IBM Security zSecure V2.4.0
APAR OA58509

TCP Networking
Documentation updates

Chapter 1. About this document

This document describes the documentation updates as a result of APAR number OA58509.

The following publications were updated as result of this APAR:

- Chapter 2, “zSecure (Admin and) Audit User Reference Manual,” on page 3
- Chapter 3, “zSecure CARLa Command Reference,” on page 5
- Chapter 4, “zSecure Alert User Reference Manual,” on page 7
- Chapter 5, “zSecure Messages Guide,” on page 9

Note:

- The revision bars in the margin indicate updates since publication of MQ auditing, Command Audit Trail, compliance automation, and other enhancements (OA59807, OA59823, OA59861, OA59862) on July 15, 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 CARLa Command Reference* is 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.

Chapter 2. zSecure (Admin and) Audit User Reference Manual

Chapter. Calling zSecure, section "Supported file definitions for CKRCARLA"
The following file definition was updated:

C2RSYSLG
File that receives the redirected output from the UNIX syslog when the OPTION SYSLOGTOFILE setting is specified, or when a syslog message could not be delivered to any destination (neither primary, nor alternate). To support the line length for writing syslog messages as specified in RFC5424, specify the following values for the record format and line length: `RECFM=VB`, `LRECL=2052`. If the DD name is not allocated, SUPPRESS SYSLOG_FALLBACK_FILE is automatically set.

Chapter 3. zSecure CARLa Command Reference

OPTION statement
The following keywords and parameters were added:

ACTIVITY_REPORT_INTERVAL=*minutes*
This option can be used to request a message "CKR2103 Activity report interval ended at ..." with a timestamp, issued with the indicated frequency. The message shows local time of day and CPU time spent in the interval. It is followed by continuation lines that list input records that are processed (SMF or ACCESS) and output to TCP syslog, UDP syslog, and SNMP ports, as well as alert WTOs and remedial commands that are issued in the interval. By default, this option is not set. For CKQRADAR, this option is set in CARLa specification member CKQSPECL (see SCKRCARL for default). For CKQCEF, this option is set in CARLa specification member CKQCEFP (see SCKRSAMP for sample).

DESTINATION *destid* PRIMARY=*ipv4v6* ALTERNATE=*ipv4v6*
This statement allows specification of a fall-back address for TCP traffic. If the TCP connection is broken and cannot be recovered by re-allocating the socket, resolving the address, and connecting, then it is sent to the alternate address as soon as the primary destination's buffer is full of syslog records. The *destid* can be used instead of an *ipv4v6* specification in the SYSLOGTCP parameter. The destination ID *destid* is case sensitive.

Using a target IP address and port as both a primary and alternate destination is not supported. Specifying an IP address and optional port on a SYSLOGTCP printoption parameter counts as a primary destination.

SYSLOGTCP=*destination*[*:port*]
SYSLOGTCP=(*destination*[*:port*],destination[*:port*], ...)
If the SYSLOGTCP= specification precedes the first NEWLIST statement or if it is specified on a NEWLIST statement that specifies the SYSLOG option, it determines the output destination for TCP SYSLOG traps.

The destination can be a name from a DNS or IP address lookup, or a destination ID that is defined by a prior DESTINATION statement. The default port is 514. For more information, see the SNMPTO= parameter description. Note that DESTINATION IDs are case sensitive.

For more information about syslog destination alternatives, see the description of the SYSLOG option for the NEWLIST statement.

TCP_KEEPALIVE_INTERVAL=*seconds*
This option can be used to request TCP syslog connections to exploit the KEEPALIVE option with the indicated interval in seconds. For instance, if a firewall is set to drop connections after five minutes of idle time, dropping of connections can be prevented by adding an OPTION TCP_KEEPALIVE_INTERVAL=240 statement to request a four minute interval of TCP keep-alive messages. The default is 0 (no KEEPALIVE interval).

Chapter 4. zSecure Alert User Reference Manual

Alert configuration: specify general settings
The following panel was updated:

```
  Menu            Options            Info            Commands            Setup
------------------------------------------------------------------------------
                          zSecure Suite - Setup - Alert
Command ===> ____________________________________________________________

Name  . . . . . . . . . AHJB__                    (also report member)
Description . . . . . . zSecure Alert default alert configuration_

You might need to scroll forward/backward to view all parameters

SMTP node . . . . . . . ________
SMTP sysout . . . . . . B
SMTP writer . . . . . . SMTP____
SMTP atsign . . . . . . @

Interval  . . . . . . . 60__                      (in seconds)
Environment refresh . . 60__                      (in minutes)
Use internal refresh    Y                         (Y/N,blank)
Average . . . . . . . . 300_                      (in seconds)
Buffer size . . . . . . 1024   KB                 (in KB/MB)
Number of buffers . . . 10
TCP keepalive interval  60__                      (in seconds)

RACF database . . . . . BACKUP_                   (PRIMARY or BACKUP)
Collect started task    C2PCOLL_
CKFREEZE data set . . . CRMA.T.DATA.SP390.C2POLICE.CKFREEZE_____
CKFREEZE Collect time   0100                      (Time of day in hhmm)

Extended Monitoring . . y                         (Y/N)
Snapshot retention  . . 12                        (Number of hours, 2-99)

_  Suppress copy of UNIX syslog message in SYSPRRPT


Enter / to view/edit the global CARLa skeleton
_  Skeleton            C2PSGLOB
```

Figure 1. Setup Alert panel: Copying the default Alert Configuration

Use internal refresh
Select this option to use an internal restart of CKRCARLA to refresh environment information. Using this option enables completion of SMF records with additional data from other SMF records for a longer period of time. If this option is not selected, completion of job data is available only if those other SMF records are written during the current environment refresh interval.

Use of this option requires additional storage to retain job information. Ensure that sufficient storage above the 2GB boundary is available; one gigabyte of storage is sufficient to retain data for approximately 8 million jobs.

TCP keepalive interval
Specifies the TCP keepalive interval in seconds. Blank or 0 means no keepalive interval.

Chapter 5. zSecure Messages Guide

The following messages were updated or added:

CKR1235 **Start of data analysis interval *number* at *time***

Explanation

This message indicates that a new pass of processing has started after receiving a soft end-of-file condition.

Severity

00

CKR1481 **[Queuing | Sending] *name* to *addr* port *port* on sockdesc *n*, *name source size* byte [while free *freesize*] *syslog_line***

Explanation

Indicates the destination for a syslog message. It also shows the syslog message EBCDIC encoding. However, the information is sent in UTF-8 format.

The *addr* format corresponds to the IP stack for creating the socket descriptor. If the IPv6 stack is available, IPv4 address are mapped to the IPv6 socket and shown in the following format: `::FFFF:n.n.n.n` where `n.n.n.n` is the IPv4 address. The following examples show the different message formats for IPv4 and IPv6:

Message for an IPv4 address mapped to an IPv6 stack for a UDP destination:

```
CKR1481 00 Sending IPV6V4
to ::FFFF:127.0.0.1 port 514 on sockdesc
0, IPV6V4 at SYSIN line 6 - 245 byte
```

Message for an IPv6 stack:

```
CKR1481 00 Sending IPV6V4 to ::1 port 514
on sockdesc 0, IPV6V4 at SYSIN line 6 -
245 byte
```

Message for an IPv4 stack:

```
CKR1481 00 Sending IPV4LCL to 127.0.0.1
port 514 on sockdesc 0, IPV4LCL at SYSIN
line 6 - 245 byte
```

Severity

00

CKR1483 **Syslog message *name* has more than 1 line, *name source syslog_line_1 syslog_line_2***

Explanation:
Notification that a syslog message sends only the first line.

User response:
Change the message to reduce it to one line.

Severity

12

CKR2003 **Syslog messages not delivered to port *port* of *destination syslog_line***

Explanation:
This message shows the messages that were dropped because the destination could not be reached while the buffer space got filled up. This message can be suppressed so that the JES spool space is not filled in the event of a network breakdown. For CKQRADAR that is in member CKQSPECL.

User response:
Use SUPPRESS SYSLOG_FALLBACK_FILE to suppress this behavior.

Severity

08

CKR2004 **Failed to deliver *number* bytes in *number* messages to port *port* of *IPdestination***

Explanation:
This message is issued at program end or just before program restart. It shows the number of syslog messages that are lost during the current restart interval for the indicated destination. There is one message per destination that lost a syslog message in the current restart interval.

Severity

08

CKR2092 **Buffer overflow: record len *LENGTH* but free only *LEN2* byte, record skipped: *syslog_line***

Explanation:

This message documents an unexpected condition encountered during the buffering operation. The message can be suppressed.

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

CKR2093 **TCP write socket error sockdesc *num* failed RC *nn* [*meaning*] reason *qqqq rrrrx* [*meaning*] of port *port* of *destination***

Explanation:
This message gives diagnostic information for a potentially recoverable write failure on a TCP connection involving the socket level, for example for SYSLOGTCP.

User response:
Look for subsequent messages for the same socket number (sockdesc) to understand whether the retry was successful.

Severity

04

CKR2099 **Real time security event monitoring started [at *timestamp*]**

Explanation:
This WTO message is issued with routing code 9 to help automated operations scripts keep track of the security event monitoring. It is not issued during the hourly RESTART; the SMF feed has no gap during a restart. The SYSPRINT and SYSTERM versions have the local timestamp added at the end.

Severity

00

CKR2101 **BPX*n*OPT setsockopt TCP_KEEPALIVE failed on socket *sockdesc unix error***

Explanation:
A UNIX error occurred during a setsockopt call to set the TCP KEEPALIVE socket option to the OPTION TCP_KEEPALIVE_INTERVAL value. This message can be suppressed.

User response:
See your UNIX system codes book to determine the cause and actions.

Severity

08

CKR2102 **BPX*n*OPT setsockopt SO_KEEPALIVE active failed on socket *sockdesc unix error***

Explanation:
A UNIX error occurred during a setsockopt call to request the connection to be tested periodically. This message can be suppressed.

User response:
See your UNIX system codes book to determine the cause and actions.

Severity

08

CKR2103 **Activity report interval ended at *datetime* cpu *seconds***
[Processed *number type* records]
[Still delayed *number* bytes in *number* messages to *protocol* port *number* of *dest*]
[Dropped *number* bytes in *number* messages to *protocol* port *number* of *dest*]
[Rerouted *number* bytes in *number* messages from *protocol* port *number* of *dest* to port *number* of *dest*]
[Still delayed *number* bytes in *number* messages to *protocol* port *number* of *dest*]
[Sent *number* bytes in *number* messages to *protocol* port *number* of *dest*]
[Issued *number* WTO messages]
[Issued *number* remedial commands]

Explanation:
This message is issued at the end of a reporting interval if that was requested by an OPTION ACTIVITY_REPORT_INTERVAL=*minutes* statement. It shows the local time and the CPU time that is spent in the interval (for the first reporting interval this is since the start of the restart interval). It is followed by optional detail lines for various possible types of activity; these lines are shown only if that type of activity occurred during the interval.

Severity

00

CKR2104 **Sent *number* bytes in *number* messages to *protocol* port *number* of *dest***

Explanation:
This message is issued at the end of the program or at the end of a RESTART interval. It lists the total number of bytes and messages that are sent over the indicated protocol to the indicated destination.

Severity

00

CKR2105 **Issued *number* alert WTO messages**

Explanation:
This message is issued at the end of the program or at the end of a RESTART interval. It lists the total number of (alert) WTOs that are issued.

Severity

08

CKR2106 **Issued *number* remedial commands**

Explanation:
This message issued at the end of the program or at the end of a RESTART interval. It lists the total number of commands that are generated.

Severity

00

CKR2107 **BPX*x*AIO connect failed on socket *SOCKET unix error* {Port *PORT* of *IPADDRESS* | unexpected SOCKADDRLEN=*length*]**

Explanation:
This message indicates that a UNIX error occurred during an asyncio (BPX1AIO or BPX4AIO) connect call on the indicated socket for the indicated port and IP address.

User response:
See your UNIX system codes book to determine the cause and actions.

Severity

12 or 04

CKR2108 **PRIMARY must specify exactly one address**

Explanation:
The DESTINATION statement must provide an alternate address for when a specific primary address stops responding.

User response:
Use a separate DESTINATION statement for each primary/alternate pair of addresses.

Severity

12

CKR2109 **Waiting on destination to be resolved of port *port* of *destination***

Explanation:
This is a critical eventual action operator message that is displayed on the operator console. The message is deleted and repeated once at every RESTART interval (default 60 minutes) when the output is being dropped while waiting for a connection. The *destination* is the destination string as it is passed on a SYSLOGTCP or similar parameter. The *port* can be the default port or a port that the destination string explicitly mentions.

User response
Verify the following conditions:

- The target receiver is known to the DNS resolver and listening on the port. A modification of a SYSLOG or SNMP destination in the input member, followed by /F task,RESTART might be required to resolve the issue.
- There is no firewall that blocks DNS traffic.
- There were no typing errors in the destination.

For more detailed diagnostic information, like return and reason codes, look for a message CKR3039 in the SYSPRINT of the program.

Severity

04

CKR2111 **ALTERNATE must specify exactly one address**

Explanation:
The DESTINATION statement must provide an alternate address for when a specific primary address stops responding.

User response:
Use a separate DESTINATION statement for each primary/alternate pair of addresses.

Severity

12

CKR2112 **DESTINATION *destination* did not contain a resolved *protocol* address at *ddname* line *number***

Explanation:
None of the target address that are defined in the specified destination can be reached.

Severity

12

CKR2113 **BPX*n*OPT setsockopt TCP_NODELAY active failed on socket *sockdesc unix_error***

Explanation:
A UNIX error occurred during a setsockopt call to request the connection to not delay messages. This message can be suppressed.

User response:
See your UNIX system codes book to determine the cause and actions.

Severity

08

CKR2114 **Rerouted *number* bytes in *number* messages from *protocol* port *number* of *prim-dest* to port *number* of *alt-dest***

Explanation:
This message is issued at the end of the program or at the end of a RESTART interval to list the total number of bytes and messages that are rerouted over the indicated protocol from the primary destination to the alternate destination.

Severity

00

CKR2115 **BPX*x*AIO receive on socket *number abend***

Explanation:
An abend occurred during an asyncio receive call on the indicated socket.

User response:
See *z/OS MVS System Codes* to determine the cause and actions.

Severity

12 or 04

CKR2116 **BPX*x*AIO receive failed on socket *SOCKET unix error* {Port *PORT* of *IPADDRESS* | unexpected SOCKADDRLEN=*length*]**

Explanation:
A UNIX error occurred during an asyncio (BPX1AIO or BPX4AIO) receive call on the indicated socket for the indicated port and IP address.

User response:
See your UNIX system codes publication to determine the cause and actions.

Severity

12 or 4

CKR2117 **TCP receive sockdesc*socket* failed *unix error* of port *PORT* of *IPADDRESS* at *timestamp***

Explanation:
The TCP connection monitoring receive operation returned the indicated error condition.

User response:
Ensure that the network connection gets re-established.

Severity

04

CKR2118 **Re-routing TCP traffic of port *number* of *destination* to alternate destination at *timestamp***

Explanation:
This message is issued at most once per restart interval per destination and port to indicate that a buffer was rerouted to the alternate destination that is defined for it. You can use OPTION ACTIVITY_REPORT_INTERVAL=*minutes* to see how much traffic was rerouted.

Severity

00

CKR2119 **TCP destination cannot be used as both primary and alternate address - port *number* of *destination***

Explanation:
An alternate destination IP address and port is used as both the primary destination and the alternate address. That is not supported.

Severity

12

CKR2531 **CKRPRTR.CKRCONN Unexpected state *STATE* of port *port* of *destination***

Explanation:
This message indicates an unexpected condition that the program likely cannot recover from.

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

24

CKR3039 **Connect failed on socket *num* RC *nn* [*meaning*] reason *qqqq rrrrx* [*meaning*] [after *mum* seconds] [contacting port *port* of *IPaddress* at *timestamp* | unexpected SOCKADDRLEN=*len*]**

Explanation

This shows a failure to connect to a remote port. Maybe a firewall blocks the connection, or the destination service is not available, or the port or IP address is incorrect. This message indicates that a BPX1CON or BPX4CON call failed with the indicated return code in decimal and the reason code split into reason code qualifier *qqqq* and reason code *rrrr*, both in hexadecimal. For well-known return codes and reason codes, the numeric values are followed by an explanatory string.

The severity of this message depends on whether this is a retry or an initial attempt, and what the environment is. A job step program gives RC 12 on first attempt.

User response

Look for other return and reason codes in the *z/OS® UNIX System Services Messages and Codes* reference manual available from the IBM Knowledge Center for z/OS. Verify IP address and port number are correct. Verify the destination is actually listening on the port. Verify there is no firewall in between that blocks the traffic.

Severity

4 or 12

CKR3040 **Connect on socket *num* succeeded to *destination*, port *port* of *family* address *IPaddress* at *timestamp* [after *number* seconds]**

Explanation

This logs the successful TCP connection from the indicated socket descriptor number to the *destination* as specified on a destination keyword like SYSLOGTCP. It also shows the port, socket family, and resolved IP address.

Severity

00

CKR3041 **Waiting for connection to port *port* of *destination***

Explanation:
This is a critical eventual action operator message that is displayed on the operator console. The message is deleted and repeated once every RESTART interval (default 60 minutes) when the output is being dropped while waiting for a connection. The *destination* is the destination string as it is passed on a SYSLOGTCP or similar parameter. The *port* can be the default port or a port that is explicitly mentioned in the *destination* string.

User response
Verify the following conditions:

- The target receiver is active and listening on the port. A restart of the application might be required to resolve the issue.
- There is no firewall that blocks traffic.
- There were no typing errors in the destination or port.

For more detailed diagnostic information, like return and reason codes, look for a message CKR3039 in the SYSPRINT of the program.

Severity

04

CKR3043 **TCP write for sockdesc *num* failed RC *nn* [*meaning*] reason *qqqq rrrrx* [*meaning*] of port *number* of *destination***

Explanation

This message gives diagnostic information for an unrecoverable write failure on a TCP connection, for example for SYSLOGTCP.

User response

Check whether the connection was successfully recovered.

Severity

04

CKR3044 **CKR3044 BPX*x*AIO connect on socket *number abend***

Explanation:
An abend occurred during an asyncio connect call on the indicated socket.

User response:
See *z/OS MVS System Codes* to determine the cause and actions.

Severity

12 or 4

CKR3046 **TCP write connection error sockdesc *num* failed RC *nn* [*meaning*] reason *qqqq rrrrx* [*meaning*] of port *number* of *destination***

Explanation

This message gives diagnostic information for a potentially recoverable write failure on a TCP connection, for example for SYSLOGTCP. Look for subsequent messages for the same socket number (sockdesc) to understand whether the retry was successful.

The severity is 4 because waiting for the connection and attempting to reconnect might remove the error condition.

User response

Check whether the connection was successfully recovered.

Severity

04

CKR3800... ***message***
CKR3899

Explanation

These messages are in response to debugging options. If you need information about these messages, 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

00