IBM Security zSecure V2.3.0 Service Stream Enhancement

Enhancements for data encryption and SIEM feeds Documentation Updates zSecure Messages Guide

IBM Security zSecure V2.3.0 Service Stream Enhancement

Enhancements for data encryption and SIEM feeds Documentation Updates zSecure Messages Guide

Chapter 1. *IBM Security zSecure Messages Guide*

This document lists the documentation updates for the *zSecure Messages Guide* as a result of the V2.3.0 SSE for Enhancements for data encryption and SIEM feeds.

The following messages were changed or added:

- CKF messages
- Chapter 3, "CKQ messages," on page 5
- CKR messages
- C2P messages

Chapter 2. CKF messages

The following CKF messages were added or updated:

CKF080I **Unexpected IXCQUERY** *function* **return code** *rc* **reason code** *rr* **(hexadecimal)**

Explanation: The IXCQUERY service issued an unexpected return code. The *function* indicates the type of information that was requested. The corresponding XCF record is missing from the file.

Severity: 00

CKF081I **CF** *data* **not retrieved. No CFRM data set or no policy active**

Explanation: Information from the active CFRM policy could not be retrieved, because the couple data set supporting TYPE(CFRM) is not accessible to this system or no policy has been activated. The value data can be either `information` or `structures`.

Severity: 04

CKF182I **Options for this run are: FOCUS=(***focus***) IO=***Y/N***,TCPIP=***Y/N***, DASD=***Y/N***, TAPE=***Y/N***, SWCH=***Y/N***, PATH=***Y/N***, VTOC=***Y/N***, VVDS=***Y/N***, PDS=***Y/N***, CAT=***Y/N/MCAT***, MCD=***Y/N***, BCD=***Y/N***, DMS=***Y/N***, ABR=***Y/N***, TMC=***Y/N***, RMM=***Y/N***, VMF=***Y/N***, UNIX=***Y/N*** [,UNIXCLIENT=***Y/N***] RECALL=***Y/N*** [,AUTOMOUNT=***Y/N***, UNIXACL=***Y/N***], SHARED=***Y/N***, OFFLINE=***Y/N***, SMS=***Y/N***, STATS=***Y/N***, IDR=***Y/N***, CHECK=***Y/N***, SCAN=***Y/N***, PARALLEL=***NONE/PATHGROUP/PATH*** [,NO]REPORT[,ALLRECS] [,WAIT=***Y/N***[,BURSTS=***num***, BURSTWAIT=***num***,BURSTSIZE=***num***]] [,[NO]KEY0, [NO]BYPASS, [NO]SIO, [NO]XMEM, [NO]XMDSN, [NO]DIAG, [NO]UID0[,UNCONNECTED] [,SLOWDOWN] [,FREE] [,MONITOR=***num***] [,INTERVAL=***num***]], ENQ=***Y/N***, DDLIMIT=***num***, IOTIMEOUT=***nn***, PDSEBUFSIZE=***num***, SIGVER=***Y/N***, XTIOT=***Y/N***, MOD=***Y/N***, NJE=***Y/N***, CICS=***Y/N***, IMS=***Y/N***, MQ=***Y/N***, DB2=***Y/N***, DB2CAT=***Y/N***, [NO]DB2ADM, CKDS=***Y/N***, PKDS=***Y/N***, TKDS=***Y/N***, SYMKEYTEST=***Y/N***,CF=***Y/N***, SERIALIZATION(NOENQ|ENQ(SYSDSN/CKRDSN/SYSDSN,CKRDSN)[,WAIT[,MAXWAIT(***nn***)]|,FAIL][,VOLSER][,UNIT])**

Explanation: This message lists the basic options (options that are not a combination of others) that are currently in effect.

Severity: 00

CKF218I **Number of Coupling Facilities queried:** *nn*, **Structures:** *nn*, **Function DSNs:** *nn*

Explanation: This is an informational message that shows the total number of Coupling Facilities that were processed and the total number of structures and coupling data sets that were found.

Severity: 00

CKF373I **BPX1PCT FSINFO failed. RC=***nn*, **reason=***nn*

Explanation: The values of the `COMPRESSED`, `COMPRESS_STATE`, `ENCRYPTED`, and `ENCRYPT_STATE` fields are missing as the result of an error during the execution of the BPX1PCT "FSINFO" function. This function determines the compression/encryption state of a zFS aggregate.

User response: See the return and reason codes to resolve the issue:

- RC=*nn* is the return code qualifier.
- reason=*nn* is the reason code as described in *UNIX System Services Messages and Codes*.

Severity: 04

CKF374I **BPX1PCT query failed. RC=***nn*, **reason=***nn*

Explanation: This message indicates that an error occurred during the execution of the BPX1PCT function. This function is used to determine some of the zFS information. The reason code given consists of two half words. The first is the reason code qualifier. The second is the reason code as described in the *UNIX System Services Messages and Codes manual*. As result, the values of the `ZFS_SMF`, `ZFS_SMF_INTERVAL`, `ZFS_FORMAT_COMPRESSION`, `ZFS_FORMAT_ENCRYPTION`, and `ZFS_FORMAT_PERMS` fields (TYPE=SYSTEM or MOUNT) are missing.

User response: See the return and reason codes to resolve the issue:

- RC=*nn* is the return code qualifier.

- reason=*nn* is the reason code as described in *UNIX System Services Messages and Codes*.

Severity: 04

CKF522I **Error collecting data on common storage blocks:** *message*

Explanation: An error occurred during collection of records describing common storage blocks. The *message* field shows the encountered inconsistency. Depending on the severity of the problem, either individual or all common storage blocks are unavailable for further analysis. This is indicated by the message severity, equal to 4 or 20, respectively.

Severity: 4 or 20

CKF523I **Copied information on** *decnum* **common storage blocks and on** *decnum* **of its owners**

Explanation: This informational message shows the number of records that describe common storage blocks that were copied to the CKFREEZE file. It also shows the number of collected records that contain owners of the common memory blocks.

Severity: 00

Chapter 3. CKQ messages

Use the CKQ-prefixed messages to respond to issues associated with the zSecure™ CKQEXSMF program.

The CKQ messages are issued by the CKQEXSMF program running in the zSecure SMF Collector address space. The message identifier uses the format CKQ*nnnnX*, where *X* indicates the severity of the message. The CKQEXSMF program uses the following severity level codes:

I Informational message.

W Warning message: the task continues, but an error occurred.

E Error message: the task might either end immediately or attempt to continue.

S Severe error message.

A Action message: operator action is needed to correct the situation.

The CKQ messages are identical to the C2P messages, with the exceptions as documented in this chapter. If the message does not occur in the list of messages using the CKQ prefix, check C2P messages, replacing the CKQ prefix with a C2P prefix. The C2P messages are issued by both the zSecure Alert address space and the zSecure Admin Access Monitor address space.

Messages from 0 to 999

CKQ0100A zSecure SMF Collector not active

Explanation: The zSecure SMF Collector stopped.

User response: If CKQ messages preceding this message indicate problems, solve them, then restart.

CKQ0352E Version mismatch, exit

Explanation: This error message is returned to the caller of the CKQIO2PC when the version indicator in the C2PC communication area is not correct.

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.

CKQ0353E Unknown DDname

Explanation: This error message is returned to the caller of the CKQIO2PC module in case an attempt is made to open a file that is not one of the supported types. The file type must be represented in characters five to seven of the DDname.

User response: Ensure that the DDnames reflect supported file types only.

CKQ0356E Invalid function code

Explanation: This error message is returned to the caller of the C2PIORTN module when an invalid function code is provided via the invocation parameters.

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.

CKQ0361I Open of *ddname* for type *newlist-type*

Explanation: This diagnostic trace message is written because of DEBUG IO.

CKQ0362I Close of *ddname*

Explanation: This diagnostic trace message is written because of DEBUG IO.

CKQ0363I Get record for *ddname*

Explanation: This diagnostic trace message is written because of DEBUG IO.

CKQ0375I *hexdata*

Explanation: This diagnostic message shows the first 16 bytes of the current SMF or WTO record in hexadecimal format.

CKQ0550E No buffer yet, exit

Explanation: The CKQIOPC routine was called to retrieve a record before any in-storage buffer was created.

User response: Restart the CKQRADAR started task. If the operation fails again, 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.

CKQ0551I Task NT not found

Explanation: This is the first time that the client started task contacted the CKQEXSMF started task. A named token recording the status of the client was not found. This diagnostic message is only issued when DEBUG IO is active.

CKQ0552E Error return from IEANTCR, RC=*nnnn*

Explanation: The named token that is used to record the status of the client could not be created. Processing continues without saving the client status.

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.

CKQ0553I Buffer switched *ddname* **reached end of current**

Explanation: The active buffer for collecting SMF records was switched and the program reading the records reached the end of that buffer. This message is followed by message CKQ0554I. This diagnostic message is only issued when DEBUG IO is active.

CKQ0554I Next buffer *index*

Explanation: The active buffer for collecting SMF records was switched and the program starts reading records from the indicated buffer. This diagnostic message is only issued when DEBUG IO is active.

CKQ0551I Task NT not found

Explanation: This is the first time that the client started task contacted the CKQEXSMF started task. A named token recording the status of the client was not found. This diagnostic message is only issued when DEBUG IO is active.

CKQ0556E File not open, exit

Explanation: The CKQIO2PC routine received a request to retrieve a record from a file, but the file was not currently open.

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.

CKQ0557E SMF collector not active, exit

Explanation: The CKQIO2PC routine was called, but the zSecure SMF Collector task was not found in the system. Data transfer is not possible.

User response: Start the zSecure SMF Collector started task (CKQEXSMF) and retry the operation. If it fails again, 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.

CKQ0558I First call this task

Explanation: The current instance of the client program did not invoke the CKQIO2PC routine before. Necessary control blocks are obtained and initialized. This diagnostic message is only issued when DEBUG IO is active.

CKQ0559I Cursor determined by PC: Idx=*xx* **Csr=***nnnnnnnn*

Explanation: This diagnostic message is issued only when DEBUG IO is active. It indicates the starting point for retrieving records, based on the saved status for the client task.

CKQ0560I Default cursor used: Idx=*xx* **Csr=***nnnnnnnn*

Explanation: This diagnostic message is issued only when DEBUG IO is active. It indicates that the CKQIOPC routine could not determine the starting point for retrieving records. The CKQIO2PC routine determined a default location.

CKQ0561I Open buffer *nn*

Explanation: This diagnostic message is issued only when DEBUG IO is active. It indicates that the CKQIO2PC routine received a request to open a data stream. As a result, the indicated in-storage buffer was accessed.

CKQ0562I *ddname* **Processing STOP**

Explanation: The CKQIO2PC routine detected that the zSecure SMF Collector program was stopped on console operator request. The CKQIO2PC routine notifies the client program that no more records are available.

CKQ0563I no record found

Explanation: This diagnostic message is issued only when DEBUG IO is active. The CKQIOPC routine could not locate a new record to be passed to the client program. Execution continues.

CKQ0564I Locate resume point

Explanation: The CKQIOPC routine starts to locate the last record that was passed to a previous instance of the client program. The record following this last record is the first record to be passed to the current instance of the client program. This diagnostic message is only issued when DEBUG IO is active.

CKQ0565W Cannot locate resume point

Explanation: The CKQIOPC routine could not find any record that matches the last record that was passed to a previous instance of the client program. The CKQIOPC routine returns only records that are created after the current timestamp.

CKQ0566I Scan next buffer *nn*

Explanation: During the process to locate the resume point, the end of the current buffer was reached. The CKQIOPC routine continues the process with the buffer that is identified in the message. This diagnostic message is only issued when DEBUG IO is active.

Chapter 4. CKR messages

The following CKR messages were added or updated:

CKR0852 **RESTART interval end detected at** *timestamp* **during** *ddname* **input wait at record** *number*

Explanation: The end of a restart interval is reached. This can be later than expected if the program was waiting in a blocking call while the interval expired.

Severity: 00

CKR0853 **GETPROC** *procname* **OPEN (call type** *type* **) on** *ddname* **return code** *rc*,

Explanation: The OPEN of a GETPROC routine fails and no other message was issued wIth CKR0929.

Severity: 00

CKR0854 **GETPROC** *procname* **OPEN (call type** *type* **) on** *ddname* **return code** *rc* **- recovery attempt in progress**

Explanation: This message is issued after a CKR0929 message if the GETPROC procedure requested a retry by CLOSE/OPEN and the CLOSE and OPEN were successful. The next part of the recovery attempt is a GET request. If that fails, CKR0855 is issued.

Severity: 00

CKR0855 **GETPROC** *procname* **GET (call type** *type* **) on** *ddname* **return code** *rc* **- recovery failed**

Explanation: This message is issued after a CKR0929 message if the GETPROC procedure requested a retry, and the CLOSE and OPEN were successful, but the next GET failed again. zSecure concludes that recovery failed.

Severity: 16

CKR0913 **Serialization WAIT stopped by ATTN interrupt**

Explanation: The program attempted to obtain ENQs on all requested resources, but not all resources were immediately available. While waiting for the resources to become available, the terminal user pressed the attention key. The program stops waiting and terminates.

User response: Look for a preceding CKR0911 message to identify the unavailable resources.

Severity: 16

CKR1460 **BPX1PCT query failed. RC=***nn*, **reason=***nn*

Explanation: The values of the `ZFS_SMF`, `ZFS_SMF_INTERVAL`, `ZFS_FORMAT_COMPRESSION`, `ZFS_FORMAT_ENCRYPTION`, and `ZFS_FORMAT_PERMS` fields (TYPE=SYSTEM or MOUNT) are missing as the result of an error during the execution of the BPX1PCT function. This function determines the zFS default compression, encryption and permission format, and SMF recording settings.

User response: See the return and reason codes to resolve the issue:

- RC=*nn* is the return code qualifier.
- reason=*nn* is the reason code as described in *UNIX System Services Messages and Codes*.

Severity: 04

CKR2000 **Error loading GQE/XCOM related record** *num* **system** *system* **[***version***] of** *source: message*

Explanation: An error occurred during loading of records that describe common storage blocks. An unexpected record containing GQE/XCOM-related data was found in the CKFREEZE. This message is usually a result of a corruption in the indicated record. *message* shows the encountered inconsistency. Depending on the severity of the problem, either individual or all GQE/XCOM records are unavailable for further analysis and reporting. This is indicated by the message severity, equal to 4 or 20, respectively.

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: 4 or 20

CKR2001 **CKFREEZE appears to be truncated, system** *system* **[***version***] [- generation] file** *ddname source*

Explanation: Records that were expected at the end of a CKFREEZE file were not found. This suggests that either the CKFCOLL run abended, for example, on a B37 abend, or the CKFREEZE file was truncated during transport.

User response: Make sure the CKFCOLL run did not abend (for example, because the allocation for the

CKFREEZE was insufficient) and that the file or data set was not truncated during transport.

Severity: 16

CKR2269 **SMF records skipped due to INMEM** *rname* **wraparound, increase RESSIZMAX or prio**

Explanation: The message indicates that the SMF INMEM real-time interface experienced a buffer wrap-around before all the SMF records could be passed. To keep up with log records, the dispatching priority of SMF, the consumer job (for example, CKQRADAR), and the TCPIP stack must all be higher compared to the dispatching priority of the tasks that write many SMF records, or spare processor capacity must be available.

Severity: 8

CKR3033 **RESTART iteration** *number* **requesting next iteration**
Pass *source* **at record** *number*

Explanation: The end of a restart interval is reached or an immediate restart command was requested. This can be later than expected if the program was waiting in a blocking call while the interval expired. See message CKR0852 for the date and time that the interval expiry was detected.

The message is followed by one line per input file that will be kept open across the restart.

Severity: 00

CKR3037 **Continue input from** *source* **after record** *number*

Explanation: This message is issued after a restart to identify open files that were found during a restart. The program resumes reading where the previous iteration left off.

Severity: 00

CKR3084 **Current MASKTYPE=ACF2 at** *source1* **conflicts with earlier MASKTYPE=EGN at** *source2* **for** *pattern*

Explanation: There is a conflict in mask type between two SIMULATE commands for a single data set name pattern *pattern*, in response to the SENSITIVE keyword on the latter SIMULATE command. The program can only use one mask type per data set name pattern.

Severity: 12

CKR3085 **Current MASKTYPE=EGN at** *source1* **conflicts with earlier MASKTYPE=ACF2 at** *source2* **for** *pattern*

Explanation: There is a conflict in mask type between two SIMULATE commands for a single data set name pattern *pattern*, in response to the SENSITIVE keyword on the latter SIMULATE command. The program can only use one mask type per data set name pattern.

Severity: 12

CKR3086 **Current MASKTYPE=ACF2 at** *source1* **conflicts with earlier MASKTYPE=EGN at** *source2* **for** *pattern*

Explanation: There is a conflict in mask type between two SIMULATE commands for a single data set name pattern *pattern*, in response to the CLASS=DATASET keyword on the latter SIMULATE command. The program can only use one mask type per data set name pattern.

Severity: 12

CKR3087 **Current MASKTYPE=EGN at** *source1* **conflicts with earlier MASKTYPE=ACF2 at** *source2* **for** *pattern*

Explanation: There is a conflict in mask type between two SIMULATE commands for a single data set name pattern *pattern*, in response to the CLASS=DATASET keyword on the latter SIMULATE command. The program can only use one mask type per data set name pattern.

Severity: 12

CKR3088 **Resource name length** *len* **exceeds maximum of 44 for class DATASET** *source*

Explanation: The maximum length of a data set name is 44 characters.

User response: Check for a typing mistake in the data set name or make the generic specification shorter.

Severity: 12

CKR3089 **Mask specification must have a non-generic prefix of at least 3 characters** *source* **for** *dsnmask*

Explanation: Generic resource name specification on the SIMULATE command must start with at least three (3) non-generic characters.

User response: Change the mask specification.

Severity: 12

Chapter 5. C2P messages

The following C2P messages were added or updated:

C2P0234I Access Monitor captures requests for a user's own resources

Explanation: This message indicates that requests for a user's own resources are captured in the Access Monitor events. Use of this option can significantly increase the amount of collected information.

C2P0235I Access Monitor ignores requests for a user's own resources

Explanation: This message indicates that requests for a user's own resources are not captured in the Access Monitor events. This is the default status if the INCLUDEOWNRESOURCE keyword is not specified.

C2P0236I Access Monitor captures requests for a user's own resources

Explanation: This message is part of the response to the console operator DISPLAY command. At the moment of the DISPLAY command, the zSecure Access Monitor captures records for each request for a user's own resources, like a private data set or a job running with the user's user ID.

C2P0308E Crashing without ESTAEX

Explanation: This message indicates that the CRSH command is processing.

C2P0436I Extended Monitoring is *status*.

Explanation: This message is issued in response to the operator `DISPLAY` command to indicate that extended monitoring is active or not. *status* can have one of the following values:

`active` CKFREEZE snapshot data sets are created and analyzed for Alert situations.

`not active`
CKFREEZE snapshot data sets are not created and no extended monitoring alerts are issued.

`delayed`
Extended monitoring alerts are not issued until the temporary error condition has been resolved.

C2P0439W Insufficient snapshot data sets. Extended monitoring is delayed.

Explanation: This warning message is issued if less than two extended monitoring snapshot data sets exist. Since extended monitoring is based on a comparison of two data sets, extended monitoring is not possible. As part of normal processing, additional extended monitoring snapshot data sets are created, and extended monitoring analysis and alert creation will be resumed. This message is issued at the beginning of each extended monitoring interval start as long as the situation exists.

C2P0542I Debug BUFFER DETAIL mode

Explanation: This debug-only message is issued to indicate that statistics about the SMF records in the in-memory buffers are displayed at the end of each interval.

C2P0543I Debug BUFFER NODETAIL mode

Explanation: This debug-only message is issued to indicate that statistics about the SMF records in the in-memory buffers are not displayed.

C2P0544I Rectype Subtype Count

Explanation: This message has two types of content. The first row shows the header for the tabular display that follows. Subsequent rows show occurrences of the SMF record types (Rectype) and subtypes in the current in-memory buffer:

C2P0544I	**Rectype**	**Subtype**	**Count**
C2P0544I	*rectype*	*subtype*	*count*
C2P0544I	*rectype*	*subtype*	*count*

For RACF systems, the Subtype columns for the RACF records lists the numerical value of the RACF event code. For ACF2 systems, the Subtype columns lists the numerical value of the ACF2 record subtype.
The message format that includes the text "total" in the Subtype column shows the total number of record type records for the subtypes that follow. Those subsequent records do not include a value for the record type to indicate that they provide information for the subtypes for the previous record type.

Printed in USA