IBM Security zSecure 2.4.0

Event Correlation And Compliance Automation Service Stream Enhancement (OA61058, OA61059) Documentation Updates - IBM Security zSecure Alert User Reference Manual

Chapter 1. About this document

This document describes the documentation updates as a result of the zSecure event correlation and compliance automation Service Stream Enhancement (SSE, for APAR numbers OA61058 and OA61059 - April 2021).

The following enhancements were made:

- End-to-end event correlation between IBM® z/OS® Connect, CICS®, and Db2® events
- Support for a new layout of SMF record type 123, subtype 1 (z/OS Connect)
- Alerts 1124 (RACF®) and 2124 (CA ACF2) for a TSO logon from an IP address that is not allow-listed
- Support for tape data set sensitivities
- Ability to evaluate STCs through STIG by using a Site Security Plan approach
- More STIG automation (5 controls for CA ACF2, 3 controls for IBM RACF and CA Top Secret) and other STIG-related improvements, such as ensuring a result when no objects are evaluated
- More reporting of ICSF settings
- Audit concern for UACC of ID(*) access of ALTER to discrete profiles
- Ability to use CARLa literals for sorting only (NONDISPLAY)
- Ability to sort command output from RECREATE by profile
- Ability to use longer messages and descriptions in alerts
- Ability to show OPERROUT in exploded format
- Performance improvements for zSecure support for CA ACF2

The documentation updates apply to 2.4.0 zSecure Admin, zSecure Audit, and zSecure Alert. The following publications were updated:

- *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*

Note:

- Referenced topics that were 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 customers only. To access the zSecure 2.4.0 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

The following SCKRCARL member was renamed, from a generic name to an ESM-specific member name.

Table 1. SCKRCARL generic member names renamed for RACF, ACF2, and Top Secret systems. Member C2RGM420 for control AAMV0420 was renamed from a generic name to a member name that is specific for the External Security Manager (ESM). Note that member C2RGM420 is now obsolete.

Control	**Original member**	**Renamed members**		
		RACF	**CA ACF2**	**CA Top Secret**
AAMV0420	C2RGM420	CKAGM420	C2AGM420	CKTGM420

Chapter 2. zSecure Alert configuration

The following sections were updated:

- Identification section in "CARLa skeleton for existing alerts" on page 3
- "Identification section" on page 3

CARLa skeleton for existing alerts

The information in the remainder of this section describes the content of the model skeleton member C2PSMODL. The skeleton consists of several sections, each containing its own specific statements:

Identification section
The alert skeleton starts by setting three text values for the alert messages:

C2PXNAME
Represents an event name that is used in Unix SYSLOG and CEF messages to categorize the event. It must be a short, fixed value without quotes.

C2PXMSG
Specifies the alert message text that is to be included in all alerts. The message can be composed of quoted literals and CARLa fields. The maximum length depends on the number of field names that are used and is approximately 15,000 characters.

C2PXDES
Specifies a description of the event that is to be included in all alerts formats except Cellphone and WTO messages. The message can be composed of quoted literals and CARLa fields. The maximum length is approximately 25,000 characters.

For the syntax of C2PXMSG and C2PXDES, see "Identification section" on page 3.

The message formatting skeleton C2PSFMSG uses these dialog variables to construct the appropriate fields for the destination.

Identification section

To facilitate maintenance of alert skeletons, zSecure Alert contains a message formatting skeleton C2PSFMSG that constructs part of the SORTLIST commands that contain the part of the message that humans should read. There are three dialog variables that you can use to specify these common fields:

C2PXNAME
Represents an event name that is used in Unix SYSLOG and CEF messages to categorize the event. It must be a short, fixed value without quotes.

C2PXMSG
Specifies the alert message text that is to be included in all alerts. The message can be composed of quoted literals and CARLa fields. The maximum length depends on the number of field names that are used and is approximately 15,000 characters.

C2PXDES
Specifies a description of the event that is to be included in all alerts formats except Cellphone and WTO messages. The message can be composed of quoted literals and CARLa fields. The maximum length is approximately 25,000 characters.

```
)SETF C2PXNAME = &STR(Event_name)
)SETF C2PXMSG = &STR('Alert msg about' user(0))
)SETF C2PXDES = &STR('Alert description')
```

Chapter 3. Predefined alerts

New alerts 1124 and 2124 were added to the table in section "Predefined alerts":

Table 2. Predefined Alerts

ID	Description	Class	Severity
1124	Logon from a not allowed IP address	2	3
2124	Logon from a not allowed IP address	2	3

The following sections were added for these new alerts 1124 (RACF) and 2124 (ACF2):

- “Logon from a not allowed IP address (1124)” on page 5
- “Logon from a not allowed IP address (2124)” on page 5
- “Allowed IP address configuration (alerts 1124 and 2124)” on page 6

Logon from a not allowed IP address (1124)

Alert 1124 is sent when a user ID with the SPECIAL, AUDITOR, OPERATIONS, or ROAUDITOR attribute logs on to TSO from an IP address that is not allowed.

To receive this alert, perform the following steps:

1. Log SMF record types 30 subtype 1, 80, and 118 or 119.
2. Set SMFINIT parameter for TELNETPARMS to TYPE119 in the telnet configuration file.
3. Set internal refresh to Y in the Alert configuration.

The email format of the alert is:

```
Alert: Authorized user CRMBXX2 logged on from 9.145.159.178
Logon by a userid from a not allowed IP address

   Alert id        1124
   Date and time   29Mar2021 13:33:08.88
   User            CRMBXX2  IBM DEFAULT USER
   Result          Success
   Job name + id   CRMBXX2  TSU07970
   System ID       8018
   Source terminal STCP0010
   Source IP       9.145.159.178
```

The text message format of the alert is:

```
Subject: Alert 1124: Authorized user CRMBRT2 logged on from 9.145.159.178

Alert 1124: Authorized user CRMBRT2 logged on from 9.145.159.178
```

The generated email report shows the user ID that is used to log on to the system and its IP address.

You can configure the alert for your site. When selecting the alert, you are prompted with a panel. You can enter up to 10 IP addresses or network prefixes that specify from where the user ID is allowed to logon. See “Allowed IP address configuration (alerts 1124 and 2124)” on page 6.

Logon from a not allowed IP address (2124)

Alert 2124 is sent when a logonid with a system-level authority (SECURITY, NON-CNCL, or READALL) logs on to TSO from an IP address that is not allowed.

To receive this alert, perform the following steps:

1. Log SMF record types 30 subtype 1 and 118 or 119.
2. Set SMFINIT parameter for TELNETPARMS to TYPE119 in the telnet configuration file.
3. Set internal refresh to Y in the Alert configuration.

The email format of the alert is:

```
Alert: Authorized user CRMBXX2 logged on from 9.145.159.178
Logon by a logonid from a not allowed IP address

   Alert id        2124
   Date and time   29Mar2021 13:33:08.88
   User            CRMBXX2  IBM DEFAULT USER
   Result          Success
   Job name + id   CRMBXX2  TSU07970
   System ID       8018
   Source terminal STCP0010
   Source IP       9.145.159.178
```

The text message format of the alert is:

```
Subject: Alert 2124: Authorized user CRMBRT2 logged on from 9.145.159.178

Alert 1124: Authorized user CRMBRT2 logged on from 9.145.159.178
```

The generated email report shows the user ID that is used to log on to the system and its IP address.

You can configure the alert for your site. When selecting the alert, you are prompted with a panel. You can enter up to 10 IP addresses or network prefixes that specify from where the logonid is allowed to logon. See “Allowed IP address configuration (alerts 1124 and 2124)” on page 6.

Allowed IP address configuration (alerts 1124 and 2124)

Alert 1123 or 2124 facilitates alerts on logons with high authorizations to TSO from unwanted IP addresses. When it is selected, the following panel is displayed to specify IP addresses or network prefixes from which logons are allowed.

When either alert 1124 or 2124 is selected, the following panel is displayed to specify IP addresses or network prefixes from which logons are allowed.

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

Specify allowed IP addresses or network prefixes
IP address 1  . . . . .
IP address 2  . . . . .
IP address 3  . . . . .
IP address 4  . . . . .
IP address 5  . . . . .
IP address 6  . . . . .
IP address 7  . . . . .
IP address 8  . . . . .
IP address 9  . . . . .
IP address 10 . . . . .

IP addresses can specified in IPv4 format, 111.112.123.78, or specifying a
range with a network prefix, 111.112.0.0/16
```

Figure 1. Setup Alert panel: Specifying allowed IP addresses or network prefixes (alerts 1124 and 2124)