the comment from the SET CKACUST and SET CKACUSV parameters and update the data set name.
- Section "Creating zSecure configuration data sets"
  Step 7 (optional) was removed:

7. Optional: Only for zSecure Audit users that use option AU.R - Rule-based compliance evaluation. Update job CKAZCUST following the comments in the JCL and submit job to create the CKACUST library. For every new release, run the job CKAZCUST to create all members expected by AU.R that do not exist yet; the job will not touch members that already exist. The members created will contain empty lists.

- "Appendix D. Configuration parameters and members"
  The description for CKACUST was updated:

CKACUST and CKACUSV
These parameters specify the data set names of the "compliant authorized ID population" members for zSecure Audit option AU.R - Rule-based compliance evaluation. CKACUST specifies a fixed blocked data set and CKCUSV specifies a variable blocked data set. Users can concatenate their own CKACUST and CKACUSV libraries in front of the library that is specified in the configuration member, and in the zSecure product library with option CO.1 or SE.8. See the topic "CO.1 LIBRARIES - Data set selection" in the User Reference Manual for your zSecure product.

Alert / C2POLICE

The following sections were updated:

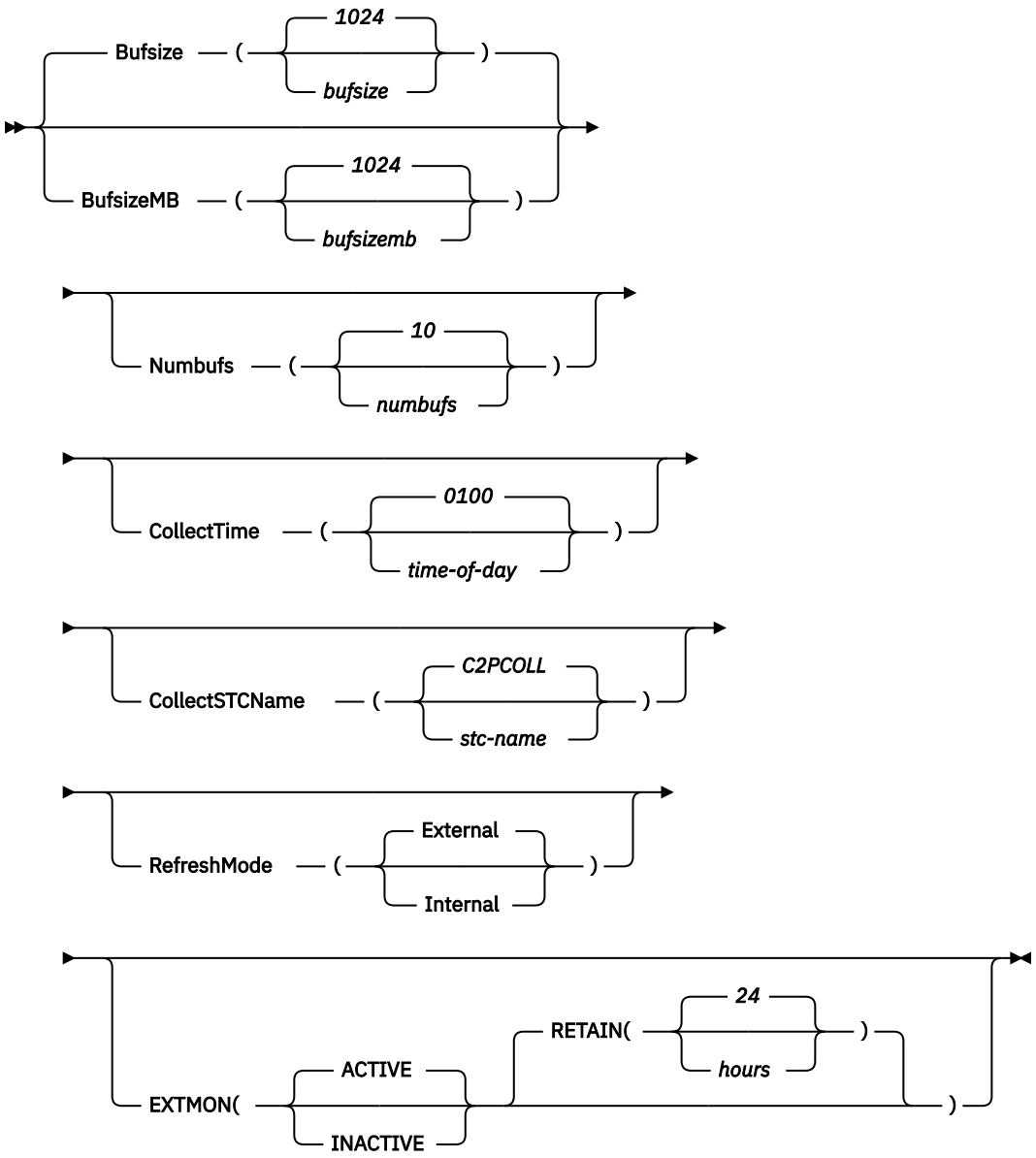
- In section "Intervals", the following paragraphs were updated:

The preprocessing subtask (also known as stage-1) obtains current information about the system environment and user attributes. This task is carried out hourly by default. If you require current information, you must process the security database and the CKFREEZE file more frequently. Processing the security database is relatively quick, but obtaining a new I/O configuration image is a costly process. zSecure Collect is typically scheduled to run once a day at a particular time to refresh the full CKFREEZE file. However, it is also possible to have zSecure Alert dispatch this task by using the operator command MODIFY C2POLICE,COLLECT. At the preprocessing interval, zSecure Alert can also create a small CKFREEZE snapshot of a subset of the system environment. This small CKFREEZE snapshot is taken and processed only if extended monitoring is active. The small CKFREEZE is not intended for any other process.

As part of SMF processing, the CKRCARLA program retains certain SMF data to complete other SMF records that lack this data. An example of such SMF data is the user ID for SMF record type 15. By default, the refresh of the environment information involves stopping and starting the CKRCARLA subtask. As a result, the retained information is lost, and must be re-established. This often results in the fields being reported as "missing". It is possible to retain the information for a longer period through specification of the REFRESHMODE(INTERNAL) option (see “RefreshMode” on page 5). The necessary SMF information will be retained until the C2POLICE started task is restarted or stopped.

- In section "OPTION command", the syntax was updated and a description was added:

Option



RefreshMode

Specifies whether the environment refresh involves a complete stop and start of the CKRCARLA subtask, or whether it exploits the CKRCARLA internal restart function. During an external refresh (default), the CKRCARLA subtask is stopped and the SMF job information is lost. The internal restart mode has the advantage that SMF job information, that is retained to complete other SMF records, is kept for a longer period. Information that is lacking in certain SMF records (for example, the user ID in record type 15) is saved from previous SMF records; this information is available in the applicable CARLa fields.

The saved job information is kept until the C2POLICE started task itself is restarted or stopped. The amount of retained data can be significant if the started task is kept running for long periods. You must ensure that sufficient storage above the 2GB boundary is available. The example C2POLICE started task procedure in SCKRPROC specifies MEMLIMIT=8G. One gigabyte of storage is sufficient to retain information for approximately 8 million jobs.

"TSO and ISPF command tables for zSecure Admin"

The following paragraph was added:

If you wish to run CKGRACF from outside the zSecure ISPF environment, the program must be available from either LINKLIST, STEPLIB, or JOBLIB (just like any other authorized program). Using STEPLIB or JOBLIB ha a performance penalty and this method works only when all data sets in your STEPLIB or JOBLIB concatenation are APF-authorized.

"Setup of zSecure Admin Command Logger"

Step 11 (optional) was added:

11. Optional: Enable calling CKXLOGID from APF environment. The CKXLOGID command is a regular TSO command that does not need APF authorization. However, if it is invoked from inside an APF-authorized program, additional definitions are required. If you plan to create your own APF-authorized program that calls CKXLOGID through the TSO service route IKJEFTSR, then you must add CKXLOGID to the list of APF-authorized commands (AUTHCMD) in the active TSO parmlib member (IKJTSOnn). If you do not plan to write such a program, no further action is required, and you can skip this step.