Security zSecure Alert
Version 1.13.1

User Reference Manual

SC22-5467-00

Security zSecure Alert
Version 1.13.1

User Reference Manual

SC22-5467-00

Note

Note

Before using this information and the product it supports, read the information in "Notices" on page 123.

October 2012

This edition applies to version 1, release 13, modification 1 of IBM Security zSecure Alert (product number 5655-T11) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this publication

This manual explains how to configure, use, and troubleshoot IBM Security zSecure Alert, a real-time monitor for z/OS systems protected with the Security Server (RACF) or CA-ACF2.

For information about installing IBM Security zSecure Alert, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Intended audience

This publication is intended for the following people:

- Systems support personnel responsible for configuring IBM Security zSecure Alert
- Security administrators responsible for implementing the additional RACF command controls provided by IBM Security zSecure Alert.

Users of this book must also be familiar with RACF and ACF2 concepts and commands.

What this publication contains

This publication includes the following information:

- Chapter 1, "Introduction," on page 1 introduces IBM Security zSecure Alert and explains what it does and the advantages of using it.
- Chapter 2, "zSecure Alert configuration," on page 3 explains the various alert message formats. These formats include email, text message for pagers or cell phones, WTO for automated operations, SNMP trap for network consoles, and UNIX syslog. The chapter also describes how to configure and select the predefined alerts you are interested in and how to add your own.
- Chapter 3, "Predefined alerts," on page 39 describes the predefined alerts.
- Chapter 4, "Periodical overview," on page 101 explains what you need to do to send a periodical overview.
- Chapter 5, "Problem determination guide," on page 103 explains how to diagnose and fix any problems with IBM Security zSecure Alert.
- Appendix A, "SNMP output," on page 107 describes the format of the SNMP output.
- Appendix B, "Tivoli Enterprise Console and NetView configuration," on page 111 explains how to configure IBM Tivoli Enterprise Console to properly display IBM Security zSecure Alert traps and user-defined IBM Security zSecure Alert traps, and how to configure IBM NetView on AIX for IBM Security zSecure Alert.

Publications

This section lists publications in the IBM Security zSecure library and related documents. The section also describes how to access and order IBM Security zSecure and other IBM Security publications online.

IBM Security zSecure library

The following documents are available in the IBM Security zSecure library:

- *IBM Security zSecure: Release Information*

  For each product release, the Release Information topics provide information about new features and enhancements, incompatibility warnings, and documentation update information for the IBM Security zSecure products. You can obtain the most current version of the release information from the IBM Security zSecure Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_1.13.1/welcome.html.

- *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide, SC22-5463-00*

  Provides information about installing and configuring the following IBM Security zSecure components:

  – IBM Security zSecure Admin
  – IBM Security zSecure Audit for RACF®, CA-ACF2, and CA-Top Secret
  – IBM Security zSecure Alert for RACF and ACF2
  – IBM Security zSecure Visual for RACF
  – IBM Tivoli Compliance Insight Manager Enabler for z/OS

- *IBM Security zSecure Admin and Audit for RACF: Getting Started, GI13-2309-00*

  Provides a hands-on guide introducing IBM Security zSecure Admin and IBM Security zSecure Audit product features and user instructions for performing standard tasks and procedures. This manual is intended to help new users develop both a working knowledge of the basic IBM Security zSecure Admin and Audit for RACF system functionality and the ability to explore the other product features that are available.

- *IBM Security zSecure Admin and Audit for RACF: User Reference Manual, LC22-5464-00*

  Describes the product features for IBM Security zSecure Admin and IBM Security zSecure Audit. Includes user instructions to run the features from ISPF panels, RACF administration and audit user documentation with both general and advanced user reference material for the CARLa command language and the SELECT/LIST fields. This manual also provides troubleshooting resources and instructions for installing the zSecure Collect for z/OS component. This publication is only available to licensed users.

- *IBM Security zSecure Audit for ACF2: User Reference Manual, LC22-5465-00*

  Explains how to use IBM Security zSecure Audit for ACF2 for mainframe security and monitoring. For new users, the guide provides an overview and conceptual information about using ACF2 and accessing functionality from the ISPF panels. For advanced users, the manual provides detailed reference information including message and return code lists, troubleshooting tips, information about using zSecure Collect for z/OS, and details about user interface setup. This publication is only available to licensed users.

- *IBM Security zSecure Audit for ACF2: Getting Started, GI13-2310-00*

  Describes the IBM Security zSecure Audit for ACF2 product features and provides user instructions for performing standard tasks and procedures such as analyzing Logon IDs, Rules, and Global System Options, and running reports. The manual also includes a list of common terms for those not familiar with ACF2 terminology.

- *IBM Security zSecure Audit for Top Secret: User Reference Manual, LC22-5466-00*

Describes the IBM Security zSecure Audit for Top Secret product features and provides user instructions for performing standard tasks and procedures.

- *IBM Security zSecure Alert: User Reference Manual, SC22-5467-00*

  Explains how to configure, use, and troubleshoot IBM Security zSecure Alert, a real-time monitor for z/OS® systems protected with the Security Server (RACF) or CA-ACF2.

- *IBM Security zSecure Visual: Client Manual, SC22-5470-00*

  Explains how to set up and use the IBM Security zSecure Visual Client to perform RACF administrative tasks from the Windows-based GUI.

- *IBM Security zSecure Command Verifier: User Guide, SC22-5471-00*

  Explains how to install and use IBM Security zSecure Command Verifier to protect RACF mainframe security by enforcing RACF policies as RACF commands are entered.

- *IBM Security zSecure CICS Toolkit: User Guide, SC22-5472-00*

  Explains how to install and use IBM Security zSecure CICS Toolkit to provide RACF administration capabilities from the CICS® environment.

- *IBM Security zSecure: Messages Guide, SC22-5468-00*

  Provides a message reference for all IBM Security zSecure components. This guide describes the message types associated with each product or feature, and lists all IBM Security zSecure product messages and errors along with their severity levels sorted by message type. This guide also provides an explanation and any additional support information for each message.

- *IBM Security zSecure: Quick Reference, SC22-5469-00*

  This booklet summarizes the commands and parameters for the following IBM Security zSecure Suite components: Admin, Audit, Alert, Collect, and Command Verifier. Obsolete commands are omitted.

- *IBM Security zSecure: Documentation CD, LCD7-1387-12*

  Supplies the IBM Security zSecure Information Center, which contains the licensed and unlicensed product documentation. The *IBM Security zSecure: Documentation CD* is only available to licensed users.

- *Program Directory: IBM Security zSecure Suite CARLa-driven components, GI11-7862-07*

  This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of IBM Security zSecure CARLa-Driven Components: Admin, Audit, Visual, Alert, and the IBM Tivoli Compliance Insight Manager Enabler for z/OS. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure Information center available at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_1.13.1/welcome.htm.

- *Program Directory: IBM Security zSecure CICS Toolkit, GI11-7863-06*

  This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of IBM Security zSecure CICS Toolkit. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure Information center available at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_1.13.1/welcome.htm.

- *Program Directory: IBM Security zSecure Command Verifier, GI11-7864-07*

This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of IBM Security zSecure Command Verifier. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure Information center available at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_1.13.1/welcome.htm.

- *Program Directory: IBM Security zSecure Admin RACF-Offline, GI11-8146-06*

  This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of the IBM Security zSecure Admin RACF-Offline component of IBM Security zSecure Admin. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure Information center available at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_1.13.1/welcome.htm.

Related documentation

More information about RACF and the types of events that are reported through IBM Security zSecure Alert can be found in several IBM manuals. For information about incompatibilities, see the **Incompatibility** section under **Release Information** of zSecure in the IBM Information Center. You can find information about the various types of events that are recorded by RACF in the *RACF Auditor's Guide*.

Table 1. Further information about RACF administration, auditing, programming, and commands

Full title of manual	Order number
z/OS V1R13 Security Server RACF Command Language Ref.	SA22-7687
z/OS V1R13 Security Server RACF System Administrator's Guide	SA22-7683
z/OS V1R13 Security Server RACF Auditor's Guide	SA22-7684
z/OS V1R13 Security Server RACF System Programmer's Guide	SA22-7681
z/OS MVS System Commands	SA22-7627

Accessing terminology online

The IBM Terminology website consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

Visit the IBM® Accessibility Center at http://www.ibm.com/alphaworks/topics/accessibility/ for more information about IBM's commitment to accessibility.

Accessing publications online

The *IBM Security zSecure: Documentation CD* contains the publications that are in the product library. The format of the publications is PDF, HTML, or both.

IBM posts publications for this and all other Tivoli® products, as they become available and whenever they are updated, to the Tivoli Information Center website at http://www.ibm.com/tivoli/documentation.

Note: If you print PDF documents on other than letter-sized paper, set the option in the **File → Print** window that allows Adobe Reader to print letter-sized pages on your local paper.

Ordering publications

You can order many IBM publications online at:

http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss.

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order IBM publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss.
2. Select your country from the list and click the Arrow icon.
3. Click **About this site** in the main panel to see an information page that includes the telephone number of your local representative.

Licensed publications

Licensed publications are indicated by a publication number that starts with *L* (for example, LC22-5464-00). To obtain PDF or printed copies of licensed publications, send an email requesting the publication to:

tivzos@us.ibm.com

Include the following information:

- IBM customer number
- List of publication numbers that you want to order
- Preferred contact information

You will be contacted for further instructions for fulfilling your order.

Accessibility

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use software products successfully. For keyboard access in the IBM Security zSecure products, standard shortcut and accelerator keys are used by the product, where applicable, and are documented by the operating system.

Technical training

For technical training information, see the following IBM Education website at:

http://www.ibm.com/software/tivoli/education/.

Support for problem solving

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

Online

Go to

the IBM Software Support site at http://www.ibm.com/software/support/probsub.html and follow the instructions.

IBM Support Assistant

The IBM Support Assistant is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The Support Assistant provides quick access to support-related information and serviceability tools for problem determination. To install the Support Assistant software, go to http://www.ibm.com/software/support/isa.

Chapter 1. Introduction

IBM Security zSecure Alert is a real-time monitor for z/OS systems protected with the Security Server (RACF) or CA-ACF2. zSecure Alert issues alerts for important events relevant to the security of the system at the time they occur. It is part of the IBM Security zSecure suite and builds on zSecure Audit. This chapter explains the functionality of zSecure Alert in terms of its relationship to basic z/OS components and other auditing, automation, and monitoring software.

The main audit log of a z/OS system is the System Management Facilities (SMF) log. This log records events for Data Facility Storage Management Subsystem (DFSMS); for example, opening a data set, z/OS UNIX System Services, network functions (VTAM, TCP/IP), RMF (performance data), JES2/JES3 (job activity, TSO sessions, started task activity, SYSIN/SYSOUT/NJE processing), the external security manager (RACF, ACF2, TSS), and other applications. Data can be extracted by post-processing the SMF log for many different purposes. Commercial software is available for various purposes including accounting and billing based on resource use, performance analysis, capacity management, and monitoring security. zSecure Audit analyzes z/OS system security for RACF or ACF2 systems, using the SMF log as primary information for the event audit reports.

The traditional post-processing of SMF records has one major drawback: the time elapsed between the event and the post-processing can often be up to a day. While this drawback can be acceptable for billing and capacity management, it can pose a problem for security. If a real intrusion attempt is going on, you must respond to it right away. zSecure Alert is designed to do this job. You can deactivate part of your application or network, or collect data on the location and identity of the intruder while the trail is hot. You also know when a global security setting is changed to turn off logging for certain events to SMF.

zSecure Alert is active in your system, capturing SMF data before it is written to the SMF log. It can notify you in seconds to minutes about suspicious events. In addition, zSecure Alert also captures WTOs so that you can, for example, be notified the instant the SMF log becomes full. Notifications can be sent in the following forms:

- As an email
- As a text message to your pager or cell phone through an e-mail-based relay
- As a WTO, which can be used to trigger your automated operations package
- As an SNMP trap, which can be picked up by, for example, IBM Tivoli Security Operations Manager or your network console
- To the UNIX syslog

zSecure Alert also supports Extended Monitoring alerts. Unlike the event-based alerts triggered by SMF and WTO events, Extended Monitoring alerts are status-based. They are triggered by changes in the status of the system and security settings. These types of alerts are based on comparing a snapshot of the current system and security settings to a snapshot of previous system and security settings. The snapshots are taken at regular, user-specified intervals. The data is compared each time a new snapshot is taken. Whenever something significant changes, an alert can be generated. This alert type can notify you of changes that occur in the system, even when those changes do not generate an SMF or WTO event.

On RACF systems, zSecure Alert can dynamically install and activate an additional RACF exit (ICHPWX01) to create SMF records for user password changes. These SMF records are similar to the records created by the RACF PASSWORD command, but they can be recognized by a special value for the SMFUID field. You can control activation of these exits using the C2XEXITS parameter in the zSecure configuration. For more information, see the configuration information in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

zSecure Alert consists of two components:

- A long-living address space (a started task) that does the actual capturing, correlation, and alert generation.
- An ISPF interface that you can use to specify which events are to be reported, and in what format.

zSecure Alert comes with a set of predefined alerts described in Chapter 3, "Predefined alerts," on page 39. You can also specify your own alerts. See the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual* for information about the full power of the CARLa Auditing and Reporting Language (CARLa) and its great flexibility in selecting events and applying thresholds. You can also use CARLa to customize alerts by including installation-specific data such as user data or parts of the installation data held in the security database, and key-based lookups in general.

The following graph presents the zSecure Alert architecture.

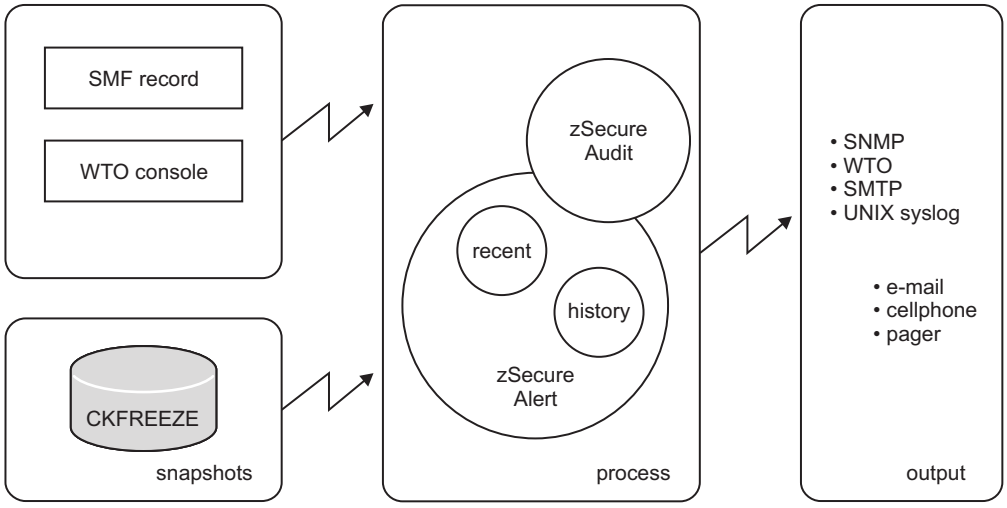

Figure 1. zSecure Alert architecture

Chapter 2. zSecure Alert configuration

This chapter describes the zSecure Alert configuration process. It explains the various steps to select, configure, and activate zSecure Alert in detail.

The ISPF user interface used during the zSecure Alert configuration process has its own configuration. This IBM Security zSecure configuration must be completed and selected as described in the post-installation tasks section in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

For information about zSecure Alert address space operations, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Overview

In the configuration process, you must specify the settings that are unique to your installation. You must specify alert conditions, the destination where you want to deliver the resulting alerts, and the alert format. You can find all this information in the Alert Configuration.

If you want to work on a configuration without immediately impacting the production environment, you can create multiple Alert Configurations. By doing so, you can easily have different configurations for multiple environments or different z/OS images. In each z/OS image, only one configuration can be active at a time. In a full sysplex environment, sometimes known as a PlatinumPlex, you can use the same Alert Configuration on all z/OS images. In partial sysplex implementations, sometimes called BronzePlex or GoldPlex, you can use a different Alert Configuration for each z/OS image. After completing the Alert Configuration, you can activate the configuration.

The Alert Configuration contains two types of information.

- General settings that are required for the started task, such as the number and size of the data buffers.
- A specification of which alert conditions you want to monitor, and how the resulting alerts can be delivered.

Because zSecure Alert provides many predefined Alert Conditions, these Alert Conditions are grouped into Alert Categories. Because the alert conditions are grouped, you can configure multiple alert conditions at the same time. The following sections explain how to set options for an entire category or for individual alerts.

Aside from the Alert Configurations, you can also create an *email Destination*. An Email Destination refers to a data set that contains email addresses. The Email Destination specifies how to interpret the data and locate the email addresses you want. Alert Configurations use several of the created Email Destinations to specify where alerts can be sent.

Note: Text messages to mobile phones are also sent by email, and thus require an email address.

Figure 2 provides an overview of the configuration of zSecure Alert. The zSecure Alert Configuration data set contains multiple Alert Configurations and zero or more Email Destination definitions. Each configuration and destination has a unique name.

Note: The names of the Alert Configurations and Email Destinations can be unrelated. However, to make it easier to identify Alert Configurations and Email Destinations, create names that are short mnemonics that reflect their intended use.

In the example in Figure 2, the Alert Configuration `ProdA` has default Email Destination `TEST`. Several Alert Categories and individual Alert Conditions have overriding Email Destinations. Each Email Destination defines which parts of the associated data sets contain the desired email addresses. The email address data sets are physically separate from the zSecure Alert Configuration data set.

Alert Configuration data set

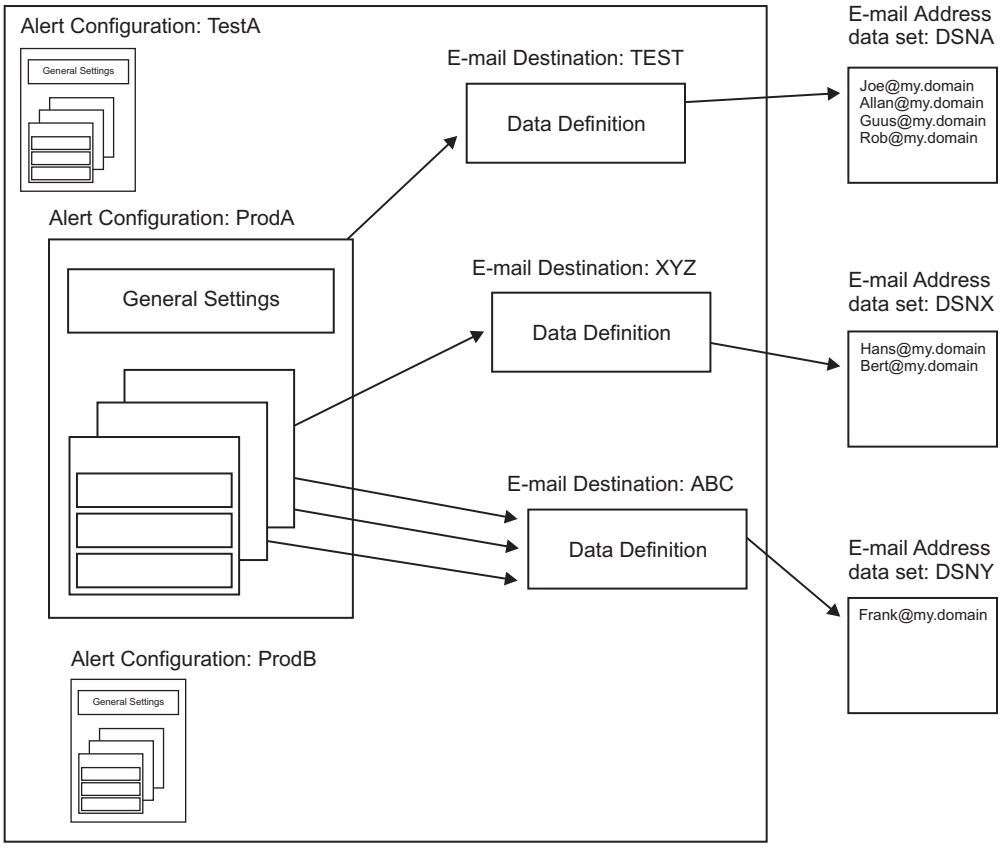

Figure 2. Alert Configuration data set

Alerts can be sent to various destinations. zSecure Alert currently supports the following destination types:

- Email
- Text message
- WTO
- SNMP trap
- UNIX syslog

The alert format is specified per destination type. The alerts provided with the product have a common email layout that is described in “Standard email layout” on page 42. The text message format is a shortened version of the email format for use with an e-mail-to-text-message gateway. It is displayed on a cell phone or pager. For the UNIX syslog layout, see “UNIX syslog layout” on page 36. The SNMP trap format is explained in Appendix A, “SNMP output,” on page 107. For more information about the supplied IBM-alerts, see Chapter 3, “Predefined alerts,” on page 39. For questions about configuring text messaging, contact IBM Software Support.

When you add your own alerts, you can tailor the various formats to suit your needs. See “Installation defined alerts” on page 27.

Alert activation guidelines

An important step in configuring zSecure Alert is deciding which alert conditions to monitor and whether you want specific destinations for the alerts. For example, activating all alerts might cause the designated recipients to be flooded with emails. You can monitor only the most relevant alert conditions first, and see how much attention they demand.

To assist you in selecting alert conditions, zSecure classifies all predefined alerts. See Table 5 on page 39.

- Class 1 contains the Alert Conditions that are most likely to be active for a basic or Low level of vigilance.
- Class 2 contains likely candidates to add for reaching a Medium level of vigilance.
- Class 3 contains Alert Conditions that you must activate if you want a High level of vigilance.

This classification is just a global guideline. To activate the alerts to reach a certain level of vigilance mainly depends on your security policy and the attacks you want to guard against. Monitoring possible abuse of authorization has other requirements than detecting an intrusion attempt or being alerted to a denial of service attack.

For example, alert 1301 is triggered when a started task gets its user ID from a catchall profile in the STARTED class on a RACF system. Alert 2301 is triggered when a started task uses the default logon ID as specified by the GSO OPTS setting DFTSTC on an ACF2 system. Your security policy might forbid this action; in that case you can monitor it. You might, in fact, have an administrative policy in place to minimize effort in administering started tasks. In this case, activating the alert would be distracting and your vigilance level would deteriorate.

You can also configure Extended Monitoring alerts. Extended Monitoring alerts are based on the detection of changes in the system. They are useful for those types of changes that are not accompanied by an SMF or WTO event record. For example, in-storage updates to certain z/OS control blocks can be detected by an appropriate Extended Monitoring alert. Such a change need not be detected by SMF-based or WTO-based alerts. Extended Monitoring alerts only detect that something has changed. They do not provide details about who made the change and how the change was made.

Note: Before Extended Monitoring Alerts can be activated, the person who installs and configures zSecure Alert must perform some configuration tasks. For more

information about the configuration tasks, see the zSecure Alert Post-installation tasks section in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

During the implementation phase, consider writing specific alerts to a file instead of sending them. This practice decreases the number of alert messages that are being generated and reduces the chance that the recipient might decide to ignore all of the messages. For more information about writing alerts to a file, see "Alert configuration: managing alert configurations (SE.A.A)" on page 10.

Configuration guidelines and performance implications

zSecure Alert processing consists of several parts. The parameters specified at startup influence the overall performance of zSecure Alert and its impact on other users. The parameters that are specified in the general settings of each Alert Configuration are the *intervals*, the *buffer size*, and the *number of buffers*.

Intervals

There are several relevant intervals:

- The reporting interval for performing data analysis and generating alerts
- The `stage 1` interval for reassessing the environment
- The "average" interval for "moving window" analysis

By default, data analysis is done every 60 seconds. This interval can be increased if you do not need almost real-time alert messages. If you need a faster response, you can reduce the interval time.

Note: For each reporting interval, a new buffer is used so that this ties in with the buffer considerations explained in "Buffers."

The `stage-1` preprocessing subtask obtains current information about the system environment and user attributes. This task is carried out hourly by default. For example, information about data sets and system control blocks, is collected in a CKFREEZE data set, which is refreshed once a day at the specified time. However, it is also possible to have zSecure Alert dispatch this task by the operator command MODIFY C2POLICE,COLLECT.

Some "averaging" alerts with thresholds might use a time window larger than the reporting interval. For these alerts, SMF records are kept in history buffers for five times the reporting interval, for example. This long-term analysis interval can be adjusted as well, depending on your reporting needs.

Buffers

Another important consideration for the configuration of zSecure Alert is the in-memory buffer usage. The buffer space used by zSecure Alert is regular pageable storage in the private area of the zSecure Alert started task address space. It is similar in all aspects to the working storage of a TSO user editing a data set. As a guideline for calculating the buffer size, you can perform the following steps.

Note: The numbers given in the steps are for illustration purposes only and must not be used as a starting point for your system.

1. Look at the output of your SMF dump program. Summarize the number of RACF SMF records (Record type 80) or ACF2 SMF records, and Accounting SMF records (Record type 30) written per day.

For instance, on a small system, during an average day, the MAN data sets are switched and dumped five times. The output of the IFASMFDP program shows the following numbers of RACF or ACF2 SMF records: 50,000 32,000 69,000 49,000 and 27,000. The total number of RACF or ACF2 SMF records written during that average day is 227,000. The number of SMF 30 Records were: 19000 15000 31000 23000 and 17000. The total number of SMF 30 records during the day is 105,000.

2. Assuming an alert reporting interval of 1 minute (the default), calculate the number of records per interval.

   In this example, it yields 227,000 / 1440 = 158 RACF or ACF2 records, and 105,000 / 1440 = 73 SMF-30 records per minute.

3. Look at the output of your SMF dump program for the average record length of these SMF records. It must be 250 - 300 bytes for the RACF records, 600 - 700 bytes for ACF2 records, and 1000 - 1500 bytes for the SMF-30 records.

4. Multiply the average number of records by the average record length to find the average buffer size per interval.

   In the example of the small system, it results in (158 * 274) + (73 * 1224) = 132,644 bytes.

5. To accommodate for normal fluctuations in system workload, multiply the average found by a factor of 5, and round up to the nearest "nice" number to find the best starting point for your *bufsize* parameter.

   In the example, a good setting for the *bufsize* parameter is 700 KB.

After determining the minimum buffer size, the next concern is about the number of buffers required. As mentioned, the minimum number of buffers is also related to your long-term event analysis. For instance, if you want to generate an alert whenever a user generates more than 10 RACF logon violations in 10 minutes, the amount of data kept in the buffers must represent at least 10 minutes. Because one buffer is always being filled with new events and therefore not available for the averaging process, the formula becomes:

```
Numbufs > (AverageInterval / Interval) + 1
```

As a starting point, use twice the number of buffers based on the previous formula. So, assuming that you use the default values for *Interval* (60 seconds) and for *AverageInterval* (300 seconds), you end up with 2*((300/60)+1) = 12 buffers.

Additional buffers allocated through this procedure can be used as overflow buffers for periods with high system activity. Typically, such periods do not last long. The previous example calculation allows for short periods (1 minutes or 2 minutes) where three to four times the normal amount of SMF records must be captured.

In the previous examples, it is assumed that the default values for *Interval*, and *AverageInterval* are used. The main criteria for determining these parameters are the reporting requirements. For most installations, an alert response time of about 1 minute seems appropriate. It is also well in the normal response time of people to emails, or other methods of alert delivery. For the *AverageInterval*, the use of a 5-minute interval is sufficiently long to avoid excessive false alarms, It is also short enough to detect most situations for which alerts are wanted.

You can use the following values as starting values for these OPTION and REPORT parameters:

Bufsize

1024 (=1 MB) for RACF systems or 2028 (=2 MB) for ACF2 systems.

This is based on the average length of an RACF or ACF2 SMF-record, the following specified interval, and an average of 40 RACF or ACF2 SMF-records per second during periods of high activity.

NumBufs
12

This is based on the long-term threshold time-period (*AverageInterval*) and the *Interval* period. It also allows for an additional six overflow buffers.

Interval
60 Seconds

AverageInterval
300 Seconds

During initial execution of zSecure Alert, monitor the in-memory buffer usage, using the DEBUG BUFFER operator or PARMLIB command. This results in three messages at the end of each *Interval* period. The C2P0325 and C2P0326 messages indicate how much buffer space was used for SMF-records and WTO-messages. If the amount of space for the SMF-records and WTO-records for each interval adds up to around the size calculated in step 4, the buffer space is adequate and does not need any further changes. In step 5, the buffer size was specified at five times the average expected space required. So, the buffers are expected to be used for only about 20 percent. It leaves ample space for fluctuations in system activity.

Using the same numbers as used in the previous example calculation, you might expect these messages:

```
C2P0333I Buffer index is 09
C2P0325I Buffer stats: SMF(cnt,len) 00000214-00131928
C2P0326I Buffer stats: WTO(cnt,len) 00000000-00000000
```

The messages confirm that your expected record rate was about right, that is, 214 records versus the expected 231, and that the average size of the records was also in the right order of magnitude, that is, 131,928 versus the expected 132,644.

When activating buffer debug messages, zSecure Alert also generates a message whenever there is a need for an overflow buffer. See the following message example:

```
C2P0334I Extended buffer used
C2P0333I Buffer index is 02
C2P0325I Buffer stats: SMF(cnt,len) 00002728-01037650
C2P0326I Buffer stats: WTO(cnt,len) 00000000-00000000
C2P0333I Buffer index is 03
C2P0325I Buffer stats: SMF(cnt,len) 00000814-00307855
C2P0326I Buffer stats: WTO(cnt,len) 00000000-00000000
```

These messages are issued in addition to the regular buffer usage messages. The indicated buffer '02' is the previous buffer that was overflowing into the subsequent buffer ('03'), which is shown in the regular C2P0325 and C2P0326 messages that follow. If the C2P0334 message is only issued a few times per day, the buffer size is adequate and does not need any further changes. During normal processing, a few C2P0334 messages are expected and their presence does not indicate any buffer shortage or problem.

Using the steps previously outlined, you can select a minimum buffer size and number of buffers that fits your needs, without using excessive system resources. The method starts with small buffers that can be increased when needed. An

alternative approach is to start with many large buffers, and monitoring the buffer statistics messages. After a few tests, you can decide by which amount the buffer size can be reduced.

When allocating buffers, you must also consider the amount of virtual storage specified in the zSecure Alert started task JCL. The region parameter in the JCL must be at least 64 MB larger than the total buffer space specified by *bufsize* and *numbufs*.

Configuring zSecure Alert

About this task

The zSecure Alert configuration process involves several steps, which are performed from the option **SE.A** on the zSecure Admin and Audit menu. If you select this option, you can see the following panel:

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

A    Alert           Select and customize alerts
E    E-mail          Configure e-mail address lists
```

Figure 3. zSecure Suite: Setup Alert panel for configuring zSecure Alert

The zSecure Alert configuration application provides the following options.

- Use **Alert** to configure Alert Conditions and destination of the resulting alerts.
- Use **Email** to define how to obtain email addresses from external data sets, to avoid using hardcoded email addresses in the Alert Configuration.

Procedure

To configure zSecure Alert, perform the following steps:

1. Optionally, define at least one Email Destination for use in the Alert Configuration to avoid hardcoded email address specifications. You can reach this through option SE.A.E. See note 1.
2. Copy the default Alert Configuration (C2PDFL), which is provided as part of the shipped product. This step and the following ones are reached through option SE.A.A. See note 2.
3. Edit the General Settings.
4. Specify the Alert Destinations on the Alert Configuration level.
5. Select which Alert Conditions you want to monitor. During this process, you can override Destinations on the alert category level or on the individual alert level.
6. Verify the Alert Configuration. See note 3.
7. Refresh or Activate the Alert Configuration. See note 3.

Results

Note:

1. After completing step 1, you can use the Email Destination in the other steps. However, if you are a first time user, you can skip step 1. In that case, you cannot use Email Destinations, but you can still hardcode an email address in

the Alert Configuration. In this way, you can gain experience with alert monitoring and creation. At a later stage during the zSecure Alert implementation, you can revisit the configuration process. At that time you can add the necessary Email Destinations and change the Alert Configuration to use them.

2. Step 2 on page 9 is included because the default Alert Configuration is intended to be used as a template for your own configuration. For this reason also, not all adaptations are used with the default configuration. A side effect of using the Copy command to create an Alert Configuration is that the configuration application takes you automatically to all the required configuration steps. That way, you do not need to track the steps, but complete the necessary fields.
3. Steps 6 on page 9 and 7 on page 9 are both required to make the updated Alert Configuration available for the zSecure Alert address space. In some cases, it is necessary to rerun these transactions. These cases include:
   - If you have been running, for a time, with a higher release of the ISPF interface, and need to perform a fallback, see the section about backing out an upgrade in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.
   - In some cases, maintenance was applied to specific components of IBM Security zSecure. If so, the installer of the maintenance must notify you.

The following sections describe how to perform the tasks, set up email destinations for easier maintenance, and add your own alert definitions.

Alert configuration: managing alert configurations (SE.A.A)

About this task

To manage Alert configurations, use option **SE.A.A (Alert)**. An Alert configuration specifies which alert conditions you want to monitor, and where and how the alerts must be sent. It also contains general parameters that are required for the zSecure Alert started task. Only one Alert configuration can be active at a time on a z/OS image. After setting the alert conditions, destinations, and parameters, you must verify the Alert configuration. The verification process ensures that the configuration is consistent and does not contain errors that prevent it from being used. The Alert configurations that have been verified can be made active.

Note: Changes made to the alert configuration are not permanently saved until you leave option SE.A.A.

When you select option SE.A.A (Alert), the following panel is displayed:

```
  Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                        zSecure Suite - Setup - Alert     Row 1 from 2
 Command ===> _____________________________________________          Scroll ===> CSR

Managing alert configurations
Line commands are available depending on the configuration stage: C(opy),
D(elete), I(nsert), E(dit), W(Who/Where), S(elect), V(erify), F(Refresh),
B(rowse)

------------------------------------------------------------------------------ Configuration steps ---
    Name      Description                                                      Set Des Sel Ver Ref  Act
_   C2PDFL    zSecure Alert default alert configurati                          Req Req Req Req Req  _
------------------------------------------------------------------------------
_   PRODA1    Alert config for production image A1                             Req Req Req Req Req  _
------------------------------------------------------------------------------
 ****************************** Bottom of data ********************************
```

Figure 4. Setup Alert panel: Configuring zSecure Alert

This panel provides an overview of the existing Alert configurations and shows how far configuration has proceeded. The Configuration steps show `OK` if a step has completed or `Req` if the Alert configuration requires that particular step. The Act column can show an indication that the configuration is currently active on this system. In the screen display, you must perform all configuration steps. The panel shows the following fields:

Name

The name of the Alert configuration. The Alert configuration name must be unique and has a maximum length of six characters. Alert configuration names with prefix `C2P` are reserved for IBM Security zSecure use. Several PDS/E members prefixed with this name are created by the Verify (**V**) and Refresh (**F**) line commands. For more information about the members generated during these steps, see "Alert configuration: verifying alert configuration" on page 22.

Description

A description for the Alert configuration.

Configuration steps

This group of fields indicates the steps required to complete the configuration and the order of these steps. The corresponding line commands are available only when the previous step has been completed. Initially a step is indicated as **Req**. After it is successfully completed, it shows **OK**. Perform the following steps:

1. **Set:** Specify the zSecure Alert parameters. The corresponding line command is **E**; that is, Edit general Alert configuration settings.
2. **Des:** Set the default Alert destination for all selected Alert conditions in this Alert configuration. Destinations can be email addresses, text message/cell phone receivers, SNMP addresses, WTO messages, and UNIX syslog. The corresponding line command is **W**; that is, Specify Who can receive alerts or Where alerts must be sent.
3. **Sel:** Select which Alert conditions you want to monitor, and optionally specify Alert destinations on the alert category or individual alert level. You can also specify your own Alert conditions. The corresponding line command is **S**; that is, Specify alerts and their destinations for this Alert configuration.
4. **Ver:** After finishing all previous steps, you must verify the Alert configuration for errors. The corresponding line command is **V**; that is, Verify Alert configuration.

5. **Ref:** After successful verification, you can decide to put the verified Alert configuration in production. The Refresh command copies several PDS/E members over the existing production members. In addition, a refresh command is issued to the possibly active zSecure Alert address space in this system. This command causes the system to read its configuration members again. The corresponding line command is **F**; that is, Refresh production members.

   Note: The PARMLIB DD-statement in the started task JCL must point to your configuration data set and this alert configuration.
6. **Act:** A **Yes** in this column indicates that this Alert Configuration is the active configuration on this z/OS image. The converse is not necessarily true, because you might not have sufficient authority to issue the z/OS MODIFY command required to retrieve this information. If the name of the active started task does not match the name specified in this Alert configuration, the **Act** column is blank.

The Alert configuration overview panel provides all Alert configuration management functions. The following table describes the line commands that are available. Some line commands are available only after the earlier configuration steps have been completed. Enter a forward slash (/) to see the currently allowed line commands.

Table 2. Alert Configuration Management line commands

C	Copy the Alert Configuration. This action can display the general settings panel with all fields. These fields are copied from the selected Alert configuration, except for the Name field, which must be unique for each Alert configuration.
I	Insert a new Alert configuration. This action displays the general settings panel with all fields blank. When all required fields have been entered, the new Alert configuration is added.
E	Edit general settings for this Alert configuration. The corresponding configuration step is **Set**.
D	Delete the selected Alert configuration.
W	Set the Alert destinations on the Alert configuration level. Destinations can be email addresses, text message/cell phone destinations, SNMP addresses, WTO messages, and UNIX syslog. The corresponding configuration step is **Des**.
S	Select which Alert conditions you want to monitor, and optionally specify Alert destinations on the alert category or individual alert level. It is also possible to create your own Alert conditions. The corresponding configuration step is **Sel**.
V	Verify the Alert configuration for errors. The corresponding configuration step is **Ver**.
F	Refresh production members. The verified members are copied to production members. If the address space is active on this system, a command is issued to reprocess its production members. This is effective only if the started task JCL uses this Alert configuration. The corresponding configuration step is **Ref**.
B	Browse the general settings for this Alert configuration.

Alert configuration: specifying general settings

The General Settings panel is displayed when you use the **E**(Edit), **C**(Copy) or **I**(Insert) line command on the Alert Configuration overview panel. The main difference between the three actions is the amount of information already present in the panel.

- When you Edit, all current information for the selected configuration is shown.

- When you Copy, all information except the Name is taken from the copied configuration.
- When you Insert, only default settings are entered. You must provide the additional information to make the configuration a valid one.

The following screen shows the panel image that you see when using the Copy command to copy the default Alert configuration (C2PDFL).

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Admin+Audit for RACF - Setup - Alert
Command ===> ____________________________________________________________

Name  . . . . . . . . . AHJB                    (also report member)
Description . . . . . . zSecure Alert default alert configuration

You may scroll forward/backward to view all parameters

SMTP node . . . . . . . ________
SMTP sysout . . . . . . B
SMTP writer . . . . . . SMTP

Interval  . . . . . . . 60                      (in seconds)
Environment refresh . . 60                      (in minutes)
Average . . . . . . . . 300                     (in seconds)
Buffer size . . . . . . 1024                    (in kilobytes)
Number of buffers . . . 10

RACF database . . . . . BACKUP                  (PRIMARY or BACKUP)
Collect started task    C2PCOLL
CKFREEZE data set . . . CRMA.T.DATA.SP390.C2POLICE.IOCONFIG
CKFREEZE Collect time   0100                    (Time of day in hhmm)

Extended Monitoring . . y                       (Y/N)
Snapshot retention  . . 12                      (Number of hours, 1-99)


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

Figure 5. Setup Alert panel: Copying the default Alert Configuration

You must provide the relevant information in this panel. After you complete the fields, you can use the END key (PF3) to save these settings. If you used the Copy or Insert line command to reach this panel, pressing END automatically takes you to the next step in the configuration process. Otherwise, you can return to the Alert Configuration overview panel.

Note: Before you use this panel, see "Configuration guidelines and performance implications" on page 6.

The General Settings panel has the following fields:

Name The name of the Alert configuration. This field is required. See Name.

Description
A description for the Alert configuration. This field is required.

SMTP node
Specifies the JES destination to which emails are routed for final processing. This setting is initially taken from SETUP OUTPUT. (This option is part of the zSecure Admin and Audit interface.) When not specified on SETUP OUTPUT, a search is done for REXX SMTPNOTE to obtain the value of SMTPNODE. If the SMTP server is running on your

local system, this field can be left blank. If the SMTP server is running on your local system, ask your system programmer for the correct setting.

SMTP sysout
Specifies the JES output class to be used for the SMTP output processing of emails. This setting is initially taken from SETUP OUTPUT. When not specified, a default of sysout class B is used. This field is required. Ask your system programmer for the correct setting.

SMTP writer
Specifies a name for use in SMTP when selecting an email SYSOUT data set. The external writer name is equal to the SMTP address space name. This setting is initially taken from SETUP OUTPUT. When not specified on SETUP OUTPUT, a search is done for REXX SMTPNOTE to obtain the value of SMTPJOB. This field is required. Ask your system programmer for the correct setting.

Interval
Specifies the reporting interval. At each interval, zSecure Alert analyzes the collected WTO and SMF records and generates alert messages. The interval also defines the frequency with which messages can be sent. A recipient gets a message for every alert subscribed, if it was triggered one or more times during the interval. The default is 60 seconds.

Interval corresponds to the REPORT option INTERVAL. See the description of the **Interval** field in the REPORT command section of the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Environment refresh
Specifies the interval at which zSecure Alert generates the environment-dependent selection criteria (that is, analyze the RACF database and CKFREEZE file, and refresh alert definitions based on current RACF database content). The default is 60 minutes.

Environment refresh corresponds to the REPORT option STAGE1INTERVAL. See the description of the **PreProcessInterval or Stage1Interval** field in the REPORT command section of the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Average
Specifies the time period in seconds over which zSecure Alert averages the occurrence of certain events for *moving window* analysis. The default is 300; that is, 5 minutes. See the description of the **Number of buffers** field for the relation between **Average**, **Interval**, and **Number of buffers**.

Average corresponds to the REPORT option AVERAGEINTERVAL. See the description of the **AverageInterval** field in the REPORT command section of the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Buffer size
Specifies in kilobytes the size of each of the in-memory buffers used for storing WTO and SMF records during the interval period. The number must be 1 - 16384. The default is 1024; that is, 1 MB. If a buffer proves to be too small during an interval, zSecure Alert attempts to switch to an unused buffer. If no free buffer is available, the buffer with the oldest information is overlaid with current information. If the size and number of buffers is insufficient, data-loss error messages are logged.

Buffer size corresponds to the OPTION BUFSIZE. See the description of the **Bufsize** field in the OPTION command section of the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Number of buffers
Specifies the number of buffers allocated. The number must be 2 - 32. The number must be sufficient to contain Average / Interval + 1 buffers. To cope with peaks in the event arrival rate, extra buffers beyond the minimum must be allocated. The extra buffers can be used in event of a buffer overflow.

Number of buffers corresponds to the OPTION NUMBUFS. See the description of the **Numbufs** field in the OPTION command section of the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Security database
Specifies whether the PRIMARY or BACKUP security database is used to generate the environment-dependent selection criteria. Use of the PRIMARY database might be needed if you create your own alerts that use certain statistical information like the time of last user access. In all other cases, use of the BACKUP database has the least impact on other system components and provides all information used by the predefined alerts.

Collect started task
Specifies the name of the started task that is started by the zSecure Alert address space at **CKFREEZE Collect time**. This started task calls program CKFCOLL to collect environmental data.

Collect started task corresponds to the OPTION COLLECTSTCNAME. See the description of the **CollectSTCName** field in the OPTION command section of the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

CKFREEZE data set
Specifies the name of the CKFREEZE data set containing environmental data.

Note: zSecure Alert does not enforce that the data set name you specify here matches the one that is specified in the **Collect started task** JCL. In that case, the name you specify here is only used during Verify processing of the Alert Configuration. If this data set is specified in the **Collect started task**, it is refreshed daily at **CKFREEZE Collect time**.

CKFREEZE Collect time
Specifies the time of day at which the Collect started task must be started. The value 0000 is used to signify that the zSecure Collect for z/OS started task must not be started at all.

CKFREEZE Collect time corresponds to the OPTION COLLECTTIME. See the description of the **CollectTime** field in the OPTION command section of the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Extended Monitoring
This field determines whether the Extended Monitoring process is active. If you specify YES, Extended Monitoring is activated. It results in a system snapshot being taken and written to a CKFREEZE data set at the interval specified in the **Environment refresh** field. This option is effective only if

Extended Monitoring alerts are selected. If no Extended Monitoring alerts are selected, a warning message is issued during the verification process.

Snapshot retention
Specifies the retention period for the Extended Monitoring snapshot data sets. Snapshot data sets older than the specified period are automatically deleted. The retention period is specified in hours. The value must be in the range 1 through 99, inclusive. The default value is 24 hours. The main reason to retain snapshot data sets is that you can analyze the details for generated alerts.

Skeleton
This member contains the global CARLa statements, such as ALLOCATE, DEFTYPE, and DEFINE statements. You need this option if you defined your own Alert conditions. See "Installation defined alerts" on page 27. Normally, however, you use the provided C2PSGLOB member.

Alert configuration: specifying alert destinations

You can select the Alert Destination panel from the **W** (Who/Where) line command on either the Alert Configuration overview panel or one of the alert selection panels. In this panel, you can specify where you want alerts to be sent. Using the **W** line command, you can specify Alert destinations separately for each of the following alert types:

- An Alert configuration
- An Alert category
- An individual alert.

This panel can be shown automatically if you use the Copy or Insert function on the Alert Configuration overview panel. It is shown after you complete the General Settings from END, or PF3.

You can have alert messages sent to multiple destination types by selecting more than one destination type on this panel. Each destination type can have its own destinations.

When all destination types are selected, the panel displayed looks like the following screen:

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


Select the alert destination
/  E-mail
   _  Write e-mails to C2RSMTP DD

   Specify e-mail recipient(s)
   From . . . . . . . &jobname at &system <mbox@domain>_______________

   Mail to  . . . . . ____________________________________________________
   (You may specify : to receive a list of defined recipients :setname.fields)

   CC . . . . . . . . ____________________________________________________
   BCC  . . . . . . . ____________________________________________________
   Reply to . . . . . ____________________________________________________
   Output format  . . 1  1. Normal (MIME/HTML)
                         2. Plain text (formatting may be lost)
       Font size  . . . . _  (number in range 1-7)

/  Text message to cell phone
   _  Write text messages to C2RSMTP DD

   Specify text message/cell phone recipient
   From . . . . . . . &jobname at &system <mbox@domain>_______________

   Phone@gateway  . . ____________________________________________________
   (You may specify : to receive a list of defined recipients :setname.fields)

   Reply to . . . . . ____________________________________________________

/  SNMP
   _  Write SNMP traps to C2RSNMP DD

   Specify SNMP receiver address(es) (multiple addresses in parentheses,
   separated by a comma)
   Address  . . . . . ____________________________________________________

/  UNIX syslog
  _  Write messages to C2RSYSLG DD

    Specify UNIX SYSLOG address(es) (multiple addresses in parentheses,
    separated by a comma)
    Address(es)  . . . ____________________________________________________

/  WTO
   _  Write WTOs to C2RWTO DD

_  Reset all existing destination settings for this Alert Configuration
```

Figure 6. Setup Alert panel: Specifying destination types

When your screen size is 24 x 80, you must scroll down to see all fields.

The **Mail to** and **Phone@gateway** fields on this panel accept email addresses in several formats. You can specify the email addresses as:

- One or more email addresses of the form `auditor@mydomain.com` separated by commas (,).
- If the email addresses are contained in a data set and the data set has no other data in it, not even line numbers, you can use ***//data_set_name***.
- If you have defined an email destination, you can refer to it from:***destination-name.field-name***.

If you do not know the names of your email destinations, or the field names that you have used, use a single colon (:) to request information. A panel is displayed with a selection list of the defined email destinations and their defined fields.

The following fields are displayed in the **Email** section:

Email Send the alert as email.

Write emails to C2RSMTP DD
When both this field and **email** are tagged, the generated emails are not sent, but written to the C2RSMTP DD. You can use this option when you define your own alert conditions. If you are not sure how many alerts are generated, this option ensures that you are not flooding the intended recipient with alert emails.

From The "From" email address. This address is added to the "From:" header.

You can use the variables `&jobname` and `&system`, that is, SMF system ID, as part of the phrase, but not in quotation marks. For example, use `&jobname` at `&system<mbox@domain>`. These variables are case-sensitive. `&SYSTEM`, `&system` and `&System` are allowed, but no other variations.

Mail to
Enter the destination email address. For information about the specification of email addresses, see the information earlier in this section about "Mail to" and "Phone" specifications.

CC Enter email addresses, separated by commas, for those recipients that are to receive a copy of the email.

BCC Enter email addresses, separated by commas, for those recipients that are to receive a blind carbon copy of the email. These addresses are not displayed on the recipient list.

Reply to
The address or list of addresses to be set in the email "Reply-To" header.

Output format
This option can be used to specify the method that is to be used to format the report. The supported options are:

Normal
Use MIME/HTML email with limited HTML encoding.

Plain text
No special formatting is done. This means that no MIME/HTML encoding is performed.

Font size
This sets the HTML font size used for email. The default is 1. The HTML font size is a number in the range 1 - 7. It corresponds to 8, 10, 12, 14, 18, 24, and 26 point size if the browser default font is set at 12 point. The user can change that.

The following fields are displayed in the text message section:

Text message to cell phone
Send the alert as a text message to a mobile phone or a pager.

Write text messages to C2RSMTP DD
When both this field and **Text message to cell phone** are tagged, the generated text message is not sent, but written to the C2RSMTP DD. You can use this option when you define your own alert conditions. If you are

not sure how many alerts can be generated, this option ensures that you are not flooding the intended recipient with alerts.

From, Reply to
These fields are analogous to the **From** and **Reply to** fields in the email section.

Phone@gateway
The phone or text pager address as <phone number>@<gateway>. See also the field description for Mail to.

The following fields are displayed in the SNMP section:

SNMP
Send the alert as an SNMP trap. The field SNMP destination must be specified.

Write SNMP traps to C2RSNMP DD
When both this field and **SNMP** are tagged, the generated SNMP traps are not sent, but written to the C2RSNMP DD in symbolic form; that is, the `sortlist` output is written, and not the actual ASCII trap. This field is meant for testing purposes.

Addresses
When **SNMP** is selected, you must use this field to specify where SNMP traps are sent. The destination can be a name (looked up by DNS), an IP address, or a list separated by commas. Each destination can be followed by a colon and a port number in decimal form.

The following fields are displayed in the UNIX syslog section:

UNIX syslog
Send the alert to the UNIX syslog

Write messages to C2RSYSLG DD
When both this field and UNIX syslog are selected, the generated alert message is not sent to the UNIX syslog, but written to the C2RSYSLG DD. This field is meant for testing purposes.

Addresses
When UNIX syslog is selected, you must use this field to specify where alert messages are sent. The destination can be a name (looked up by DNS), an IP address, or a list separated by commas. Each destination can be followed by a colon and a port number in decimal form.

The following fields are displayed in the WTO section:

WTO Generate a WTO for the alert.

Write WTOs to C2RWTO DD
When both this field and **WTO** are tagged, the generated WTO is not sent to the console, but written to the C2RWTO DD. This field is meant for testing purposes.

The **Reset all existing destination settings for this Alert Configuration** option resets all destination settings for the individual alerts. This option is available only on the Alert Configuration level.

Alert configuration: selecting alert categories

You can select this panel by using the **S**(elect) line command on an Alert configuration.

This panel is shown automatically if you do Copy or Insert on the Alert Configuration overview panel. It is shown after you complete the Alert destination panel through END or PF3.

```
  Menu Options Info Commands Setup
                        zSecure Suite - Setup - Alert   Row 1 to 8 of 8
Command ===> _____________________________________________ Scroll ===> CSR

Select the alert category you want to work with
The following line commands are available: W(Who/Where), S(elect)
-------------------------------------------------------------------------------
    Id  Category                                #alerts        #selected
S   1   User alerts                            15             0
_   7   Group alerts                           1              0
_   2   Data set alerts                        6              0
_   3   General resource alerts                3              0
_   4   UNIX alerts                            8              8
_   5   RACF control alerts                    3              0
_   6   System alerts                          2              0
    0   Other alerts                           1              0
****************************** Bottom of data ********************************
```

Figure 7. Setup Alert panel: Selecting Alert categories

This panel shows the available Alert categories. The following fields are displayed:

Id The report category ID. The second position of the alert ID is used to determine the category.

Category
The zSecure Alert report category. Currently, the following categories are defined:

- User alerts
- Group alerts (only on RACF systems)
- Data set alerts
- General resource alerts
- UNIX alerts
- RACF (or ACF2) control alerts
- System alerts
- Other alerts

#alerts The number of defined alerts in this category.

#selected
The number of selected alerts in this category.

You can use the **W** (that is, Who or Where) line command to specify a destination for all alerts in this category. Destinations set on the individual alert level for alerts in this category are then discarded.

The **S**(elect) command displays all alerts in the category. For example, on RACF systems, the alerts display looks like the following screen:

```
  Menu         Options       Info    Commands     Setup
_______________________________________________________________________________
                        zSecure Audit for RACF - Setup - Al Row 1 to 13 of 15
Command ===> _____________________________________________ Scroll ===> CSR

User alerts
Select the alert you want to work with.
The following line commands are available: A(Preview), C(opy), D(elete),
E(dit), I(nsert), W(Who/Where),S(elect), U(nselect), B(rowse)
-------------------------------------------------------------------------------
    Alert                                          Id    Sel  gECSWU  CA  EM
_   Logon by unknown user                          1101  No   g    U  __  N
_   Logon with emergency userid                    1102  No   g    U  Y   N
_   Logon of a userid with UID(0) (Unix superuser) 1103  No   g    U  __  N
_   Highly authorized user revoked for pwd violatio 1104 No   g    U  __  N
_   System authority granted                       1105  No   g    U  __  N
_   System authority removed                       1106  No   g    U  __  N
_   Group authority granted                        1107  No   g    U  __  N
_   Group authority removed                        1108  No   g    U  __  N
_   SPECIAL authority used by non-SPECIAL user     1109  No   g    U  __  N
_   non-OPERATIONS user accessed data set with OPER 1110 No   g    U  __  N
_   Invalid password attempts exceed limit         1111  No   g    U  __  N
_   Password history flushed                       1112  No   g    U  __  N
_   Suspect password changes                       1113  No   g    U  __  N
****************************** Bottom of data ********************************
```

Figure 8. Setup Alert panel: Display of alerts in the selected category

On ACF2 systems, the alerts display looks like the following screen:

```
Menu Options Info Commands Setup
_______________________________________________________________________________
         zSecure Suite - Setup - Alert                      Row 1 to 11 of 11
Command ===> _____________________________________________ Scroll ===> CSR

User alerts
Select the alert you want to work with.
The following line commands are available: A(Preview), C(opy), D(elete),
E(dit), I(nsert), W(Who/Where),S(elect), U(nselect), B(rowse)
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
    Alert                                          Id    Sel  gECSWU  CA  EM
_   Logon with emergency logonid                   2102  Yes  gE      Y   N
_   Highly authorized user revoked for pwd violatio 2104 No   gE      __  N
_   System authority granted                       2105  No   gE      __  N
_   System authority removed                       2106  No   gE      __  N
_   Invalid password attempts exceed limit         2111  No   gE      __  N
_   Password history flushed                       2112  No   gE      __  N
_   Suspect password changes                       2113  No   gE      __  N
_   Too many violations                            2115  No   gE      Y   N
_   non-SECURITY user accessed data set with SECURI 2116 No   gE      __  N
_   non-NON-CNCL user accessed data set with NON-CN 2117 No   gE      __  N
_   non-READALL user accessed data set with READALL 2118 No   gE      __  N
****************************** Bottom of data ********************************
```

Figure 9. Setup Alert panel for ACF2 systems: Display of alerts in the selected category

The following fields are displayed:

Alert A description of the alert.

Id A numeric ID for the alert. IBM alert IDs use range 1000-1999. The range 4000-4999 is reserved for installation defined alerts. The ID is used to generate the skeleton member name, the WTO output message number, and the SNMP trap number.

Sel Indicates whether this alert is selected.

gECSWU
The Destination Types for this alert as set with the W line command. The following values can be displayed:

E email **C** Cell phone (text message) **S** SNMP trap **W** WTO **U** UNIX syslog

The value can be prefixed with **g**, which means the destination has been set globally by the **W** line command on an Alert configuration.

C Flag indicating whether this alert allows configuration to reflect items such as installation-specific names. When the alert is selected, a panel is displayed so that configuration can be performed. See "Predefined alert configuration" on page 95.

A Flag indicating whether this alert is configured to generate an action command.

EM Flag indicating whether this alert is an Extended Monitoring alert that requires activation of Extended Monitoring in the Alert Configuration general settings panel. For more information about Extended Monitoring alerts, see Chapter 1, "Introduction," on page 1 and "Alert activation guidelines" on page 5.

The following line commands are available:

Table 3. Line commands available on the Alert list display

A	**Preview CARLa code**. This action displays the generated CARLa for this alert in ISPF BROWSE mode.
C	**Copy alert**. This action displays the alert definition panel with all fields. These fields are copied from the selected alert, except for the field ID, which must be unique for each alert.
D	**Delete the selected alert**. IBM Security zSecure defined alerts cannot be deleted.
E	**Edit alert**. Specify the alert characteristics such as the alert ID, record types, and CARLa code.
I	**Insert new alert**. This action displays the alert definition panel with all fields blank. When all required fields are entered, a new alert is added.
W	**Who/Where to alert**. Destinations can be email addresses, text message/cell phone receivers, SNMP addresses, UNIX syslog addresses, and WTO formats. When all destinations for an alert are cleared, the destinations of the alert category are used. If the destinations of the alert category are also not set, the destinations of the Alert Configuration are used.
S	**Select alert**. After verification and refresh of the Alert Configuration, this alert is reported.
U	**Unselect alert**. After verification and refresh of the Alert Configuration, this alert is no longer reported.
B	**Browse Alert definition**. This action displays the alert definition and also allows you to specify an action command. See "Alert definition - specify action" on page 96.

See "Installation defined alerts" on page 27 for information about using the C(opy) or I(nsert) line commands to add alerts.

Alert configuration: verifying alert configuration

You can request verification by using the **V**(Verify) line command on an Alert configuration.

This panel can be shown automatically if you do Copy or Insert on the Alert Configuration overview panel. It is shown after you complete selecting the alert conditions.

```
  Menu   Options   Info   Commands   Setup   Startpanel
------------------------------------------------------------------------------
                        zSecure Admin+Audit for RACF - Setup - Alert
Command ===> ____________________________________________________________

   Use SETUP FILES input instead of zSecure Alert input data
_The following selections are supported:
B Browse file           S Default action (for each file)
V View file

Enter a selection in front of a highlighted line below:

   AHJBVS       Stage one member
   AHJBVO       Environment dependent selection criteria
   AHJBV        zSecure Alert report member
   AHJBVE       zSecure Alert extended monitor member
   AHJBVP       zSecure Alert parameter member

Press Enter to start Alert set verification
```

Figure 10. Setup Alert panel: Verifying the Alert configuration

If you select the option **Use SETUP FILES input instead of zSecure Alert input data**, the verification process uses the SETUP FILES-selected input set instead of the security database and CKFREEZE data set configured for this alert set.

Note: This option applies only to the verification function. The Alert address space always uses the security database and CKFREEZE data set as configured.

After you press **Enter**, the same panel shows the results of the verification process. You can browse or view the members that were created by the verification process. When an error is detected during verification, the file that contains the error is highlighted in red. To view the CARLa output of the successful "Alert Generation" verification process, you can use the SYSPRINT primary command. Because no SMF and WTO records are provided during the verification process, no actual alerts are generated.

The following members are created by the verification process:

<configuration-name>VS
: The verified zSecure Alert stage1 member. This member contains the CARLa commands used to generate system-dependent CARLa selection statements used during the alert analysis. When the **F** line command is issued, this member is copied to member **<configuration-name>S**. For information about the function of the stage1 member, see the sections about the Alert address space in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

<configuration-name>VO
: This member contains the environment-dependent selection criteria used during analysis and generated by the stage1 member. This member is only used by the user interface, so the zSecure Alert report member can be verified. The zSecure Alert started task writes this stage1 output to the C2P1OUT DD.

<configuration-name>V
The verified zSecure Alert report member. This member contains the main (primary) CARLa commands used to analyze the captured records. When the **F** line command is issued, this member is copied to member **<configuration-name>**.

<configuration-name>VE
The verified zSecure Alert report member for Extended Monitoring alerts. This member contains the CARLa commands used to compare the latest two CKFREEZE snapshot data sets. When the F line command is issued, this member is copied to the member **<configuration-name>E**.

<configuration-name>VP
This member contains the zSecure Alert parameters. When the **F** line command is issued, this member is copied to parameter member **<configuration-name>P**. This member is allocated by the PARMLIB DD in the started task JCL.

Alert configuration: refreshing the alert configuration

About this task

A refresh of your alert configuration copies the verified members in the configuration data set to production members.

Procedure

1. Select this panel by using the **F** (Refresh) line command on an Alert Configuration.

   This panel displays automatically if you do Copy or Insert on the Alert Configuration overview panel at the end of verification processing.

   During the Refresh step, the verified members in the configuration data set is copied to production members. After a successful copy, the following confirmation panel is displayed:

```
            zSecure Suite - Setup - Alert

Production members generated. Use '/' to issue a refresh
command for the current system. The selected alerts will then
be reported.

_  Refresh Alert started task


Enter to continue
```

Figure 11. Setup Alert panel: Refreshing the Alert configuration

2. In this panel, specify that a REFRESH command must be issued to the started task.

   If the JCL of the started task (PARMLIB DD-statement) is configured to use the current Alert configuration, the REFRESH command instructs the started task to reprocess the new members.

3. You can use '/' to issue an MVS MODIFY C2POLICE,REFRESH command.

   When you leave the Refresh panel by pressing PF3, the Alert configuration panel displays again. If all configuration steps complete successfully, the status shows OK.

Email address lists (SE.A.E)

In zSecure Alert, you can use email address lists to mail alert messages to multiple people. You can do that from direct specification of a list of comma-separated email addresses in the various panels. The email option provides an alternative approach. From the option email, you specify a data set and how email addresses are to be extracted from each record. Use the term email destination to differentiate this from the list of comma-separated email addresses. The email destination referenced by its name can be used in the **Mail to** field of an alert. For details, see the field description for Mail to.

Note: Changes made to the alert configuration are not permanently saved until you leave option SE.A.E.

If you are a first time user of zSecure Alert, you can skip this configuration step. If you later need more flexible email addresses, revisit this section and create the required email destinations.

The first time you enter this option, the following panel is displayed:

Note: As an example, most of the fields are already completed.

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

Enter zSecure Alert definition for e-mail destinations
Name  . . . . . . . . . . SECADM
Description . . . . . . . Security administrator e-mail addresses


Enter / to edit the e-mail destination data set
/  Data set name     'C2P.DATA.MAIL(SECADM)'

Field definitions
Field name        Start   Length||Word  Delimiter
secadmin userid   ______  ______  1     ;
e-mail address    ______  ______  2     ;
```

Figure 12. Setup Alert panel: Specifying email destinations

The panel has the following fields:

Name A short descriptive name for this email destination. This field is required and must be unique. You use this name during the Alert configuration to refer to this email destination.

Description
A description for the email destination. This field is required.

Data set name
The data set containing the email addresses. It can be a sequential data set, or a partitioned data set, with the member name enclosed in parentheses: 'C2P.DATA.MAIL(SECADM)', for example. Use a partitioned data set, preferably PDS/E, because the data set is allocated (with DISP=SHR) by the zSecure Alert address space. A sequential data set requires an exclusive enqueue for edit. You would never obtain it when the started task had allocated it, and a PDS needs exclusive enqueue when you need to compress it.

Any change to the member takes effect at each F C2POLICE,REFRESH and at each environment refresh interval; default is 60 minutes.

Field name
A field name such as **e-mail address**.

When the data set consists of just email addresses but has line numbers, use the **Start** and **Length** fields to define the email address field. For example, for an FB 80 data set, enter 1 for **Start** and 72 for **Length**.

If the data set contains other information besides the email address, you need the Field Name to identify which part of the record is the email address you want to use.

During the alert configuration, you can refer to this field by specifying `:destinationname.fieldname`.

Start Enter the numeric start position of the field. For example, enter 1 to start directly at the leftmost character. This field is used with the **Length** field to extract the email address from the data set.

This field is mutually exclusive with the fields **Word** and **Delimiter**.

Length
The length of the field. This field is used with the **Start** field.

This field is mutually exclusive with the fields **Word** and **Delimiter**.

Word The sequence number of the "word" wanted. This field is used with the **Delimiter** field to extract the email address from the data set.

This field is mutually exclusive with the fields **Start** and **Length**.

Delimiter
The character used to separate the words from each other. Examples are ";" or a space. This field is used with the **Word** field.

This field is mutually exclusive with the fields **Start** and **Length**.

By entering a "/" before the data set name, it is possible to view or edit the email destination set. With the data as shown in Figure 12 on page 25, the data set layout would be:

```
  File  Edit  Confirm  Menu  Utilities  Compilers  Test  Help
------------------------------------------------------------------------------
EDIT       C2P.DATA.MAIL(SECADM)                          Columns 00001 00072
Command ===> _____________________________________________ Scroll ===> CSR
****** ***************************** Top of Data ******************************
000001 C2PSA01;JohnBrown@company.com;
000002 C2PSA02;MarkTyler@company.com;
000003 C2PSA03;SteveJohnson@company.com;
000004 C2PSA04;KarenJones@company.com;
****** **************************** Bottom of Data ****************************
```

Figure 13. Panel for viewing or editing the email destination set

When the Email Destination has been saved by pressing END, the following panel is displayed. This panel provides an overview of the available email destinations, and enables you to manage them. In the following example, only one email destination has been defined.

```
 Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                        zSecure Suite - Setup - Alert     Row 1 from 6
Command ===> _____________________________________________ Scroll ===> CSR
CKRM839 E-mail destination added
Select Alert e-mail destination
The following line commands are available: B(rowse), C(opy), D(elete),
E(dit set), I(nsert), S(elect), V(iew)
------------------------------------------------------------------------------
    Set name  Description
              Data set name
_   SECADM    Security administrator e-mail addresses
              'C2P.DATA.MAIL(SECADM)'
------------------------------------------------------------------------------
****************************** Bottom of data ********************************
```

Figure 14. Setup Alert panel: Save Confirmation message for email destination update

The following line commands can be used on the email destination set overview panel:

Table 4. Line commands available on the email destination set overview panel

Line Command	Description
/	Display a popup panel showing the available line commands.
C	Copy the Email Destination. This action displays the definition panel as shown in Figure 12 on page 25 with all fields. These fields are copied from the selected Email Destination, except for the field **Name**, which must be unique for each Email Destination.
D	Delete the Email Destination. This action does not affect any associated data set.
I	Insert a new Email Destination. This action displays the definition panel with all fields blank.
S	Select the General Settings for this Email Destination for modification.
B	Browse the data set with the ISPF BROWSE service.
E	Edit the data set with the ISPF EDIT service, so email addresses can be modified.
V	View the data set with the ISPF VIEW service.

Installation defined alerts

New alerts can be created by copying and adapting an existing alert or by creating an alert from scratch.

The specification of an alert is largely done by a number of CARLa code sections in a skeleton member. This skeleton member is used during the Verify operation to create the actual CARLa to be passed to the zSecure Alert engine. In general, it requires advanced CARLa coding skills. This knowledge is assumed throughout this section. See the*IBM Security zSecure Admin and Audit for RACF: User Reference Manual* for details.

When creating an alert, you must decide on the following items:

- The alert ID. This four-digit number serves as an identifier and is always prominently present. IBM-supplied alerts have alert numbers 1000-1999 (RACF), 2000-2999 (ACF2), and 3000-3999 (TSS). The ranges 4000-4999 (RACF), 5000-5999

(ACF2), and 6000-6999 (TSS) are reserved for installation-defined alerts. The second digit of this number assigns the alert to an Alert Category.

- The event that you want to trigger your alert.
- How to format relevant data from the Alert condition into your alert.
- Whether your alert is customizable.

  For instance, your alert might need a list of data sets or user IDs. You want to maintain this list without the need to edit the skeletons each time. If you want your alert to be customizable, you must have a panel to allow customizing it.

  It is up to you how the panel looks and which parameters it accepts to customize your alert. You can create a panel from scratch, or you can use, copy, or clone a standard zSecure panel that fits your requirements. If you need a panel of your own, you must store it in a library of your own. You must use the UPREFIX/WPREFIX zSecure configuration parameters to make that library available to ISPF. See *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide* for the UPREFIX/WPREFIX parameters.

  To supply your skeletons with the parameters they need to generate the CARLa for your alert, you must assign the names of these parameters to a variable named EXTVAR; that is:
  &extvar='c2peeus0,c2peeus1,c2peeus2,c2peeus3,c2peeus4'

The format in which an alert is to be sent is specified per Destination Type. There are the following Destination types:

- Email
- Text message
- WTO
- SNMP trap
- UNIX syslog

The email format is the most descriptive. The alerts provided with the product have a common layout, described in “Standard email layout” on page 42. The emails are sent in HTML format.

The text message format in all IBM Security zSecure-supplied alerts is a shortened version of the email format for use with an e-mail-to-text-message gateway where the recipient (for example, cell phone or pager) is specified in the "To" header of the email message. The text message itself can be taken from the subject or the body of the email, depending on the gateway. The subject and body as sent are therefore similar, though the body can contain a little more information.

The WTO format can be used with automated operation software.

The SNMP trap format can be used with IBM Tivoli Compliance Insight Manager or Tivoli Security Information and Event Manager or your network console. For more description of this format, see Appendix A, “SNMP output,” on page 107.

Specifying the alert ID and data source

Procedure

Follow these steps to create an alert:

1. To create an alert, go to the option SE.A.A and select the Alert Configuration you want to work with.
2. In the Alert Category panel, select any category; for example **System alerts**.

The category to which the new alert belongs is determined by its second digit, and not by which category you use to create it.

```
  Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                        zSecure Suite - Setup - Alert  Row 1 to 1 of 1
 Command ===> _____________________________________________ Scroll ===> CSR

 System alerts
 Select the alert you want to work with.
 The following line commands are available: A(Preview), C(opy), D(elete),
 E(dit), I(nsert), W(Who/Where), S(elect), U(nselect), B(rowse)
------------------------------------------------------------------------------
    Alert                                          Id    Sel  gECSW  C EM
I   SMF data loss started                          1601  Yes  gE W     N
_   SMF logging resumed after failure              1602  Yes  gE W     N
_   SVC definition changed                         1603  No   gE W     Y
 ****************************** Bottom of data ********************************
```

Figure 15. Setup Alert panel: Specifying Alert ID and data source for custom Alerts

3. You can create an alert by issuing the **C**(Copy) or **I**(Insert) line command. The Copy command copies all fields except the Alert Id.

   The following panel is displayed after issuing the **I** line command:

```
  Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                        zSecure Admin+Audit for RACF - Setup - Alert
 Command ===> ____________________________________________________________

 Description  . . ____________________________________________________________
 Member prefix    ___
 Alert id. . . .  ____  Severity. . . . _  (I, W, E or S)
 Data source  . . SMF ____________________
 Parameters . . . ____________________________________________________________
 Panel name . . . ________  (Panel for additional customization)

 Specify SMF records to be collected for this alert
 Type Sub    Type Sub    Type Sub    Type Sub    Type Sub
 ____ ___    ____ ___    ____ ___    ____ ___    ____ ___

 Specify WTO filters for this alert
 Prefix    Prefix    Prefix    Prefix    Prefix

 ________  ________  ________  ________  ________
 Allowable destination types   _  E-mail    _  Cellphone    _  SNMP     _  WTO
                               _  UNIX syslog               _  Action command
 Specify action  . . . . . . . N  (Y/N)
 Extended Monitoring alert . .  _  (Y/N)
 View/edit the alert skeleton   _  ISPF Skeleton
```

Figure 16. Setup Alert panel: Adding an Alert

The following fields are displayed:

Description
A description of the alert.

Member prefix
A three-character prefix for the skeleton member. The generated name of the skeleton member is: **<Member prefix>S<Alert id>**. The three-character prefix must start with a letter or "@", "#", or "$", and not with a numeric digit.

Prefix `C2P` is reserved for IBM Security zSecure use.

Alert id

A numeric ID for the alert. IBM alert IDs use ranges 1000-1999 (RACF), 2000-2999 (ACF2), and 3000-3999 (TSS). The ranges 4000-4999 (RACF), 5000-5999 (ACF2), and 6000-6999 (TSS) are reserved for installation defined alerts. The second digit determines the Alert category. The ID is used to generate the skeleton member name.

When WTO is selected as a Destination type, the value is also used to populate the **<Alert id>** field in the message ID: **C2P<Alert id><Severity>**.

Severity

A severity for the alert. When WTO is selected as a Destination type, this value is used to populate the **<Severity>** field in the message ID: **C2P<Alert id><Severity>**

The following list shows the valid severities:

I Information. Action is not required.

W Attention. Action might be required.

E Error. Action is required.

S Severe error. Action is required urgently.

For alerts with destination type UNIX, these severities are translated as shown in the following list:

Severity	**Priority**
I	117
W	116
E	115
S	114

Data source

The data source of CARLa newlist type for the alert, `SMF` or `WTO` for example.

Parameters

This field is intended to pass additional parameters to the generated NEWLIST statement. For Extended Monitoring alerts, the required COMPAREOPT=<compareopt-name> must be entered in this field.

Panel name

If you want your new alert to be customizable, specify the name of the customizing panel in this field. The panel you specify must exist and be accessible, either as a standard zSecure panel if there is one that fits your requirements, or as a panel that you created yourself. This panel is shown as the next transaction during creation of the new alert. It can also be used for future configuration of this alert.

Type If the data source is SMF: the SMF record type that must be collected for this alert. To collect ACF2 records, you can specify the pseudo-type ACF2. The zSecure Alert program looks up the correct record type from the ACF2 control blocks.

Sub Specifies the SMF-record subtype that must be collected. The subtype is

only used for SMF-record types 30, 80, and ACF2 records. For all other SMF-record types, the subtype is ignored. The subtype is interpreted as follows:

Rectype 30 The subtype is the standard SMF-record subtype.

Rectype 80 The subtype is the RACF event code. For a complete list of RACF event codes, see the RACF Auditor's guide.

Rectype ACF2 See *IBM Security zSecure Audit for ACF2: User Reference Manual* for a complete list of ACF2 subtypes.

Prefix
If the data source is WTO: specifies which message prefixes must be collected.

Allowable destination types
Select the Destination Types for which reports can be generated by this alert. The alert skeleton must have a section for each Destination Type selected.

Specify action
Select **Y** to specify an action command for this alert. See "Alert definition - specify action" on page 96.

Extended Monitoring alert
This field specifies whether the alert is an Extended Monitoring alert. Specify **Y** if it is an Extended Monitoring alert that compares the current and previous CKFREEZE snapshot data sets. Specify **N** if it is an Event-based alert. Ensure that the **Data Source** field specifies the correct value to match the Extended Monitoring setting. For event-based alerts, the **Data Source** field must have the value SMF or WTO. For Extended Monitoring alerts, the **Data Source** field can have the value of any supported CKFREEZE-based NEWLIST type. See "Alert activation guidelines" on page 5 for more information about Extended Monitoring alerts.

ISPF Skeleton
Type a forward slash (/) in this field to edit the ISPF skeleton for this alert. The skeleton contains the CARLa code to specify the Alert Condition, the alert contents, and the alert layout.

When you add an alert using the Copy command, the skeleton of the source alert is copied; otherwise a model skeleton is used. If the skeleton exists, it is not changed.

For Extended Monitoring alerts, only the selection criteria, the alert contents, and the alert layout are specified in this ISPF Skeleton. You must also add the required CompareOpt statements at the bottom of the Global CARLa Skeleton, similar to the default CompareOpt statements that are already present. You specified the name for the required CompareOpt statement in the **Parameters** field, described earlier in this list.

For example, to define an alert to be triggered on the event that the APF list is updated by the SETPROG command:

```
  Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Admin+Audit for RACF - Setup - Alert
Command ===> ____________________________________________________________

Description  . . APF List changed using SETPROG command_____________________
Member prefix    AHJ
Alert id . . . . 4000  Severity . . . . W  (I, W, E or S)
Data source  . . WTO_____________________
Parameters . . . ____________________________________________________________
Panel name . . . ________  (Panel for additional customization)

Specify SMF records to be collected for this alert
Type Sub    Type Sub    Type Sub    Type Sub    Type Sub

____        ____        ____        ____        ____

Specify WTO filters for this alert
Prefix    Prefix    Prefix    Prefix    Prefix
CSV410I   ________  ________  ________  ________
Allowable destination types   /  E-mail    _  Cellphone   _  SNMP    _  WTO
                              _  UNIX syslog
 Extended Monitoring alert . .  _  (Y/N)
View/edit the alert skeleton  /  ISPF Skeleton
```

Figure 17. Setup Alert panel: Defining an Alert

CARLa skeleton for existing alerts

You can edit the CARLa skeleton of an existing installation-defined alert. Tag the **ISPF skeleton** option in the panel you reach with the **E**(Edit) line command on an individual alert. If you perform this action on an IBM Security zSecure-supplied alert, you get an ISPF VIEW session instead. You reach the same panel with the **B**(Browse) line command.

When adding an alert with the **C**(Copy) or **I**(Insert) line commands, you reach the panel where you can tag that option. In that case, the skeleton member does not normally exist yet. For Copy, it is then copied from the skeleton member of the copied alert. If the copied member defines local pre-selection filters, their names must be changed in the copy to avoid name clashes. The names are supposed to end in the alert ID. For Insert, you get an "empty" skeleton member.

The information in the rest of this section is based on the "empty" skeleton member. In any case, you must see seven sections with CARLa code. The first two sections specify the Alert Condition. The next four sections specify the alert message format for the various Destination types. The last section specifies a possible command to be issued when the Alert Condition is raised.

The CARLa sections in the skeleton are each marked with an identifying comment line as follows:

)CM Pass one query

Here you can specify a two-pass CARLa query for the stage1 member. Use it if your Alert Condition depends on the environment. During the stage1 step of this query, its output is used as a prefix for the reporting step. This output is a one-pass CARLa query populated with current environmental values. It enables you to generate a pre-selection based on the actual environment. Your Alert Condition can refer to this pre-selection. The pre-selection is adapted with each environmental refresh run. Normally, it is one time per hour. See “Alert configuration: specifying general settings” on page 12.

)CM Alert condition
Specify the Alert Condition that you want to trigger your alert. For Extended Monitoring alerts, it requires only a selection of the complex, for example, `select complex=(base, current)`. The fields that determine which records trigger the alert are specified in the CompareOpt statement defined in the Global CARLa Skeleton.

)CM Action command
Here you can specify the following to embed statements to be able to specify an action command:

```
)IM C2PSACTX
)IM C2PSACTS
```

See "Alert definition - specify action" on page 96.

)CM EMAIL sortlist
Here you can specify the alert message in the layout to be used for email destinations.

)CM Cellphone sortlist
Here you can specify the alert message in the layout to be used in text messages. Whether the text message as received is taken from the subject or the body of the email depends on the e-mail-to-text-message-gateway you use. All IBM Security zSecure-supplied alerts send a similar message in both subject and body.

)CM SNMP sortlist
Here you can specify the alert message in the layout to be used for SNMP destinations.

)CM UNIX syslog sortlist
Here you can specify the alert message in the layout to be used for SYSLOG destinations.

)CM WTO sortlist
Here you can specify the alert message in the layout to be sent to the console.

)CM Command
Here you can add a command to be issued when the condition occurs.

You do not need to specify message formats that you do not want to use. However, you can keep at least the alert ID in each section so that you can recognize the alert if it ever gets used in that format. The alert ID parts can be recognized by the occurrence of the `&c2pemem.` skeleton variable.

Each actual CARLa section is bounded by)SEL and)ENDSEL skeleton directives. The stage1 section also has an)IM directive. Do not change these directives.

The next manual sections explain each CARLa section in detail. When you are done changing the skeleton, return to the alerts panel by pressing PF3. If you add an alert, it is selected automatically. Pressing PF3 twice more, you can return to the Alert Configuration panel, where you can then issue the **V**(Verify) command to check the new alert. If the verification is successful, you can enter the **F**(Refresh) command to activate the new alert.

Environment-dependent selection

You must enter the **)CM Pass one query** section if you want to use environment-dependent selection criteria in your Alert Condition.

The following example is from skeleton member C2PS1204 for IBM Security zSecure-supplied alerts 1204 and 2204. It shows a stage1 query that asks the system what data sets are currently part of the APF list, that is, the DSN field and APF flag field of NEWLIST TYPE=SENSDSN. For more explanation, see *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*. These data set names are substituted into another CARLa query. This query is otherwise contained in quotation marks and thus literally copied to the output file to become the start of the reporting step query.

```
  )CM Pass one query
  )SEL &C2PEPASS = Y
  n type=system outlim=1 nopage
  sortlist,
    "n type=smf name=uapf1204 outlim=0" /,
  )SEL &C2PESECP = RACF
    " select event=access(allowed) intent>=update likelist=recent," /,
  )ENDSEL
  )SEL &C2PESECP = ACF2
    " select likelist=recent acf2_subtype=D," /,
    " acf2_access=(OUTPUT,UPDATE,INOUT,OUTIN,OUTINX)," /,
  )ENDSEL
n type=sensdsn nopage
  select apf
  sortlist,
    "           " dsn(0) | ","
  n type=system outlim=1 nopage
  sortlist,
    "            )" /,
    " sortlist ''"
  )ENDSEL
```

The generated query is named UAPF1204 by the NAME keyword on the generated N (Newlist) statement. It allows the Alert Condition to refer to it. The NAME ends in the alert ID to avoid name clashes with filters specified in other alerts.

The generated query is meant as a pre-selection only, and thus specifies OUTLIM=0, meaning that no output must be generated. The pre-selection is for SMF records for `event=access(allowed) intent>=update` on RACF systems. Or, it is for `acf2_subtype=D ACF2_ACCESS=OUTPUT` on ACF2 systems and for the APF data sets obtained from the system.

The LIKELIST=RECENT clause further restricts the selection to the SMF records written during the current reporting interval. The following section explains about the pre-selection filters that are always available to specify what SMF and WTO input data to tie the selection to.

Alert condition

You must complete the **)CM Alert condition** section to indicate when you want to issue the alert. The following example is taken from skeleton member C2PS1204 for IBM Security zSecure-supplied alerts 1204 and 2204. The entire selection has already been done in a pre-selection named UAPF1204 that was generated by the environment-dependent selection for that alert as shown in the previous section.

```
)CM Alert condition
)SEL &C2PEPASS = N
)IM C2PSGNEW
  select likelist=uapf1204
```

Skeleton member C2PSGNEW embedded by the)IM directive generates the CARLa NEWLIST statement for selection criteria. After the)IM statement, you can enter DEFINE and SELECT statements.

The LIKELIST keyword refers to a preceding NEWLIST that has a NAME keyword with the same value. It means that the effective selection from that NEWLIST is to be used as a clause. In this case, it is the only clause so the exact same selection is used. The filters used in an alert can end in the alert ID to avoid name clashes with other alerts. See only the following global pre-selection filters and filters defined in the alert itself. There is no guarantee that references to filters in other alerts work consistently, or at all.

The Alert Condition must always be tied to a global pre-selection filter to indicate what SMF and WTO input to monitor, either directly or indirectly. In this case the UAPF1204 pre-selection was already tied to the RECENT pre-selection filter, so this condition is indirectly satisfied. You can choose the global pre-selection filters from the following list:

likelist=recent
: Tie to the recent SMF records written during the current reporting interval.

likelist=history
: Tie to the "moving window" analysis SMF records written during the "averaging" interval. There is no overlap between **recent** and **history**.

likelist=wtorec
: Tie to the recent WTO messages written during the current reporting interval.

likelist=wtohis
: Tie to the "moving window" analysis WTO messages written during the "averaging" interval. There is no overlap between **wtorec** and **wtohis**.

This list applies to the global skeleton C2PSGLOB.

Note: If necessary, you can use a different global skeleton for an Alert Configuration.
In these pre-selections, further selection on SMF record TYPE and SUBTYPE or on WTO MSGID is often required; for example, SELECT likelist=wtorec MSGID(CSV410I).

For Extended Monitoring alerts, the alert condition requires only a selection of the complex `select complex=(base, current)`, for example. However, additional selection criteria might be needed to limit the search for differences in system and security settings so that only certain records are included. For example, in Alert 1207, a NEWLIST TYPE=SENSDSN is used. However, the selection limits the comparison operation to just the APF data sets. See ID 1207 in Table 5 on page 39. The CompareOpt statement that specifies which fields to compare is defined in the Global CARLa Skeleton.

Email layout

You can specify the layout of the alert message for email destinations in the)**CM EMAIL sortlist** section. The IBM Security zSecure-supplied alerts have a common layout as shown in “Standard email layout” on page 42. The following example shows alert 1302.

```
)CM EMAIL sortlist
)SEL &C2PERCTP = MAIL
 sortlist,
  recno(nd),
  'Alert: Audited program'(t) resource(t,8) 'has been executed'(t),
  'Alert: Audited program' resource(0) 'has been executed' /,
  'A program with auditing specified has been executed' /,
  / '   Alert id        &c2pemem;',
```

```
  / '   Date and time'(18) date(9) time(11),
  / '   Program'(18) resource,
  / '   Data set'(18) dataset,
  / '   User'(18) user(8) name,
  / '   Job name'(18) jobname,
  / '   System ID'(18) system,
  / /
)ENDSEL
```

Note: The title modifier (t) is used to set the email subject.

Text message layout

You can specify the layout of the alert message for text message destinations in the **)CM Cellphone sortlist** section. Whether the text message as received is taken from the subject or the body of the email depends on the e-mail-to-text-message-gateway you use. All IBM Security zSecure-supplied alerts send a similar message in both subject and body. The following example shows alert 1204.

```
)CM Cellphone sortlist
)SEL &C2PERCTP = CELL
 sortlist,
  recno(nd),
  'Alert &c2pemem;: Update by'(t) user(t) 'on APF data set'(t),
  dataset(t),
  'Alert &c2pemem;: Update by' user(0) 'on APF data set',
  dataset(0)
)ENDSEL
```

SNMP layout

You can specify the layout of the alert message for SNMP destinations in the **)CM SNMP sortlist** section. In this layout, you specify combinations of variables and their contents. See also Appendix A, “SNMP output,” on page 107. The following example shows alert 1204.

```
)CM SNMP sortlist
)SEL &C2PERCTP = SNMP
sortlist,
 recno(nd),
 '&c2pemem.' /,
 'eventIntegral',
 'Alert: Update on APF data set' dataset(0,hor) '-',
 'APF data set successfully updated' /,
 'eventWhen' datetime(datetimezone,0) /,
 'onWhatDSNAME' dataset(0,hor) /,
 'onWhatGRANTED' intent /,
 'onWhatALLOWED' access /,
 'onWhatINTENT' intent /,
 'whoUSERID' userid(0) /,
 'whoNAME' name(0) /,
 'whatDESC' desc(0,explode) /,
 'whatJOBNAME' jobname(0) /,
 'whereSYSTEM' system(0)
)ENDSEL
```

UNIX syslog layout

You can specify the layout of the alert message for SYSLOG destinations in the **)CM UNIX syslog sortlist** section. The following example shows alert 1204.

```
)CM UNIX syslog sortlist
)SEL &C2PERCTP = SYSL
)SEL &C2PESECP = RACF
 sortlist,
  recno(nd) '<&C2PEPRIO.>' | date(month,3) date(monthday,0) time(8),
  system 'C2P&c2pemem.',
  '[C2P&C2PEMEM.',
```

```
  'onWhatDSNAME="' | dataset(0,firstonly) | '"',
  'onWhatGRANTED="' |  intent(0) | '"',
  'onWhatALLOWED="' | access(0) | '"',
  'onWhatINTENT="' |  intent(0) | '"',
  'whoUSERID="' | userid(0) | '"',
  'whoNAME="' | user:pgmrname(0) | '"',
  'whatDESC="' | desc(0,explode) | '"',
  'whatJOBNAME="' | jobname(0) | '"',
  'whereSYSTEM="' | system(0) | '"]',
   'Alert: Update on APF data set' dataset(0,hor) '-',
   'APF data set successfully updated'
)ENDSEL
```

Command section

For RACF systems, you can optionally specify a command to be issued when the Alert Condition occurs in the **)CM Command** section. In the following example, the user to which the selected alert applies is revoked by RACF.

```
)CM Command
)SEL &C2PERCTP = CMD
  "alu" userid(0) "revoke"
)ENDSEL
```

Chapter 3. Predefined alerts

This chapter describes the alerts that are shipped with zSecure Alert. For an explanation of the Class column, see "Alert activation guidelines" on page 5. The following table explains the meaning of the Severity column. Alerts with IDs in the range 1000-1999 are RACF alerts and those alerts in the range 2000-2999 are ACF2 alerts.

Table 5. Predefined Alerts

ID	Description	Class	Severity
1001	Heartbeat event (indicates that its originator is up and running)	3	0
1101	Logon by unknown user	2	3
1102	Logon with emergency user ID	1(*)	3
1103	Logon of a user ID with uid(0) (UNIX superuser)	2	2
1104	Highly authorized user revoked for password	2	3
1105	System authority granted	2	3
1106	System authority removed	3	2
1107	Group authority granted	2	2
1108	Group authority removed	3	3
1109	SPECIAL authority used by non-SPECIAL user	1	2
1110	non-OPERATIONS user accessed data set with OPERATIONS	1	3
1111	Invalid password attempts exceed limit	2	3
1112	Password history flushed	2	3
1113	Suspect password changes	3	2
1114	Connect authority>=CREATE set	2	2
1115	Too many violations	1	3
1201	WARNING mode access on data set	1	2
1202	Setting UACC>=UPDATE on a DATASET profile	2	3
1203	Setting UACC>NONE on a DATASET profile	3	2
1204	Update on APF data set	2	2
1205	Data set added to APF list using SETPROG	2	3
1206	Data set removed from APF list using SETPROG	2	2
1207	Data set addition to APF list detected	2	3
1208	Data set removal from APF list detected	2	2
1301	Catchall profile used for STC	3	2
1302	Audited program has been executed	3	2
1303	WARNING mode access on general resource	1	2
1401	UNIX file access violation	3	2
1402	Global write specified when altering file access	2	3
1403	Global read specified when altering file access	3	2

Table 5. Predefined Alerts (continued)

ID	Description	Class	Severity
1404	Extended attribute changed (Superseded by 1409)	2	2
1405	Audited UNIX program has been executed	3	2
1406	Superuser privileged UNIX program executed	2	2
1407	Superuser privileged shell obtained by user	2	2
1408	Superuser privileges set on UNIX program	2	2
1409	Extended attribute changed	2	2
1501	Global security countermeasure activated	3(**)	2
1502	Global security countermeasure deactivated	1(*) (**)	4
1503	Global security countermeasure or option changed	1	3
1504	RACF resource class activated	2	2
1505	RACF resource class deactivated	2	3
1601	SMF data loss started	1(*)	5
1602	SMF logging resumed after failure	3	2
1603	SVC definition changed	2	3
1604	IBM Health Checker found low severity problem	3	2
1605	IBM Health Checker found medium severity problem	2	3
1606	IBM Health Checker found high severity problem	1	4
1607	SMF record flood detected	1	4
1608	SMF record flood starts dropping records	1	5
1609	Attacks blocked by filter rules are no longer logged	2	2
1610	Attacks blocked by default filter rules are no longer logged	3	2
1611	Certain SMF 119 records are no longer written; audit trail incomplete	1	3
1612	IPv4 or IPv6 filtering support and IPSec tunnel support deactivated	1	4
1613	TCP or UDP ports below 1024 are not reserved any more	1	4
1614	The security class of an interface has changed	2	2
1615	IP filter rules changed	2	2
1701	Connect to an important group	2	3
2001	Heartbeat event (indicates that its originator is up and running)	3	0
2102	Logon with emergency user	1(*)	3
2104	Highly authorized user revoked for password	2	3
2105	System authority granted	2	3
2106	System authority removed	3	2
2111	Invalid password attempts exceed limit for user	2	3
2112	Password history flushed	2	3
2113	Suspect password changes	3	2
2115	Too many violations	1	3

Table 5. Predefined Alerts (continued)

ID	Description	Class	Severity
2116	SECURITY authority used by non-SECURITY logon ID	1	2
2117	NON-CNCL authority used by non-NON-CNCL logon ID	1	3
2118	READALL authority used by non-READALL logon ID	1	3
2201	WARNING mode access on data set	1	2
2204	Update on APF data sets	2	2
2205	Data set added to APF list using SETPROG	2	3
2206	Data set removed from APF list using SETPROG	2	2
2207	Data set addition to APF list detected	2	3
2208	Data set removal from APF list detected	2	2
2301	Default STC logon ID used for STC	3	2
2407	Superuser privileged shell obtained by user	2	2
2409	Extended attribute changed	2	2
2501	Global security countermeasure added	3	2
2502	Global security countermeasure deleted	1 (*)	4
2503	Global security countermeasure or option changed	1	3
2601	SMF data loss started	1(*)	5
2602	SMF logging resumed after failure	3	2
2603	SVC definition changed	2	3
2604	IBM Health Checker found low severity problem	3	2
2605	IBM Health Checker found medium severity problem	2	3
2606	IBM Health Checker found high severity problem	1	4
2607	SMF record flood detected	1	4
2608	SMF record flood starts dropping records	1	5
2609	Attacks blocked by filter rules are no longer logged	2 (***)	2
2610	Attacks blocked by default filter rules are no longer logged	3 (***)	2
2611	Certain SMF 119 records are no longer written; audit trail incomplete	1 (***)	3
2612	IPv4 or IPv6 filtering support and IPSec tunnel support deactivated	1 (***)	4
2613	TCP or UDP ports below 1024 are not reserved any more	1 (***)	4
2614	The security class of an interface has changed	2 (***)	2
2615	IP filter rules changed	2 (***)	2

(*) When this alert is issued, a fast response is required.

(**) This alert is included in alert 1503, so there is little point in activating it if they have the same receiver set.

(***) The class and severity of this alert is identical to that of its RACF counterpart.

The Severity column lists the severity levels that Tivoli Enterprise Console and IBM Tivoli NetView associate with alerts. Severity levels range from 0 to 5:

Table 6. Tivoli Enterprise Console and NetView severity levels

Severity	Meaning in Tivoli Enterprise Console	Meaning in NetView
0	Harmless	Cleared
1	Unknown	Indeterminate
2	Warning	Warning
3	Minor	Minor error
4	Critical	Critical
5	Fatal	Major

The alerts are communicated through alert messages that are available in the following different formats:

- email
- text message
- WTO
- SNMP trap
- UNIX syslog

See "Overview" on page 3.

Sample emails and text messages are shown with each individual predefined alert in this chapter. The SNMP trap format is explained in Appendix A, "SNMP output," on page 107.

The rest of this chapter explains the general layout of the email format and describes the predefined alerts in detail, divided in functional categories. If an alert can be configured, it is explained here.

Each alert requires certain SMF record types to be logged or specific WTO messages to be issued. Most predefined alerts require SMF type 80, RACF processing. It is assumed that you log these SMF types. All other requirements are shown with each individual alert. SMF logging is controlled per subsystem.

Standard email layout

All email alert messages have similar output. See the following example of an email that can be sent.

```
From:    C2POLICE at DINO
Subject: Alert: Audited program ASMIDFA  has been executed

Alert: Audited program ASMIDFA has been executed
A program which auditing specified has been executed

   Alert id        1302
   Date and time   07Feb2003 13:44:43.20
   Program         ASMIDFA
   Data set        SHARED.LINKLIB
   User            C##BDV2  DIONNE VONT
   Job name        C##BDV2
   System ID       DINO
```

You can see here that a program called ASMIDFA from the data set SHARED.LINKLIB has started execution. The user that executed the program is C##BDV2, and the user name is *Dionne Vont*. The program executes in job C##BDV2 on system DINO.

The sender of the email can be configured using the interface. The default is: *jobname* at *system name*. The subject header and the body of the email are generated by the CARLa code. The email subject is the same as the first line in the email body; however, formatting might vary slightly. Below that line is a general header that describes the event.

Below the headers of the alert is the section with details. The first line contains the alert ID. This number can be used to find the corresponding alert using SNMP, WTO, or SMS output and for finding the right entry in this documentation. The second line shows the date and time the event occurred. This is followed by the alert-specific fields. Finally, the job name, job ID, and system name are listed if available.

Predefined RACF alerts

This topic describes the RACF alerts that are shipped with zSecure Alert.

User alerts

The following alerts are used to monitor events pertaining to specific users and for auditing changes to users.

Logon by unknown user (1101)

This alert is triggered on two occasions:

1. A user, unknown to RACF, successfully logs on to TSO. This user is defined in SYS1.UADS, but not in RACF.
2. A batch job is submitted by NJE on another system for this system. On the receiving system, the user that submitted the job is not defined to RACF.

To receive this alert, you must log SMF record type 30 subtype 1.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Logon by unknown user

Alert: logon by unknown user
A user unknown to RACF logged on or submitted a batch job

   Alert id        1101
   Date and time   10Feb2003 06:53:16.60
   User            *
   Result          Success
   Job name + id   TSOB     JOB00042
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1101: Logon by unknown user *        job TSOB

Alert 1101: Logon by unknown user * job TSOB
```

The generated email report always shows a '*' for the user and whether the logon succeeded.

It can be difficult to find the source of the unknown logon because the system only logs a '*' as user. However, you can verify that the SYS1.UADS data set does not contain any user IDs that are not defined in RACF. Additionally, to stop job submissions by undefined users you can set SETROPTS JES(BATCHALLRACF).

Logon with emergency user ID (1102)

An alert is sent if a user ID that is meant for emergencies is used for TSO logon or batch job submission.

To receive this alert, you must log SMF record type 30 subtype 1.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Emergency user IBMUSER  logged on

Alert: Emergency user IBMUSER logged on
Successful logon or job submit with a userid meant for emergencies

   Alert id        1102
   Date and time   03Feb2003 09:38:44.94
   User            IBMUSER  IBM DEFAULT USER
   Result          Success
   Job name + id   IBMUSER  TSU05900
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1102: emergency user IBMUSER  logged on

Alert 1102: emergency user IBMUSER logged on
```

The generated email report shows the user ID used to log on to the system and whether the logon succeeded.

You can configure the alert for your site. When selecting the alert, you are prompted with a panel. You can enter up to 10 user IDs that must be used only in case of emergencies. See “Emergency user configuration (alerts 1102 and 2102)” on page 96.

Logon of a user ID with uid(0) (UNIX superuser) (1103)

An alert is sent if a user ID with UNIX uid 0 is used to logon to TSO or OMVS. It is a sound UNIX principle that you must not log on with superuser privileges but instead use 'su' when needed.

To receive this alert, you must log SMF record type 30 subtype 1.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Superuser C##BMR1  logon

Alert: Superuser C##BMR1 logon
A user with uid(0) has logged on

   Alert id        1103
   Date and time   03Feb2003 09:38:44.94
   User            C##BMR1  MARY ROBERTSON
   Logon to        TSO
   Result          Success
   Job name + id   C##BMR1  TSU05900
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1103: Superuser C##BMR1  logon to TSO

Alert 1103: Superuser C##BMR1 logon to TSO
```

The generated email report shows the user ID that was used to log on to the system, on which subsystem the logon took place, TSO or OMVS, and the status of the logon.

If you receive these alerts, you must remove the uid 0 definition in the OMVS segments of these users. Use profiles in the UNIXPRIV class and BPX.SUPERUSER in the FACILITY class to give users selective superuser authority.

Highly authorized user revoked for password (1104)

This alert is triggered when a user with a system-level authority (SPECIAL, OPERATIONS, or AUDITOR) is revoked because of excessive invalid password attempts. It can be caused by an intruder who is trying to guess the password of the user.

Note: You must take care not all your users with system authority get revoked at the same time. You must have some procedure to make sure that at least one unrevoked user ID with SPECIAL authority is reinstated.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Highly authorized user C##CX44  revoked for password violations

Alert: Highly authorized user C##CX44 revoked for password violations
System-level authorized user revoked due to excessive password attempts

   Alert id        1104
   Date and time   07Feb2003 14:58:27.13
   User            C##CX44  TEST USER
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1104: Highly authorized user C##CX44  revoked for password violations

Alert 1104: Highly authorized user C##CX44 revoked for password violations
```

The report shows the user ID and accompanying programmer name that is revoked for excessive password violations.

System authority granted (1105)

An alert is generated when a user obtains system-level authority (SPECIAL, OPERATIONS, AUDITOR, or CLAUTH).

To receive this alert, you must have SETROPTS setting AUDIT(USER) and SAUDIT enabled.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: System authority granted to C##BMR2

Alert: System authority granted to C##BMR2
System-level authority granted to user

   Alert id        1105
   Date and time   29May2000 13:25:12.42
```

```
   Authority       SPECIAL
   Granted to      C##BMR2  MARY ROBERTSON
   Result          Success
   RACF command    ALTUSER C##BMR2 SPECIAL
   User            C##BMR1  MARY ROBERTSON
   Job name        C##BMR1
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1105: System authority granted to C##BMR2  by C##BMR1

Alert 1105: System authority SPECIAL granted to C##BMR2 by C##BMR1
```

The report shows the system authority that is granted, the user that is granted the authority, the complete RACF command, and the result of the command. Additionally, it shows the user that performed the RACF command.

System authority removed (1106)

An alert is sent when a system-level authority, that is, SPECIAL, OPERATIONS, AUDITOR, or CLAUTH, is removed from a user.

To receive this alert, you must have SETROPTS setting AUDIT(USER) and SAUDIT enabled.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: System authority removed from C##BMR1

Alert: System authority removed from C##BMR2
System-level authority removed from user

   Alert id        1106
   Date and time   29May2000 13:25:16.15
   Authority       SPECIAL
   Removed from    C##BMR2  MARY ROBERTSON
   Result          Success
   RACF command    ALTUSER C##BMR2 NOSPECIAL
   User            C##BMR1  MARY ROBERTSON
   Job name        C##BMR1
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1106: System authority removed from C##BMR2  by C##BMR1

Alert 1106: System authority SPECIAL removed from C##BMR2 by C##BMR1
```

The report shows the removed authority, the user whose authority is removed, the complete RACF command, and the result of the command. In addition, it shows the user that performed the RACF command.

Group authority granted (1107)

If a group-level authorization, that is, SPECIAL, OPERATIONS, or AUDITOR, is granted to a user, an alert is generated.

To receive this alert, you must have SETROPTS setting SAUDIT, AUDIT(USER), or AUDIT(GROUP) enabled.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Group authority granted to C##ARO2  in C##C

Alert: Group authority granted to C##ARO2 in C##C
CONNECT  Group-level authority granted to user

   Alert id        1107
   Date and time   02Feb2003 09:47:23.29
   Authority       SPECIAL
   Granted to      C##ARO2  RICK OXSON
   Connected to    C##C
   Result          Success
   RACF command    CONNECT C##ARO2 AUTHORITY(USE) GROUP(C##C) NOADSP
                   NOAUDITOR NOGRPACC NOOPERATIONS OWNER(C##C) RESUME
                   SPECIAL UACC(NONE)
   User            C##BERT  ERWIN RETTICH
   Job name        CRRAC#17
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1107: Group authority granted to C##ARO2  in C##C

Alert 1107: Group authority SPECIAL granted to C##ARO2 in C##C
```

The generated email report shows the granted authority, the user that is granted the authority, the group the authorized user is in, the complete RACF command, the result of the command, and the user who executed the command.

Note: The RACF command field shows the specified command keywords and the default keywords so it can become rather long.

Group authority removed (1108)

An alert is generated if a group-level authorization, that is, SPECIAL, OPERATIONS, or AUDITOR, is removed from a user, or a user with such authorizations is removed from a group.

To receive this alert, you must have SETROPTS setting SAUDIT, AUDIT(USER), or AUDIT(GROUP) enabled.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Group authority removed for C##ARO2  in C##C

Alert: Group authority removed for C##ARO2 in C##C
Group-level authority removed from user

   Alert id        1108
   Date and time   02Feb2003 09:47:23.29
   Authority       OPERATIONS AUDITOR
   Removed from    C##ARO2  RICK OXSON
   Connected to    C##C
   Result          Success
   RACF command    CONNECT C##ARO2 AUTHORITY(USE) GROUP(C##C) NOADSP
                   NOAUDITOR NOGRPACC NOOPERATIONS OWNER(C##C) RESUME
                   SPECIAL UACC(NONE)
   User            C##BERT  ERWIN RETTICH
   Job name        CRRAC#17
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1108: Group authority removed for C##ARO2  in C##C

Alert 1108: Group authority OPERATIONS AUDITOR removed for C##ARO2 in C##C
```

The report shows the removed authority, or <CONNECT REMOVED> if the connection is removed, the user whose authority is removed, the group that the user is in, the complete RACF command, the result of the command, and the user who executed the command.

Note: The RACF command field shows the specified command keywords and the default keywords so it can become rather long.

SPECIAL authority used by non-SPECIAL user (1109)

This alert is generated when a user without system or group special authorization executes a command with the group or system special authorizations. It means that the user has the potential to successfully execute commands that require group or system special, but does not have SPECIAL authority itself. This condition can be set by APF-authorized software.

Note: You must analyze the SMF records cut for the job up to the time the alert was issued as a first attempt to identify the responsible program.

To receive this alert, you must have SETROPTS setting SAUDIT enabled.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: non-SPECIAL user C##BDV1  issued SPECIAL command

Alert: non-SPECIAL user C##BDV1 issued SPECIAL command
SPECIAL authority used for RACF command by user without SPECIAL

   Alert id        1109
   Date and time   17Jan2003 03:00:16.89
   User            C##BDV1  DIONNE VONT
   RACF command    ADDSD 'SYS1.APF.NODATA.**' NOSET
   Result          Success
   Job name        C##BDV1
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1109: non-SPECIAL user C##BDV1  issued SPECIAL command

Alert 1109: non-SPECIAL user C##BDV1 issued SPECIAL command ADDSD
'SYS1.APF.NODATA.**' NOSET
```

The report shows the user, the RACF command the user executed, and whether the command succeeded.

If the command is issued without valid authorization, you must examine the cause for the special authorization and remove it.

Non-OPERATIONS user accessed data set with OPERATIONS (1110)

An alert is generated when a user without system or group operations accesses a data set with group or system operation authority. It implies that the user can access all data sets in the scope of the user unless explicitly denied by an ACL. This situation can arise if an APF-authorized program sets group or system operations authority in the RACF control blocks.

Note: You must analyze the SMF records cut for the job up to the time the alert got issued as a first attempt to identify the responsible program.

To receive this alert, you must have SETROPTS setting OPERAUDIT enabled.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: non-OPERATIONS user D##MUY   accessed data set with  OPERATIONS

Alert: non-OPERATIONS user D##MUY accessed data set with OPERATIONS
Successful data set access using OPERATIONS by user without OPERATIONS

   Alert id        1110
   Date and time   22Jan2003 10:26:16.81
   Data set        D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00
   Access          ALTER
   User            D##MUY
   Result          Success
   Job name        D##MUY
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1110: non-OPERATIONS user D##MUY   accessed (ALTER  ) with
OPERATIONS data set D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00

Alert 1110: non-OPERATIONS user D##MUY accessed (ALTER) with OPERATIONS
data set D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00
```

The alert shows the data set that is accessed, the access level, the accessing user, and the result of the action.

If the access is non-valid, you must examine the reason why these OPERATIONS authorizations are set, and remove the cause if necessary.

Invalid password attempts exceed limit (1111)

An alert is sent if too many failed logon attempts are made specifying an invalid password for one specific user ID in a specific time window. The measurement interval is the sum of the REPORT options **Interval** and **AverageInterval**. See the information about the REPORT command in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

"Too many" is defined as 5 or more. If you want to use another limit, you must copy the alert to an installation defined alert. Adapt all four instances of

```
#history(nd,<5), #total(nd,>=5),
```

in the new skeleton member to use the limit you want instead of 5.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Invalid password attempts exceed limit for C##BSG2

Alert: Invalid password attempts exceed limit for C##BSG2
Excessive number of password attempts by user

   Alert id        1111
   Date and time   03Mar2003 13:30:04.39 - 03Mar2003 13:39:23.78
   Attempts        6
   User            C##BSG2  SUSAN GAYNOR
   Result          Violation
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1111: Invalid password attempts exceed limit for C##BSG2

Alert 1111: Invalid password attempts exceed limit for C##BSG2
```

The generated email report shows the interval in which the logon attempts occurred, the number of attempts, the user ID that was used for trying to log on to the system, and the status of the logon; in this alert the logons are always violations.

Currently it is not possible to display the source (terminal) of the logon attempts.

Password history flushed (1112)

An alert is sent if the password for a specific user ID is changed more often than the password history SETROPTS setting in a specific time window. It means that the user flushed the entire password history, enabling reuse of a previous password. The measurement interval is the sum of the REPORT options **Interval** and **AverageInterval**. See the information about the REPORT command in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Note:

1. Alerts 1112 and 1113 are related. When a report interval ends while a password history is being flushed, alert 1113 is triggered, while alert 1112 occurs when flushing is complete. If you receive multiple alerts 1113 for the same user, but no alert 1112, it is also likely that the history is being flushed. The user might have taken some more time for it.
2. Both alerts 1112 and 1113 depend on whether you activate the IBM Security zSecure New Password Exit. See *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*. By default, the exit is installed and activated. When the New Password Exit is activated, password changes done by a JOB card or at logon result in an SMF record identical to that generated for the PASSWORD command. These password changes are counted for alert 1112 and 1113. If you do not activate the IBM Security zSecure New Password Exit, password changes done by a JOB card or logon are not detected.

To receive this alert, you must have SETROPTS AUDIT(USER) enabled.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: Password history flushed for C##BSG2

Alert: Password history flushed for C##BSG2
Repeated PASSWORD commands flush password history

   Alert id        1112
   Date and time   05Mar2003 11:47:11.21 - 03Mar2003 11:47:12.04
   Pwd changes     33
   User            C##BSG2  SUSAN GAYNOR
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1112: Password history flushed for C##BSG2

Alert 1112: Password history flushed for C##BSG2
```

The generated email report shows the interval in which the password history flushing occurred, the number of password changes, and the user ID of the user who flushed the password history.

Suspect password changes (1113)

An alert is sent if the password for a specific user ID is changed too often in a specific time window, but not so often that the password history is flushed completely, which would result in alert 1112. "Too often" is defined as five times or more. If you want to use another limit, you must copy the alert to an installation defined alert. Adapt all four instances of

```
#history(nd,<5) #total(nd,>=5),
```

in the new skeleton member to use the wanted limit.

To receive this alert, you must have SETROPTS AUDIT(USER) enabled.

For further explanation, see “Password history flushed (1112)” on page 50.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: Suspect password changes for C##BSG2

Alert: Suspect password changes for C##BSG2
Excessive number of PASSWORD commands by user

   Alert id        1113
   Date and time   03Mar2003 15:17:12.32 - 03Mar2003 15:17:13.11
   Pwd changes     7
   User            C##BSG2  SUSAN GAYNOR
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1113: Suspect password changes for C##BSG2

Alert 1113: Suspect password changes for C##BSG2
```

The generated email report shows the interval in which the password changes occurred, the number of password changes, and the user ID that has its password changed many times.

Connect authority>=CREATE set (1114)

An alert is sent when an authority level of CREATE or higher is set on a connection. Such a level allows decentralized administrators to add group data set profiles. If the level is CONNECT or JOIN, the user can furthermore connect any existing user to the group in question. If the level is JOIN, the user can also create subgroups and give out connect authorities for the group to other users. Furthermore, if the user has class authority (CLAUTH) in the USER class, new users can be created in the group as well.

To receive this alert, you must have at least SETROPTS setting AUDIT(USER) enabled.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: Connect authority JOIN    set for C##BSG2  in C##B

Alert: Connect authority JOIN set for C##BSG2 in C##B
High authority specified when adding or altering a connect
```

```
Alert id        1114
Date and time   08May2003 10:11:09.51
Authority       JOIN
Granted to      C##BSG2 SUSAN GAYNOR
Connected to    C##B
Result          Success
RACF command    ALTUSER C##BSG2 AUTHORITY(JOIN) GROUP(C##B)
User            C##BERT  ERWIN RETTICH
Job name        CBERT#17
System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1114: Connect authority JOIN    set for C##BSG2  in C##B

Alert 1114: Connect authority JOIN set for C##BSG2 in C##B
```

The generated email report shows the granted group-authority, the user and the target group, the complete RACF command, the result of the command, and the user who executed the command.

Note: The RACF command field shows the specified command keywords and the default keywords, so it can become rather long.

Too many violations (1115)

This corrective alert is generated when more violations than a configured number are recorded for a specific user ID in the interval as specified with the zSecure Alert REPORT option **AverageInterval**. For additional information, see the information about the REPORT command in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

To generate this alert, RACF access violations must be recorded. Access violations are recorded depending on the LOGOPTION settings for the class and the audit settings of the profile.

This alert is corrective in that you can specify to automatically revoke the violating user ID. In addition, with a zSecure Admin license you can choose to generate a CKGRACF DISABLE command instead of an ALTUSER REVOKE command.

The report format of the alert depends on whether you decided to let zSecure Alert perform a corrective action.

The email format of the alert without a corrective action is:

```
From:        C2POLICE at DINO
Subject:     Alert: 15 violations recorded for user C2RMUS01

Alert: 15 violations recorded for user C2RMUS01
Number of violation exceeds the configured 10

   Alert id        1115
   Date and time   09Mar2005 14:49:55.90 - 09Mar2005 14:54:57.89
   Violations      15
   User            C2RMUS01
   System ID       DINO

 Time  Intent  Allowed Class    Resource

 14:49 READ    NONE    JESSPOOL JES2DINO.DFHSM.DFHSM.STC05782.D0000002.J
                                ESMSGLG
 14:49 READ    NONE    JESSPOOL JES2DINO.DFHSM.DFHSM.STC05782.D0000003.J
                                ESJCL
```

```
 14:50 READ    NONE    JESSPOOL JES2DINO.DFHSM.DFHSM.STC05782.D0000004.J
                                ESYSMSG
 14:50 READ    NONE    JESSPOOL JES2DINO.DFHSM.DFHSM.STC05782.D0000101.?
 14:51 READ    NONE    JESSPOOL JES2DINO.DFHSM.DFHSM.STC05782.D0000104.?
```

The text message format of the alert is:

```
Subject: Alert 1115: 15 violations recorded for user C2RMUS01

Alert 1115: 15 violations recorded for user C2RMUS01
```

When you decide to generate an ALU REVOKE command for the violating user ID, the text is changed into:

```
User C2RMUS01 revoked after 15 violations
```

When you decide to generate a CKGRACF DISABLE command for the violating user ID, the text is changed into:

```
User C2RMUS01 disabled with schedule DIS#VIOL after 15 violations
```

This alert enables you to customize for your site. When selecting the alert, you are prompted with a panel. In the panel, you can specify the number of violations you consider excessive and whether you want to generate a corrective action. Furthermore, you can specify up to 10 user IDs or user ID masks to be excluded. See "Revocation for excessive violations (1115) configuration" on page 97.

Data set alerts

This section describes the predefined alerts for data set access and data set profile changes.

WARNING mode access on data set (1201)

A data set is accessed and access is granted because of warning mode. See also "WARNING mode access on general resource (1303)" on page 59.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: WARNING mode READ    on data set CDS.SCDSSAMP

Alert: WARNING mode READ on data set CDS.SCDSSAMP
Data set access granted due to warning mode

   Alert id        1201
   Date and time   21Jan2003 09:11:11.01
   Data set        CDS.SCDSSAMP
   Granted access  READ
   Normal access   NONE
   Profile         CDS.SCDS*
   User            C##BMR1  MARY ROBERTSON
   Job name        C##BMR1
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1201: WARNING mode READ    by C##BMR1 on data set
CDS.SCDSSAMP

Alert 1201: WARNING mode READ by C##BMR1 on data set CDS.SCDSSAMP
```

The reports show the data set, the user that requested access to it, the profile against which the access is checked, the access that is granted, and the normal access that would have been granted if the profile had not been in WARNING mode.

A profile in WARNING mode can grant any access to the resource, including what the profile would not allow otherwise. WARNING mode is typically used to analyze what the effects of the access settings of a profile are before the access control is enforced. It functions as a temporary measure to overcome production problems. If you receive these alerts, you must verify whether the access must be granted. When confirmed, change the access settings of the profile accordingly. If this access is not supposed to occur, take remedial action as required.

UACC>=UPDATE on a DATASET profile (1202)

An alert is generated if a UACC equal to or higher than UPDATE is specified on a data set profile. If you want to receive alerts even when the specified UACC is equal to READ, you can use the next alert. See "UACC>NONE on a DATASET profile (1203)."

To receive this alert, you must have SETROPTS setting AUDIT(DATASET) enabled.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: UACC>=UPDATE set: C##QAP2.ONZI.**

Alert: UACC>=UPDATE set: C##QAP2.ONZI.**
High UACC specified when adding or altering a data set profile

   Alert id        1202
   Date and time   04Feb2003 01:12:18.45
   Profile         C##QAP2.ONZI.**
   UACC            UPDATE
   Result          Success
   RACF command    ALTDSD 'C##QAP2.ONZI.**' UACC(UPDATE)
   User            C##QAP2  ALEXANDER POUVIER
   Job name        C##QAP2
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1202: UACC>=UPDATE set by C##QAP2 : C##QAP2.ONZI.**

Alert 1202: UACC>=UPDATE set: C##QAP2.ONZI.** UACC set to UPDATE by C##QAP2
```

The report shows the changed profile, the specified UACC, the complete RACF command, the result of the command, and the user who executed the command.

UACC>NONE on a DATASET profile (1203)

If a UACC higher than NONE is specified on a data set profile, an alert is generated. If you want to receive alerts only when the specified UACC is higher than READ, you can use the previous alert. See "UACC>=UPDATE on a DATASET profile (1202)."

To receive this alert, you must have SETROPTS setting AUDIT(DATASET) enabled.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: UACC>NONE set: C##QAP2.ONZI.**

Alert: UACC>NONE set: C##QAP2.ONZI.**
```

```
High UACC specified when adding or altering a data set profile

   Alert id        1203
   Date and time   04Feb2003 01:12:18.45
   Profile         C##QAP2.ONZI.**
   UACC            UPDATE
   Result          Success
   RACF command    ALTDSD 'C##QAP2.ONZI.**' UACC(UPDATE)
   User            C##QAP2  ALEXANDER POUVIER
   Job name        C##QAP2
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1203: UACC>NONE set by C##QAP2 : C##QAP2.ONZI.**

Alert 1203: UACC>NONE set: C##QAP2.ONZI.** UACC set to UPDATE by C##QAP2
```

The report shows the changed profile, the specified UACC, the complete RACF command, the result of the command, and the user who executed the command.

Update on APF data set (1204)

An alert is sent when an APF authorized data set is updated.

To generate this alert, RACF successful update access must be recorded. This is the case if either AUDIT(success(update)) or GLOBALAUDIT(success(update)) has been specified for the relevant profiles. The necessary commands can be created by the zSecure Audit VERIFY SENSITIVE command.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Update by C##ASCH  on APF data set C##A.D.C##NEW.APF.LOAD

Alert: Update by C##ASCH on APF data set C##A.D.C##NEW.APF.LOAD
APF data set successfully updated

   Alert id        1204
   Date and time   03Feb2003 10:12:05.30
   Data set        C##A.D.C##NEW.APF.LOAD
   Access          ALTER
   User            C##ASCH  SIRAM CHRISTIAN
   Result          Success
   Job name        C##ASCHL
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1204: Update by user C##ASCH  on APF data set
C##A.D.C##NEW.APF.LOAD

Alert 1204: Update by user C##ASCH on APF data set C##A.D.C##NEW.APF.LOAD
```

The alert shows the data set that was updated, the employed access level, and the user who accessed the data set.

Data set added to APF list using SETPROG (1205)

An alert is generated when a data set is dynamically added to the APF list using the SET PROG or SETPROG command.

To generate this alert, WTO message CSV410I must be available, and selected for processing.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: Data set added to APF list using SETPROG: SYSPROG.APF.LOAD

Alert: Data set added to APF list using SETPROG:SYSPROG.APF.LOAD
A data set is dynamically added to the APF list

   Alert id        1205
   Date and time   21Feb2003 11:44:36.71
   Data set        SYSPROG.APF.LOAD
   Volume          <SMS MANAGED>
   Console ID      R##SLIN
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1205: Data set added to APF list using SETPROG from console R##SLIN:
SYSPROG.APF.LOAD

Alert 1205: Data set added to APF list using SETPROG from console R##SLIN:
SYSPROG.APF.LOAD on volume <SMS MANAGED>
```

The alert shows the data set added to the APF list, on what volume the data set resides, or <SMS MANAGED> if it is managed by SMS. It shows the name of the console from which the user entered the SET PROG or SETPROG command, if entered from SDSF. The console name defaults to the user ID.

Data set removed from APF list using SETPROG (1206)

An alert is generated when a data set is dynamically removed from the APF list using the SET PROG or SETPROG command.

To generate this alert, WTO message CSV410I must be available, and selected for processing.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: Data set removed from APF list using SETPROG: SYSPROG.APF.LOAD

Alert: Data set removed from APF list using SETPROG: SYSPROG.APF.LOAD
A data set is dynamically removed from the APF list

Alert id        1206
Date and time   21Feb2003 11:44:36.71
Data set        SYSPROG.APF.LOAD
Volume          <SMS MANAGED>
Console ID      R##SLIN
System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1206: Data set removed from APF list using SETPROG from console R##SLIN:
SYSPROG.APF.LOAD

Alert 1206: APF Data set removed from APF list using SETPROG from console R##SLIN:
SYSPROG.APF.LOAD on volume <SMS MANAGED>
```

The alert shows the data set removed from the APF list. It also shows on what volume the data set resides, or <SMS MANAGED> if it is managed by SMS. It shows the name of the console from which the user entered the SET PROG or SETPROG command, if entered from SDSF. The console name defaults to the user ID.

Data set addition to APF list detected (1207)

This alert is generated when a data set is added to the APF list by any method. It includes use of the SET PROG or SETPROG command and use of other products. To generate this alert, Extended Monitoring must be active. This alert is based on a comparison of two system snapshots. It does not provide any information about the user ID or jobname that was used to add the data set or the process that was used to perform the addition.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: Data set addition to APF list detected: SYSPROG.APF.LOAD

Alert: Data set addition to APF list detected: SYSPROG.APF.LOAD
An addition of a data set to the APF list has been detected

 Alert id  1207
 Data set  SYSPROG.APF.LOAD
 Volume   <SMS MANAGED>
 System ID  DINO
```

The text message format of the alert is:

```
Subject: Alert 1207: Data set addition to APF list detected: SYSPROG.APF.LOAD
Alert 1207: Data set addition to APF list detected: SYSPROG.APF.LOAD
on volume <SMS MANAGED>
```

The alert shows the data set that was added to the APF list. It also shows on what volume the data set resides (or <SMS MANAGED> if it is managed by SMS). This alert is based on a comparison of two system snapshots. It does not provide any information about the user ID or jobname that was used to add the data set or the process that was used to perform the addition.

Data set addition to APF list detected (1208)

This alert is generated when a data set is removed from the APF list by any method. It includes use of the SET PROG or SETPROG command and use of other products. To generate this alert, Extended Monitoring must be active. This alert is based on a comparison of two system snapshots. It does not provide any information about the user ID, jobname that was used to add the data set, or the process that was used to perform the addition.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: Data set addition to APF list detected: SYSPROG.APF.LOAD

Alert: Data set removal from APF list detected: SYSPROG.APF.LOAD
A removal of a data set from the APF list has been detected

 Alert id  1208
 Data set  SYSPROG.APF.LOAD
 Volume   <SMS MANAGED>
 System ID  DINO
```

The text message format of the alert is:

```
Subject: Alert 1208: Data set removal from APF list detected: SYSPROG.APF.LOAD
Alert 1208: Data set removal from APF list detected: SYSPROG.APF.LOAD
on volume <SMS MANAGED>
```

The alert shows the data set that was removed from the APF list. It also shows on what volume the data set resides (or <SMS MANAGED> if it is managed by SMS). This alert is based on a comparison of two system snapshots. It does not provide

any information about the user ID, jobname that was used to add the data set, or the process that was used to perform the addition.

General resource alerts

These alerts report on the use of and changes to general resources.

Catchall profile used for STC (1301)

An alert is sent if a started task is checked against a catchall profile in the STARTED class.

To receive this alert, you must set TRACE(YES) with an RALTER STARTED command on the catchall profile. This outputs WTO message IRR812I.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: STARTED/*.*  used for STC IEFBR1A .IEFBR1B

Alert: STARTED/*.*  used for STC IEFBR1A.IEFBR1B
A started task is checked against a catchall profile

   Alert id        1301
   Date and time   11Feb2003 18:14:48.78
   Profile         *.*
   Started task    IEFBR1A
   Started jobname IEFBR1B
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1301: STARTED/*.*  used for STC IEFBR1A .IEFBR1B

Alert 1301: STARTED/*.*  used for STC IEFBR1A .IEFBR1B
```

The report shows the matched catchall profile and the started task member and job name. This report does not show the user who began the started task.

You can remove the cause of this alert if you define the `member.jobname` in the STARTED class. The catchall profile is not checked anymore for this started task.

Audited program has been executed (1302)

Alert when a program that is audited has started execution. An audited program is protected by a profile in the PROGRAM class that has at least user or auditor auditing for READ successes.

To receive this alert, you must have at least AUDIT(SUCCESS(READ)) or GLOBALAUDIT(SUCCESS(READ)) specified on the profiles. You want these profiles to be reported on in the PROGRAM class.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Audited program ASMIDFA  has been executed

Alert: Audited program ASMIDFA has been executed
A program with auditing specified has been executed

   Alert id        1302
   Date and time   07Feb2003 13:44:43.20
   Program         ASMIDFA
   Data set        SHARED.LINKLIB
```

```
   User            C##BDV2  DIONNE VONT
   Job name        C##BDV2
   System ID       DINO
   Audit reason    <reason>
```

The text message format of the alert is:

```
Subject: Alert 1302: Audited program ASMIDFA  has been executed by C##BDV2  in
job C##BDV2

Alert 1302: Audited program ASMIDFA from data set SHARED.LINKLIB has been executed
by C##BDV2 in job C##BDV2
```

The report shows the program that has started execution, the data set where the program resides, the user who executed the program, and the audit reason.

WARNING mode access on general resource (1303)

A profile in a general resource class is checked for access, and access is granted because of warning mode. A similar alert for data sets is available in "WARNING mode access on data set (1201)" on page 53.

The e-mail format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: WARNING mode access to FACILITY IRR.LISTUSER

Alert: WARNING mode READ on FACILITY IRR.LISTUSER
Resource access granted due to warning mode

   Alert id        1303
   Date and time   07Feb2003 14:15:09.60
   Class           FACILITY
   Resource        IRR.LISTUSER
   Granted access  READ
   Normal access   NONE
   Profile         IRR.LISTUSER
   User            C##BDV2  DIONNE VONT
   Job name        C##BDV2
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1303: WARNING mode READ    by C##BDV2  on
FACILITY IRR.LISTUSER

Alert 1303: WARNING mode READ by C##BDV2 on FACILITY IRR.LISTUSER
```

The report shows the class and the name of the resource accessed, the user who requested access to it, and the profile against which the access is checked. It also shows the access that is granted and the normal access that would have been granted if the profile had not been in WARNING mode.

A profile in WARNING mode grants any access to the resource, including what the profile would not allow otherwise. WARNING mode is typically used to analyze what the effects of the access settings of a profile are, before the access control is enforced. It is also used as a temporary measure to overcome production problems. If you receive these alerts, you must verify whether the access must be allowed. If so, change the access settings of the profile accordingly. If this access is not supposed to occur, take remedial action as required.

UNIX alerts

The following alerts are triggered when events concerning UNIX files, directories, or programs occur.

UNIX file access violation (1401)

An alert is sent when an access violation occurs on a UNIX file or directory.

To generate this alert, SETROPTS setting LOGOPTIONS(FAILURES(DIRACC DIRSRCH FSOBJ)) must be set. Or, the relevant files must have access failure auditing specified by the **chaudit** command.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: UNIX access violation on ./actuator/bin/db2asc

Alert: UNIX access violation on ./actuator/bin/db2asc
Non-authorized UNIX file or directory access

   Alert id        1401
   Date and time   28May2000 01:10:06.67
   Path            ./actuator/bin/db2asc
   Access type     FACCESS
   Intended access --w-
   Granted access   r-x
   User            C##BOON  OTTO ONSLEY
   Job name        C##BOON
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1401: UNIX access violation (--w-) by C##BOON
on ./actuator/bin/db2asc

Alert 1401: UNIX access violation (--w-) by C##BOON on ./actuator/bin/db2asc
```

The report shows the path of the file or directory, the access type, that is, FACCESS, DIRACCESS, DIRSRCH, the intended access and the granted access, and the user who tried to access the file or directory. If you use a CKFREEZE file created with parameter UNIX=YES, the UNIX path mentioned in the report is an absolute path.

Global write specified when altering file access (1402)

This alert is generated if write access is specified on the *other* group of permissions of a UNIX file or directory.

To receive this alert, you must have SETROPTS setting LOGOPTIONS(ALWAYS(FSSEC)) enabled. In the absence of a CKFREEZE file created with parameter UNIX=YES and AUTOMOUNT=YES, you might also receive this alert for other non-file UNIX objects.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Global write specified on www/log/access.log

Alert: Global write specified on www/log/access.log
Global write specified when altering file access

   Alert id        1402
   Date and time   09Feb2003 08:07:01.66
   Path            www/log/access.log
```

```
   Old permissions rw-r--r--
   New permissions rw-rw-rw-
   Result          Success
   User            C##BER2  ERWIN RETTICH
   Job name        C##BER2
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1402: Global write specified by C##BER2  on www/log/access.log

Alert 1402: Global write specified by C##BER2 on www/log/access.log
```

The alert shows the path of the file or directory and the old and new permissions. It also shows the result of the **chmod** command and the user who changed the permission mode. If you use a CKFREEZE file created with parameter UNIX=YES, the UNIX path in the report is an absolute path.

Global read specified when altering file access (1403)

This alert is sent if read access is specified on the "other" group of permissions of a UNIX file.

To receive this alert, you must have SETROPTS setting LOGOPTIONS(ALWAYS(FSSEC)) enabled. In the absence of a CKFREEZE file created with parameter UNIX=YES and AUTOMOUNT=YES, you can receive this alert also for other non-file UNIX objects.

The e-mail format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Global read specified on www/log/access.log

Alert: Global read specified on www/log/access.log
Global read specified when altering file access

   Alert id        1403
   Date and time   09Feb2003 08:05:22.61
   Path            www/log/access.log
   Old permissions rw-------
   New permissions rw-r--r--
   Result          Success
   User            C##BER2  ERWIN RETTICH
   Job name        C##BER2
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1403: Global read specified by C##BER2  on www/log/access.log

Alert 1403: Global read specified by C##BER2 on www/log/access.log
```

The alert shows the path of the file, the old and new permissions, the result of the **chmod** command, and the user who changed the permission mode. If you use a CKFREEZE file created with parameter UNIX=YES, the UNIX path in the report is an absolute path.

Extended attribute changed (1404)

An alert is generated when an extended attribute (that is, APF, program control, or BPX shareas) is set or removed from a UNIX file or program.

This alert was superseded by alert 1409, available on z/OS 1.11 and later. Alert 1409 is much simpler to configure and uses considerably less resources than alert 1404.

To receive alert 1404, you must have at least SETROPTS setting LOGOPTIONS(DEFAULT(FSOBJ)) enabled. Then you can use the z/OS UNIX **chaudit** command to activate successful write auditing for the programs you want audited. If you have not activated successful auditing, the text of the alert as sent out is incomplete, and essential parts (like the alert number and the file identification) are missing. To avoid the need to set successful auditing for individual files, you might consider setting LOGOPTIONS(ALL(FSOBJ)). However, doing so significantly increases the number of SMF records created. To receive alerts of type 1404, you also cannot define a BPX.SAFFASTPATH profile in the FACILITY class.

For alerts sent by email, an attempt is made to include the actual extended attribute that has been changed. For this to be successful, READ logging on the FACILITY profiles matching BPX.FILEATTR.APF and BPX.FILEATTR.PROGCTL is also needed.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Extended attribute changed: APF

Alert: Extended attribute changed: APF
APF or program control bit changed on UNIX file or directory

   Alert id        1404
   Date and time   05Feb2003 13:17:52.49
   Path            audfrbg
   User            C##BERT  ERWIN RETTICH
   Job name        C##BERT
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1404: APF or program control bit changed by C##BERT  on
UNIX file or directory audfrbg

Alert 1404: APF or program control bit changed by C##BERT on UNIX file
or directory audfrbg
```

The alert shows the extended attribute that is set or removed. It also shows the path of the file or directory and the user who changed the attribute. If you use a CKFREEZE file created with parameter UNIX=YES, and optionally AUTOMOUNT=YES, specified, the path in the report is an absolute path.

Audited UNIX program has been executed (1405)

An alert is sent if a z/OS UNIX program that has successful execution audit (user or auditor) enabled has started execution. This alert does not cover programs that have the setuid bit enabled and have a superuser as owner. For more information, see “Superuser privileged UNIX program executed (1406)” on page 63.

To receive this alert, the audited program must be in an HFS file system. You must have at least SETROPTS setting LOGOPTIONS(DEFAULT(FSOBJ)) enabled, and must have no BPX.SAFFASTPATH profile defined in the FACILITY class. Additionally, you must use a CKFREEZE file created with parameter UNIX=YES, and optionally AUTOMOUNT=YES. Alerts are sent only for programs that have their information in the CKFREEZE file.

You can use the z/OS UNIX **chaudit** command to set the successful execution auditing bits on the programs you want audited.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: UNIX program executed: chprot

Alert: UNIX program executed: chprot
A UNIX program with execution auditing specified has been executed.

   Alert id        1405
   Date and time   11Mar2003 11:05:11.49
   Path            /usr/bin/chprot
   User            C##BSG2  SUSAN GAYNOR
   Job name        C##BSG2
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1405: UNIX program executed by C##BSG2 : /usr/bin/chprot

Alert 1405: UNIX program executed by C##BSG2: /usr/bin/chprot
```

The alert shows the path of the program and the user who started execution of that program.

Superuser privileged UNIX program executed (1406)

An alert is sent if a UNIX program with setuid enabled and owned by uid 0 has started execution. The program must have successful execution audit (user or auditor) enabled. Independent of the authorization of the user, these programs run with superuser privileges, and can read and write any file or directory on the UNIX subsystem.

To receive this alert, the audited program must be in an HFS file system. You must have at least SETROPTS setting LOGOPTIONS(DEFAULT(FSOBJ)) enabled, and must have no BPX.SAFFASTPATH profile defined in the FACILITY class. In addition, you must use a CKFREEZE file created with parameter UNIX=YES, and optionally AUTOMOUNT=YES. Alerts are sent only for programs that have their information in the CKFREEZE file.

This alert accompanies alert 1405. That alert sends a message if an audited UNIX program without these special privileges started execution. See “Audited UNIX program has been executed (1405)” on page 62. You can use the accompanying CARLa to generate UNIX command to set auditor execution auditing on all programs that execute with superuser privileges.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: Superuser privileged UNIX program executed: rdefcha

Alert: Superuser privileged UNIX program executed: rdefcha
An audited UNIX program started execution with superuser privileges

Alert id        1406
Date and time   13May2003 21:59:05.12
Path            /usr/local/bin/rdefcha
User            C##BSG1  SUSAN GAYNOR
Job name        C##BSG1
System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1406: Superuser privileged UNIX program executed: rdefcha

Alert 1406: Superuser privileged UNIX program executed: rdefcha
```

The alert shows the path of the program that has setuid privileges and the user who started execution of the program.

Superuser privileged shell obtained by user (1407)

An alert is generated when a user uses the UNIX **su** command to obtain a shell with superuser privileges.

To receive this alert, you must have successful READ logging specified on the BPX.SUPERUSER FACILITY profile.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: Superuser privileged shell obtained by user C##BSG1

Alert: Superuser privileged shell obtained by user C##BSG1
A user used su to obtain a shell with superuser privileges

Alert id        1407
Date and time   14May2003 14:15:21.98
User            C##BSG1  SUSAN GAYNOR
Job name        C##BSG1
System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1407: Superuser privileged shell obtained by user C##BSG1

Alert 1407: Superuser privileged shell obtained by user C##BSG1
```

The report shows the user who used **su** to obtain a shell with superuser privileges. This user is able to read and write any file or directory on the UNIX subsystem.

Superuser privileges set on UNIX program (1408)

This alert is generated if the setuid bit is set on a program owned by a UNIX superuser. A program with these privileges executes with superuser authority, and can thus access any UNIX file or data set.

Note: Changing the owner to uid 0 of a program with setuid enabled resets the setuid bit, so it is not a security exposure.

To receive this alert, you must have SETROPTS setting LOGOPTIONS(ALWAYS(FSSEC)) enabled.

The e-mail format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: Superuser privileges set on UNIX program collogs

Alert: Superuser privileges set on UNIX program collogs
The setuid bit is specified on a UNIX program owned by a superuser

Alert id        1408
Date and time   28Mar2003 11:49:33.66
Path            /usr/local/bin/collogs
User            C##BER2  ERWIN RETTICH
Job name        C##BER2
System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1408: Superuser privileges set on UNIX program collogs

Alert 1408: Superuser privileges set on UNIX program collogs
```

The alert shows the path of the program and the user who changed the permission so that the program executes with superuser privileges. If you use a CKFREEZE file created with parameter UNIX=YES, the UNIX path in the report is an absolute path.

Extended attribute changed (1409)

If this alert is activated, a notification message is generated when a change is detected in the extended attributes settings (APF, program control, or _BPX_SHAREAS) for a UNIX file or program. To receive this alert, the level of the z/OS system must be at least 1.11.

The e-mail format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert Extended attribute changed for <Unix-filename>

Alert Extended attribute changed for <Unix-filename>

   Alert id         1409
   Previous value   <old value>
   New value        <new value>
   Date and time    Date(9) Time(11)
   Path             Unix pathname
   User             User(8)Name
   Job name         JobName
   System id        System
```

In the e-mail notification, *old value* and *new value* can contain a combination of the following values: Shared library, APF authorized, and Program controlled.

The text message format of the alert is:

```
Subject: Alert 1409: Extended attribute changed (APS-> APS) by <userid> for <unix file name>.

Alert 1409: Extended attribute changed (APS-> APS) by <userid> for <unix file name>

The extended attributes of a UNIX file unix file name changed. The old and new extended
attributes are shown between the parentheses. The string APS stands for the extended attributes:
APF Authorized, Program controlled, and Shared Library. The command was issued by userid.
```

RACF control alerts

These alerts report on RACF SETROPTS setting changes.

Global security countermeasure activated (1501)

An alert is sent when a RACF SETROPTS command tightens the security of the system.

Note: The condition that triggers this alert is a subset of those conditions that trigger alert 1503. The only reason to select both alerts is when you want to send them to different recipients.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Global security countermeasure activated by C##BNA2

Alert: Global security countermeasure activated by C##BNA2
SETROPTS command tightened system security

   Alert id        1501
   Date and time   23Jan2003 12:13:34.58
   RACF command    SETROPTS
                   LOGOPTIONS(NEVER(FACILITY),FAILURES(DATASET))
```

```
   User            C##BNA2  NICK AFTERSOCK
   Result          Success
   Job name        C##BNA2
   System id       DINO
```

The text message format of the alert is:

```
Subject: Alert 1501: Global security countermeasure activated by C##BNA2

Alert 1501: Global security countermeasure activated by C##BNA2: SETROPTS
LOGOPTIONS(NEVER(FACILITY),FAILURES(DATASET)) PASSWORD(NOHISTORY)
```

The alert shows the executed RACF command, the user that executed the command, and the return status of the command.

Global security countermeasure deactivated (1502)

An alert is generated when a RACF SETROPTS command degraded the security of the system. This alert is available separately from 1503. It ensures a more timely notification through a cell phone message when zSecure Alert is sure that a countermeasure is being deactivated.

Note: The condition that triggers this alert is a subset of those conditions that trigger alert 1503. The only reason to select both alerts is when you want to send them to different recipients.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Global security countermeasure deactivated by C##BNAT

Alert: Global security countermeasure deactivated by C##BNAT
SETROPTS command loosened system security

   Alert id        1502
   Date and time   23Jan2003 11:51:56.01
   RACF command    SETROPTS NOSAUDIT
   User            C##BNAT  NICK AFTERSOCK
   Result          Success
   Job name        C##BNAT
   System id       DINO
```

The text message format of the alert is:

```
Subject: Alert 1502: Global security countermeasure deactivated by C##BNAT

Alert 1502: Global security countermeasure deactivated by C##BNAT: SETROPTS ADSP
NOSAUDIT <Ignored>
```

The alert shows the executed RACF command, the user that executed the command, and the return status of the command.

Global security countermeasure or option changed (1503)

An alert is generated when a RACF SETROPTS command changed the security of the system.

Note: The conditions that trigger alerts 1501 and 1502 are subsets of those conditions that trigger alert 1503. The only reason to select alerts 1501 or 1052 combined with alert 1503 is when you want to send them to different recipients.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: Global security countermeasure changed by C##BNAT

Alert: Global security countermeasure changed by C##BNAT
SETROPTS command changed system security

   Alert id        1503
   Date and time   23Jan2003 11:51:56.01
   RACF command    SETROPTS NOSAUDIT
   User            C##BNAT  NICK AFTERSOCK
   Result          Success
   Job name        C##BNAT
   System id       DINO
```

The text message format of the alert is:

```
Subject: Alert 1503: Global security countermeasure changed by C##BNAT

Alert 1503: Global security countermeasure changed by C##BNAT: SETROPTS ADSP
NOSAUDIT <Ignored>
```

The alert shows the executed RACF command, the user that executed the command, and the return status of the command.

RACF Resource class activated (1504)

This alert is generated when a RACF resource class is detected to have been activated. Because this alert is based on a comparison of two system snapshots, it does not provide any information about how the change was accomplished.

The email format of the alert is:

```
From: C2POLICE at IDFX
Subject: Alert: RACF resource class activated: DASDVOL

Alert: RACF resource class activated: DASDVOL
A change in the status of a RACF resource class has been detected

 Alert id  1504
 CLASS   DASDVOL
 Status   Active
 System ID  IDFX
```

The text message format of the alert is:

```
Subject: Alert 1504: RACF resource class activated: DASDVOL
Alert 1504: RACF resource class activated: DASDVOL
```

The alert shows the resource class that was activated. Because this alert is based on a comparison of two system snapshots, it does not provide any information about how the change was accomplished.

RACF Resource class deactivated (1505)

This alert is generated when a RACF resource class is detected to have been deactivated. Because this alert is based on a comparison of two system snapshots, it does not provide any information about how the change was accomplished.

The email format of the alert is:

```
From: C2POLICE at IDFX
Subject: Alert: RACF resource class deactivated: DASDVOL

Alert: RACF resource class deactivated: DASDVOL
A change in the status of a RACF resource class has been detected
```

```
Alert id  1505
CLASS   DASDVOL
Status   Inactive
System ID  IDFX
```

The text message format of the alert is:

```
Subject: Alert 1505: RACF resource class deactivated: DASDVOL
Alert 1505: RACF resource class deactivated: DASDVOL
```

The alert shows the resource class that was deactivated. Because this alert is based on a comparison of two system snapshots, it does not provide any information about how the change was accomplished.

System alerts

The following alerts are for monitoring general system events.

SMF data loss started (1601)

This alert is generated when WTO reports that SMF data loss has started. It is reported in messages IEE351I, IEE979W, and IEE989I.

Note: You can choose to activate alert 1602 so that you are notified when the immediate exposure passes.

To receive this alert, you must receive WTO messages IEE351I, IEE979W, and IEE989I.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: SMF data loss started

Alert: SMF data loss started
System messages report that SMF data loss has started

   Alert id        1601
   Date and time   10Feb2003 16:36:27.07
   WTO message     IEE979W SMF DATA LOST - NO BUFFER SPACE
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1601: SMF data loss started. WTO msgid: IEE979W

Alert 1601: SMF data loss started. WTO msgid: IEE979W
```

The generated email contains only the issued WTO message.

SMF logging resumed after failure (1602)

This alert is generated when SMF data was lost due to full buffers, but the system has resumed logging.

Note: You can choose to activate this alert so that you are notified when the immediate exposure indicated by alert 1601 passes.

To receive this alert, you must log SMF record type 7.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: SMF logging resumed after failure
```

```
Alert: SMF logging resumed after failure
SMF data is lost, but the system has resumed logging

   Alert id        1602
   Start of loss   10Feb2003 17:35:58.97
   Date and time   10Feb2003 17:36:27.12
   #records lost   4121
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 1602: SMF logging resumed after failure.  4121 records lost.

Alert 1602: SMF logging resumed after failure. 4121 records lost.
```

The generated email contains the start time (`Start of loss`) and end time (`Resume time`) of the period when data was lost. It also indicates the number of SMF records that were lost.

SVC definition changed (1603)

This alert is generated when a change is detected in the definition of an SVC in the SVC-table or the SVC ESR-table. Because this alert is based on a comparison of two system snapshots, it does not provide any information about how the change was accomplished.

The email format of the alert is:

```
From: C2POLICE at IDFX
Subject: Alert: SVC Definition changed: SVC/ESR 220

Alert: SVC Definition changed: SVC/ESR 220
A change in the definition of an SVC has been detected

 Alert id    1603
 SVC/ESR number  220/
 Address     00147080
 APF      Yes
 System ID    IDEX
```

The text message format of the alert is:

```
Subject: Alert 1603: SVC Definition changed: SVC/ESR 220/
Alert 1603: SVC Definition changed: SVC/ESR 220/ at address 00147080 APF
```

This alert shows the SVC and ESR number of the SVC that was changed. The current address of the SVC code is shown together with the current APF status. Because this alert is based on a comparison of two system snapshots, it does not provide any information about how the change was accomplished.

IBM Health Checker found low severity problem (1604)

This alert is generated when WTO reports that IBM Health Checker found a low severity problem. It is reported in message HZS0001I.

To receive this alert, you must receive WTO message HZS0001I.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: IBM Health Checker found low severity problem

Alert: IBM Health Checker found low severity problem
Check found a problem that should be investigated

  Alert id       1604
```

```
  Date and time  10Feb2010 16:36:27.07
  System ID      DINO
  WTO message    HZS0001I CHECK(IBMGRS,GRS_SYNCHRES):


                 ISGH0305E Global Resource Serialization synchronous
                 RESERVE processing
                 is not active.
```

The text message format of the alert is:

```
Subject: Alert 1604: IBM Health Checker low severity: HZS0001I CHECK(IBMGRS,GRS_SYNCHRES):
Alert 1604:  IBM Health Checker low severity: HZS0001I CHECK(IBMGRS,GRS_SYNCHRES):
```

IBM Health Checker found medium severity problem (1605)

This alert is generated when WTO reports that IBM Health Checker found a medium severity problem. It is reported in message HZS0002E.

To receive this alert, you must receive WTO message HZS0002E,

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: IBM Health Checker found medium severity problem

Alert: IBM Health Checker found medium severity problem
Check found a problem that should be investigated

  Alert id       1605
  Date and time  10Feb2010 16:36:27.07
  System ID      DINO
  WTO message    HZS0002E CHECK(IBMASM,ASM_LOCAL_SLOT_USAGE):


                 ILRH0107E Page data set slot usage threshold met or
                 exceeded
```

The text message format of the alert is:

```
Subject: Alert 1605: IBM Health Checker medium severity: HZS0002E CHECK(IBMASM,ASM_LOCAL_SLOT_USAGE):
Alert 1605:  IBM Health Checker medium severity: HZS0002E CHECK(IBMASM,ASM_LOCAL_SLOT_USAGE):
```

IBM Health Checker found high severity problem (1606)

This alert is generated when WTO reports that IBM Health Checker found a high severity problem. It is reported in message HZS0003E.

To receive this alert, you must receive WTO message HZS0003E,

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: IBM Health Checker found high severity problem

Alert: IBM Health Checker found high severity problem
Check found a problem that should be investigated

  Alert id       1606
  Date and time  10Feb2010 16:36:27.07
  System ID      DINO
  WTO message    HZS0003E CHECK(IBMXCF,XCF_CDS_SPOF):

                 IXCH0242E One or more couple data sets have a single
                 point of failure.
```

The text message format of the alert is:

```
Subject: Alert 1606: IBM Health Checker high severity: HZS0003E CHECK(IBMXCF,XCF_CDS_SPOF):
Alert 1606:  IBM Health Checker high severity: HZS0003E CHECK(IBMXCF,XCF_CDS_SPOF):
```

SMF record flood detected (1607)

This alert is generated when WTO reports that SMF record flood is detected. It is reported in message IFA780A.

To receive this alert, you must receive WTO message IFA780A.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: SMF record flood detected

Alert: SMF record flood detected
System messages report SMF record flood detected
   Alert id        1607
   Date and time   03May2010 17:50:05.46
   WTO message     IFA780A SMF RECORD FLOOD MSG FILTER FOR TYPE 40
                   EXCEEDED AT TIME=
   System ID       NMPIPL87
```

The text message format of the alert is:

```
Subject: Alert 1607: SMF record flood detected. WTO msgid:IFA780A SMF
RECORD FLOOD MSG FILTER FOR TYPE 40 EXCEEDED AT TIME=
Alert 1607:  SMF record flood detected. WTO msgid:IFA780A SMF RECORD FLOOD
MSG FILTER FOR TYPE 40 EXCEEDED AT TIME=
```

SMF record flood detected (1608)

This alert is generated when WTO reports that SMF record flood starts dropping records. It is reported in message IFA782A.

To receive this alert, you must receive WTO message IFA782A.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: SMF record flood starts dropping records

Alert: SMF record flood starts dropping records
System messages report SMF record flood starts dropping records
   Alert id        1608
   Date and time   03May2010 17:00:00.33
   WTO message     IFA782A SMF RECORD FLOOD DROP FILTER FOR TYPE 74
                   EXCEEDED AT TIME=
   System ID       NMPIPL87
```

The text message format of the alert is:

```
Subject: Alert 1608: SMF record flood starts dropping records. WTO
msgid:IFA782A SMF RECORD FLOOD DROP FILTER FOR TYPE 74 EXCEEDED AT TIME=
Alert 1608: SMF record flood starts dropping records. WTO msgid:IFA782A SMF
RECORD FLOOD DROP FILTER FOR TYPE 74 EXCEEDED AT TIME=
```

Attacks blocked by filter rules are no longer logged – audit trail incomplete (1609)

This alert is generated when logging for packet filtering is no longer enabled.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Attacks blocked by filter rules are no longer logged

Alert: Attacks blocked by filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP
   Alert id      1609
   Changed field IPSEC_LOGENABLE(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

The text message format of the alert is:

```
Subject: Alert 1609: Attacks blocked by filter rules are no longer logged - audit
trail incomplete in TCP/IP stack TCPIP

Alert 1609: Attacks blocked by filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP
```

The generated email shows that the IP_STACK field IPSEC_LOGENABLE indicates that logging is not enabled for packet filtering. The alert contains the name of the changed field (IPSEC_LOGENABLE), and the old value of the field (Yes), its new value (No), and the security direction (-).

Attacks blocked by default filter rules are no longer logged – audit trail incomplete (1610)

This alert is generated when logging for packets that are denied by the implicit default rules is no longer enabled.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Attacks blocked by default filter rules are no longer logged

Alert: Attacks blocked by default filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP
   Alert id      1610
   Changed field IPSEC_LOGIMPLICIT(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

The text message format of the alert is:

```
Subject: Alert 1610: Attacks blocked by default filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP

Alert 1610: Attacks blocked by default filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP
```

The generated email shows that the IP_STACK field IPSEC_LOGIMPLICIT indicates that logging is not enabled for packets that are denied by the implicit default rules.

SMF 119 subtype is no longer written - audit trail incomplete (1611)

This alert is generated when SMF 119 records are no longer written when any of the following actions occur:

- A user starts the FTP client command (FTPCLIENT)
- Statistics related to LINK utilization become available (IFSTAT)
- A tunnel is added, removed, activated, or deactivated (IPSECURITY)
- Statistics related to reserved PORT utilization become available (PORTSTAT)
- A TCP connection is established (TCPINIT)

- A TCP/IP stack is activated or terminated (TCPIPSTACK)
- TCP/IP statistics become available (TCPIPSTAT)
- A TCP connection is terminated (TCPTERM)
- The TSO Telnet Client code starts or ends a connection (TN3270CLIENT)
- A UDP socket is closed (UDPTERM)

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: SMF 119 FTPCLIENT is no longer written by stack name

Alert: SMF 119 FTPCLIENT is no longer written -
audit trail incomplete in TCP/IP stack TCPIP
   Alert id      1611
   Changed field SMF119_FTPCLIENT(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

The text message format of the alert is:

```
Subject: Alert 1611: SMF 119 FTPCLIENT is no longer written - audit trail incomplete
in TCP/IP stack TCPIP

Alert 1611: SMF 119 FTPCLIENT is no longer written -
audit trail incomplete in TCP/IP stack TCPIP
```

The generated email shows that the IP_STACK flag field corresponding with the associated SMF 119 subtype indicates that records of the given subtype will not be written.

IP filtering support and IPSec tunnel support deactivated (1612)

This alert is generated when IPv4 or IPv6 IP filtering support and IPSec tunnel support are no longer activated.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: IPv4 IP filtering support and IPsec tunnel support deactivated

Alert: IPv4 IP filtering support and IPsec tunnel support deactivated
in TCP/IP stack TCPIP
   Alert id      1612
   Changed field IPCONFIG_IPSECURITY(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

The text message format of the alert is:

```
Subject: Alert 1612: IPv4 IP filtering support and IPsec tunnel support deactivated
in TCP/IP stack TCPIP

Alert 1612: IPv4 IP filtering support and IPsec tunnel
support deactivated in TCP/IP stack TCPIP
```

The generated email shows that the IP_STACK field IPCONFIG_IPSECURITY indicates that IPv4 IP filtering and IPSec tunnel support are not activated, or that the IP_STACK field IPCONFIG6_IPSECURITY indicates that IPv6 IP filtering and IPSec tunnel support are not activated.

Ports below 1024 are not reserved anymore (1613)

This alert is generated when TCP or UDP ports 1 - 1023 are no longer reserved for users by the PORT and PORTRANGE statements.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: UDP ports below 1024 are not reserved anymore by stack name

Alert: UDP ports below 1024 are not reserved anymore in
TCP/IP stack TCPIP
   Alert id      1613
   Changed field UDP_RESTRICTLOWPORTS(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

The text message format of the alert is:

```
Subject: Alert 1613: UDP ports below 1024 are not reserved anymore in TCP/IP stack
TCPIP

Alert 1613: UDP ports below 1024 are not reserved anymore in TCP/IP stack TCPIP
```

The generated email shows that the IP_STACK field TCP_RESTRICTLOWPORTS indicates that TCP ports 1 - 1023 are not reserved for users by the PORT and PORTRANGE statements, or that the IP_STACK field UDP_RESTRICTLOWPORTS indicates that UDP ports 1 - 1023 are not reserved for users by the PORT and PORTRANGE statements.

Interface security class changed (1614)

This alert is generated when the security class used for IP filtering with this interface changes.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Security class changed for interface interface

Alert: Interface EELINK security class has changed in
TCP/IP stack TCPIP
   Alert id       1614
   Changed field  SECCLASS(255->238)
   Interface      EELINK
   Security class 238
   Stack          TCPIP
   System ID      DINO
```

The text message format of the alert is:

```
Subject: Alert 1614: Interface EELINK           security class has changed in TCP/IP
stack TCPIP

Alert 1614: Interface EELINK security class has changed in TCP/IP stack TCPIP
```

The generated email contains the IPv4 or IPv6 interface name, and the security class used for IP filtering with this interface.

IP filter rules changed (1615)

This alert is generated when an IP filter rule is changed, added, or deleted.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: IP filter rules changed in TCP/IP stack TCPIP

Alert: IP filter rules changed in TCP/IP stack TCPIP
   Alert id                    1615
   Kind of change              CHG-
   Changed fields              LOG(Yes->No)-
```

```
   Source IP
   Source prefix length          0
   Source port                   0
   Destination IP
   Destination prefix length     0
   Destination port              0
   Protocol
   Type                          64
   Code                          0
   Packet filter logging enabled No
   Routing                       LOCAL
   Security class                0
   Stack                         TCPIP
   System ID                     DINO
```

The text message format of the alert is:

```
Subject: Alert 1615: IP filter rules changed in TCP/IP stack TCPIP

Alert:1615: IP filter rules changed in TCP/IP stack TCPIP
```

The generated email contains several components of the changed, added, or deleted IP filter rule: the source IP address for the outbound rule, the prefix length for the source subnet address, the source port for the outbound rule (for TCP or UDP traffic), the destination IP address for the outbound rule, the destination subnet address prefix length, the destination port for the outbound rule (matching the source port for the generated inbound rule), the type of traffic that the rule applies to, the ICMP value (for ICMP traffic), an indication whether packet filter logging is enabled for the default filter rule, the type of packet routing that the rule applies to, and the security class of the rule.

Group alerts

Connected to an important group (1701)

This alert is generated when a userid is connected to an important group.

To receive this alert, you must have SETROPTS setting SAUDIT, AUDIT(USER), or AUDIT(GROUP) enabled.

The e-mail format of the alert is:

```
From:           C2POLICE at DINO
Subject:        Alert: C2RMUS02 issued connect to important group SYS1 for C2RMUS01

Alert: C2RMUS02 issued connect to important group SYS1 for C2RMUS01
User connected to an important group
   Alert id        1701
   Date and time   09Mar2005 14:49:55.90
   User            C2RMUS01
   Group           SYS1
   Result          Success
   Issued by       C2RMUS02
   Job name        C2RMUS0
   System ID       DINO
   Command         CONNECT C2RMUS01 GROUP(SYS1)
```

The text message format of the alert is:

```
Subject: Alert 1701:  C2RMUS02 issued connect to important group SYS1 for C2RMUS01

Alert 1701:  C2RMUS02 issued connect to important group SYS1 for C2RMUS01
```

The generated e-mail report shows which userid is connected to which important group.

This alert enables you to customize the groups for your site. When selecting the alert, you are prompted with a panel where you specify up to 20 important groups. It also shows the command that was employed to connect the userid, as well as the issuer of the command. See “Important groups (1701) configuration” on page 98.

Predefined ACF2 alerts

This chapter describes the ACF2 alerts that are shipped with zSecure Alert.

User alerts

The following alerts are used to monitor events that pertain to specific users and for auditing changes to users.

Logon with emergency logonid (2102)

An alert is sent if a logonid that is meant for emergencies is used for TSO logon or batch job submission.

To receive this alert, you must log SMF record type 30 subtype 1.

The e-mail format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Emergency user IBMUSER  logged on

Alert: Emergency user IBMUSER logged on
Successful logon or job submit with a logonid meant for emergencies

   Alert id        2102
   Date and time   03Feb2006 09:38:44.94
   User            IBMUSER  IBM DEFAULT USER
   Job name + id   IBMUSER  TSU05900
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2102: emergency user IBMUSER  logged on

Alert 2102: emergency user IBMUSER logged on
```

The generated e-mail report shows the logonid used to log on to the system and whether the logon succeeded.

This alert enables you to configure the panel for your site. When selecting the alert, you are prompted with a panel. You can enter up to 10 logonids that must only be used in case of emergencies. See “Emergency user configuration (alerts 1102 and 2102)” on page 96.

Highly authorized user revoked for password (2104)

This alert is triggered when a user with a system-level authority (SECURITY, NON-CNCL, or READALL) is revoked because of excessive invalid password attempts. The alert can be caused by an intruder trying to guess the password.

Note: You must take care not all your users with system authority get revoked at the same time. You must have some procedure to make sure at least one unrevoked logonid with SECURITY authority is reinstated.

The e-mail format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Highly authorized user C##CX44  revoked for password violations

Alert: Highly authorized user C##CX44 revoked for password violations
System-level authorized user revoked due to excessive password attempts

   Alert id        2104
   Date and time   07Feb2006 14:58:27.13
   User            C##CX44  TEST USER
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2104: Highly authorized user C##CX44  revoked for password violations

Alert 2104: Highly authorized user C##CX44 revoked for password violations
```

The report shows the logonid and accompanying name that is revoked for excessive password violations.

System authority granted (2105)

An alert is generated when a user obtains system-level authority (SECURITY, NON-CNCL, or READALL).

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: System authority granted to C##BMR2

Alert: System authority granted to C##BMR2
System-level authority granted to user

   Alert id        2105
   Date and time   29May2006 13:25:12.42
   Authority       SECURITY
   Granted to      C##BMR2  MARY ROBERTSON
   Logonid         C##BMR1  MARY ROBERTSON
   Job name        C##BMR1
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2105: System authority granted to C##BMR2  by C##BMR1

Alert 2105: System authority SECURITY granted to C##BMR2 by C##BMR1
```

The report shows the system authority that is granted, the user that is granted the authority, and the user that performed the ACF2 command.

System authority removed (2106)

An alert is sent when a system-level authority (SECURITY, NON-CNCL, or READALL) is removed from a user.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: System authority removed from C##BMR1

Alert: System authority removed from C##BMR2
System-level authority removed from user

   Alert id        2106
   Date and time   29May2006 13:25:16.15
   Authority       SECURITY
```

```
Removed from    C##BMR2  MARY ROBERTSON
Logonid         C##BMR1  MARY ROBERTSON
Job name        C##BMR1
System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2106: System authority removed from C##BMR2  by C##BMR1

Alert 2106: System authority SECURITY removed from C##BMR2 by C##BMR1
```

The report shows the authority that is removed, the user whose authority is removed, and the user that performed the ACF2 command.

Invalid password attempts exceed limit (2111)

An alert is sent if too many failed logon attempts are made with an invalid password for one specific logon ID in a specific time window. The measurement interval is the sum of the REPORT options **Interval** and **AverageInterval**. See the information about the REPORT command in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Too many is defined as 5 attempts or more. If you want to use another limit, you must copy the alert to an installation defined alert. You must adapt all four instances of

```
#history(nd,<5), #total(nd,>=5),
```

in the new skeleton member to use the limit you want instead of 5.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Invalid password attempts exceed limit for C##BSG2

Alert: Invalid password attempts exceed limit for C##BSG2
Excessive number of password attempts by user

   Alert id        2111
   Date and time   03Mar2006 13:30:04.39 - 03Mar2003 13:39:23.78
   Attempts        6
   User            C##BSG2  SUSAN GAYNOR
   Result          Violation
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2111: Invalid password attempts exceed limit for C##BSG2

Alert 2111: Invalid password attempts exceed limit for C##BSG2.
```

This alert is also raised for password phrase violations. It takes into account a combined number of violations for passwords and password phrases.

The generated email report shows the interval in which the logon attempts occurred and the number of attempts. It also shows the logon ID that was used for trying to log on to the system and the status of the logon. In this alert, the logons are always violations.

Password history flushed (2112)

An alert is sent if the password for a specific logon ID is changed more often than the password history GSO setting in a specific time window. It means that the user flushed the entire password history, enabling reuse of a previous password. The measurement interval is the sum of the REPORT options **Interval** and

AverageInterval. See the information about the REPORT command in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Note: Alert 2112 and 2113 are related. When a report interval ends while a password history is being flushed, alert 2113 is triggered; alert 2112 occurs when flushing completes. If you receive multiple alerts 2113 for the same user without alert 2112, it is likely that the history is flushed or being flushed, but the user might have taken some more time for it.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: Password history flushed for C##BSG2

Alert: Password history flushed for C##BSG2
Repeated PASSWORD commands flush password history

   Alert id        2112
   Date and time   05Mar2006 11:47:11.21 - 03Mar2006 11:47:12.04
   Pwd changes     33
   User            C##BSG2  SUSAN GAYNOR
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2112: Password history flushed for C##BSG2

Alert 2112: Password history flushed for C##BSG2
```

The generated email report shows the interval in which the password history flushing occurred, the number of password changes, and the logon ID of the user that flushed the password history of the user.

Suspect password changes (2113)

An alert is sent if the password for a specific logon ID is changed five times or more in a specific time window. The password change is not so often that the password history has been flushed completely, which would result in alert 2112. If you want to use another limit, you must copy the alert to an installation defined alert. Adapt all four instances of

```
#history(nd,<5) #total(nd,>=5),
```

in the new skeleton member to use the wanted limit instead of five.

For further explanation, see "Password history flushed (2112)" in “Password history flushed (2112)” on page 78.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: Suspect password changes for C##BSG2

Alert: Suspect password changes for C##BSG2
Excessive number of PASSWORD commands by user

   Alert id        2113
   Date and time   03Mar2006 15:17:12.32 - 03Mar2006 15:17:13.11
   Pwd changes     7
   User            C##BSG2  SUSAN GAYNOR
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2113: Suspect password changes for C##BSG2

Alert 2113: Suspect password changes for C##BSG2
```

The generated email report shows the interval in which the password changes occurred, the number of password changes, and the logon ID that has its password changed many times.

Too many violations (2115)

This alert is generated when more violations than a configured number are recorded for a specific logon ID in the interval as specified with the REPORT option . See the information about the REPORT command in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

The email format of the alert is:

```
From:        C2POLICE at DINO
Subject:     Alert: 15 violations recorded for user C2RMUS01

Alert: 15 violations recorded for user C2RMUS01
Number of violation exceeds the configured 10

   Alert id        2115
   Date and time   09Mar2006 14:49:55.90 - 09Mar2006 14:54:57.89
   Violations      15
   User            C2RMUS01
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2115: 15 violations recorded for user C2RMUS01

Alert 2115: 15 violations recorded for user C2RMUS01
```

This alert allows customization for your site. When selecting the alert you are prompted with a panel where you specify the number of violations you consider excessive. Furthermore, you can specify up to 10 logon IDs (or logon ID masks) to be excluded. See "Number of violations and logonids to exclude (2115) configuration" on page 99.

SECURITY authority used by non-SECURITY logon ID (2116)

An alert is generated when a user without SECURITY accesses a data set with SECURITY authority. It implies that the user without SECURITY authority can access all data sets and has the potential to successfully execute commands that require SECURITY. This condition can be set by APF-authorized software.

Note: You must analyze the SMF records cut for the job up to the time the alert was issued as a first attempt to identify the responsible program.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: non-SECURITY user C##BDV1 accessed data set with SECURITY

Alert: non-SECURITY user C##BDV1 accessed data set with SECURITY
Successful data set access using SECURITY by user without SECURITY

   Alert id        2116
   Date and time   17Jan2003 03:00:16.89
   Data set        D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00
   Access          UPDATE
```

```
   User            C##BDV1  DIONNE VONT
   Result          LOGGING
   Job name        C##BDV1
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2116: non-SECURITY user C##BDV1  accessed (UPDATE  ) with
SECURITY data set D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00

Alert 2116: non-SECURITY user C##BDV1 accessed (UPDATE  ) with SECURITY
data set D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00
```

NON-CNCL authority used by non-NON-CNCL logon ID (2117)

An alert is generated when a user without NON-CNCL accesses a data set with NON-CNCL authority. It implies that the user can access all data sets. This condition can be set by APF-authorized software.

Note: You must analyze the SMF records cut for the job up to the time the alert was issued as a first attempt to identify the responsible program.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: non-NON-CNCL user C##BDV1 accessed data set with NON-CNCL

Alert: non-NON-CNCL user C##BDV1 accessed data set with NON-CNCL
Successful data set access using NON-CNCL by user without NON-CNCL

   Alert id        2117
   Date and time   17Jan2003 03:00:16.89
   Data set        D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00
   Access          UPDATE
   User            C##BDV1  DIONNE VONT
   Result          LOGGING
   Job name        C##BDV1
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2117: non-NON-CNCL user C##BDV1  accessed (UPDATE  ) with
NON-CNCL data set D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00

Alert 2117: non-NON-CNCL user C##BDV1 accessed (UPDATE  ) with NON-CNCL
data set D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00
```

READALL authority used by non-READALL logon ID (2118)

An alert is generated when a user without READALL accesses a data set with READALL authority. It implies that the user can read all data sets. This condition can be set by APF-authorized software.

Note: You must analyze the SMF records cut for the job up to the time the alert was issued as a first attempt to identify the responsible program.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: non-READALL user C##BDV1 accessed data set with READALL

Alert: non-READALL user C##BDV1 accessed data set with READALL
Successful data set access using READALL by user without READALL

   Alert id        2118
   Date and time   17Jan2003 03:00:16.89
   Data set        D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00
```

```
   Access          READ
   User            C##BDV1  DIONNE VONT
   Result          LOGGING
   Job name        C##BDV1
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2118: non-READALL user C##BDV1  accessed (READ  ) with
READALL data set D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00

Alert 2118: non-READALL user C##BDV1 accessed (READ  ) with READALL
data set D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00
```

Data set alerts

This section describes the predefined alerts for data set access.

WARNING mode access on data set (2201)

A data set is accessed and access is granted because of warning mode.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: WARNING mode READ    on data set CDS.SCDSSAMP

Alert: WARNING mode READ on data set CDS.SCDSSAMP
Data set access granted due to warning mode

   Alert id        2201
   Date and time   21Jan2006 09:11:11.01
   Data set        CDS.SCDSSAMP
   Granted access  READ
   Rule            CDS.-
   User            C##BMR1  MARY ROBERTSON
   Job name        C##BMR1
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2201: WARNING mode READ    by C##BMR1 on data set
CDS.SCDSSAMP

Alert 2201: WARNING mode READ by C##BMR1 on data set CDS.SCDSSAMP
```

The report shows the data set, the user that requested access to it, the rule against which the access is checked, and the access that is granted.

A rule in WARNING mode grants any access to the resource, including what the rule would not allow otherwise. WARNING mode is typically used to analyze what the effects of the access settings of a rule are before the access control is enforced. It is used as a temporary measure to overcome production problems. If you receive these alerts, you must verify whether the access can be allowed. If so, change the access settings of the rule accordingly. If this access is not supposed to occur, take remedial action as required.

Update on APF data set (2204)

An alert is sent when an APF authorized data set is updated.

The e-mail format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Update by C##ASCH  on APF data set C##A.D.C##NEW.APF.LOAD

Alert: Update by C##ASCH on APF data set C##A.D.C##NEW.APF.LOAD
```

```
APF data set successfully updated

   Alert id        2204
   Date and time   03Feb2003 10:12:05.30
   Data set        C##A.D.C##NEW.APF.LOAD
   Access          UPDATE
   User            C##ASCH
   Result          LOGGING
   Job name        C##ASCHL
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2204: Update by user C##ASCH  on APF data set
C##A.D.C##NEW.APF.LOAD

Alert 2204: Update by user C##ASCH on APF data set C##A.D.C##NEW.APF.LOAD
```

The alert shows the data set that was updated, the employed access level, and the user who accessed the data set.

Data set added to APF list (2205)

An alert is generated when a data set is dynamically added to the APF list using the SET PROG or SETPROG command.

To generate this alert, WTO message CSV410I must be available and selected for processing.

The e-mail format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: Data set added to APF list: SYSPROG.APF.LOAD

Alert: Data set added to APF list: SYSPROG.APF.LOAD
A data set is dynamically added to the APF list

   Alert id        2205
   Date and time   21Feb2003 11:44:36.71
   Data set        SYSPROG.APF.LOAD
   Volume          <SMS MANAGED>
   Console ID      R##SLIN
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2205: Data set added to APF list from console R##SLIN:
SYSPROG.APF.LOAD

Alert 2205: Data set added to APF list from console R##SLIN:
SYSPROG.APF.LOAD on volume <SMS MANAGED>
```

The alert shows the data set that was added to the APF list, on what volume the data set resides, or, <SMS MANAGED> if it is managed by SMS, and the name of the console from which the user entered the SET PROG or SETPROG command, if entered from SDSF, the console name defaults to the logonid of the user.

Data set removed from APF list (2206)

An alert is generated when a data set is dynamically removed from the APF list using the SET PROG or SETPROG command.

To generate this alert, WTO message CSV410I must be available and selected for processing.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: Data set removed from APF list: SYSPROG.APF.LOAD

Alert: Data set removed from APF list: SYSPROG.APF.LOAD
A data set is dynamically removed from the APF list

Alert id        2206
Date and time   21Feb2003 11:44:36.71
Data set        SYSPROG.APF.LOAD
Volume          <SMS MANAGED>
Console ID      R##SLIN
System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2206: Data set removed from APF list from console R##SLIN:
SYSPROG.APF.LOAD

Alert 2206: APF Data set removed from APF list from console R##SLIN:
SYSPROG.APF.LOAD on volume <SMS MANAGED>
```

The alert shows the data set that was removed from the APF list, on what volume the data set resides, or, <SMS MANAGED> if it is managed by SMS, and the name of the console from which the user entered the SET PROG or SETPROG command, if entered from SDSF, the console name defaults to the logon ID of the user.

Data set addition to APF list detected (2207)

This alert is generated when a data set is added to the APF list by any method. It includes use of the SET PROG or SETPROG command and use of other products. To generate this alert, Extended Monitoring must be active. Because this alert is based on a comparison of two system snapshots, no information is available about the user ID, jobname that was used to add the data set, or the process that was used to perform the addition.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: Data set addition to APF list detected: SYSPROG.APF.LOAD

Alert: Data set addition to APF list detected: SYSPROG.APF.LOAD
An addition of a data set to the APF list has been detected

   Alert id        2207
   Data set        SYSPROG.APF.LOAD
   Volume          <SMS MANAGED>
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2207: Data set addition to APF list detected: SYSPROG.APF.LOAD
Alert 2207: Data set addition to APF list detected: SYSPROG.APF.LOAD
on volume <SMS MANAGED>
```

The alert shows the data set that was added to the APF list and the volume where the data set resides. If the data set is managed by SMS, the volume field shows <SMS MANAGED>. Because this alert is based on a comparison of two system snapshots, it does not provide any information about the user ID, jobname that was used to add the data set, or the process that was used to perform the addition.

Data set removal from APF list detected (2208)

This alert is generated when a data set is removed from the APF list by any method. It includes use of the SET PROG or SETPROG command and use of other

products. To generate this alert, Extended Monitoring must be active. Because this alert is based on a comparison of two system snapshots, it does not provide any information about the userid, jobname that was used to remove the data set, or the process that was used to perform the addition.

The e-mail format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: Data set removal from APF list detected: SYSPROG.APF.LOAD

Alert: Data set removal from APF list detected: SYSPROG.APF.LOAD
A removal of a data set from the APF list has been detected.


   Alert id        2208
   Data set        SYSPROG.APF.LOAD
   Volume          <SMS MANAGED>
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2208: Data set removal from APF list detected: SYSPROG.APF.LOAD
Alert 2208: Data set removal from APF list detected: SYSPROG.APF.LOAD
on volume <SMS MANAGED>
```

The alert shows the data set that was removed from the APF list and on what volume the data set resides (or <SMS MANAGED> if it is managed by SMS). Because this alert is based on a comparison of two system snapshots, it does not provide any information about the userid, jobname that was used to remove the data set, or the process that was used to perform the removal.

General resource alerts

These alerts report on the use of general resources.

Default STC logon ID used for STC (2301)

An alert is sent if a started task uses the default STC logon ID.

To generate this alert, WTO message ACF9CCCD must be available and selected for processing.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: STC default LID ACFSTCID used for STC IEFBR14A

Alert: STC default LID ACFSTCID used for STC IEFBR14A
A started task uses the STC default logonid

   Alert id        2301
   Date and time   11Feb2003 18:14:48.78
   Logonid         ACFSTCID
   Started task    IEFBR14A
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2301: STC default LID ACFSTCID used for STC IEFBR14A

Alert 2301: STC default LID ACFSTCID used for STC IEFBR14A
```

The report shows the ACF2 default logon ID used and the started task member name. This report does not show the user who began the started task.

You can remove the cause of this alert if you define a GSO STC record for this started task. The default logon ID is not checked anymore for this started task.

UNIX alerts

The following alerts are triggered when a UNIX superuser privilege is obtained.

Superuser privileged shell obtained by user (2407)

An alert is generated when a user used the UNIX **su** command to obtain a shell with superuser privileges.

To receive this alert, you must have successful READ logging specified on the BPX.SUPERUSER FACILITY rule entry.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: Superuser privileged shell obtained by user C##BSG1

Alert: Superuser privileged shell obtained by user C##BSG1
A user used su to obtain a shell with superuser privileges

Alert id        2407
Date and time   14May2003 14:15:21.98
User            C##BSG1  SUSAN GAYNOR
Job name        C##BSG1
System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2407: Superuser privileged shell obtained by user C##BSG1

Alert 2407: Superuser privileged shell obtained by user C##BSG1
```

The report shows the user who used **su** to obtain a shell with superuser privileges. This user is able to read and write any file or directory on the UNIX subsystem.

Extended attribute changed (2409)

If this alert is activated, a notification message is generated when a change is detected in the extended attributes settings (APF, program control, or _BPX_SHAREAS) for a UNIX file or program. To receive this alert, the level of the z/OS system must be at least 1.11.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert Extended attribute changed for <Unix-filename>

Alert Extended attribute changed for <Unix-filename>

   Alert id         2409
   Previous value   <old value>
   New value        <new value>
   Date and time    Date(9) Time(11)
   Path             Unix pathname
   User             User(8)Name
   Job name         JobName
   System id        System
```

In the email notification, *old value* and *new value* can contain a combination of the following values: Shared library, APF-authorized, and Program controlled.

The text message format of the alert is:

```
Subject: Alert 2409: Extended attribute changed (APS-> APS) by <userid> for <unix file name>.

Alert 2409: Extended attribute changed (APS-> APS) by <userid> for <unix file name>

The extended attributes of a UNIX file unix file name changed. The old and new extended
attributes are shown between the parentheses. The string APS stands for the extended attributes:
APF Authorized, Program controlled, and Shared Library. The command was issued by userid.
```

ACF2 control alerts

These alerts report on ACF2 GSO setting changes.

Global security countermeasure added (2501)

An alert is sent when an ACF2 GSO setting is added.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Global security countermeasure added by C##BNA2

Alert: Global security countermeasure added by C##BNA2
ACF2 command used to add GSO setting

   Alert id        2501
   Date and time   23Jan2003 12:13:34.58
   Rule key        C-GSO-CRM     PSWD
   Field/value     WRNDAYS/5
   User            C##BNA2  NICK AFTERSOCK
   Job name        C##BNA2
   System id       DINO
```

The text message format of the alert is:

```
Subject: Alert 2501: Global security countermeasure added by C##BNA2

Alert 2501: Global security countermeasure added by C##BNA2: C-GSO-CRM     PSWD
```

The alert shows the GSO rule key, the GSO field and its value, and the user that executed the command.

For SNMP, only one GSO rule key, GSO field, and value is sent with variable `whatParm`.

Global security countermeasure deleted (2502)

An alert is sent when an ACF2 GSO setting is deleted.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Global security countermeasure deleted by C##BNA2

Alert: Global security countermeasure deleted by C##BNA2
ACF2 command used to delete GSO setting

   Alert id        2502
   Date and time   23Jan2003 12:13:34.58
   Rule key        C-GSO-CRM     PSWD
   Field/value     WRNDAYS/5
   User            C##BNA2  NICK AFTERSOCK
   Job name        C##BNA2
   System id       DINO
```

The text message format of the alert is:

```
Subject: Alert 2502: Global security countermeasure deleted by C##BNA2

Alert 2502: Global security countermeasure deleted by C##BNA2: C-GSO-CRM     PSWD
```

The alert shows the GSO rule key, the GSO field and its value, and the user that executed the command.

For SNMP, only one GSO rule key, GSO field, and value is sent with variable whatParm.

Global security countermeasure changed (2503)

An alert is sent when an ACF2 GSO setting is changed.

The e-mail format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Global security countermeasure changed by C##BNA2

Alert: Global security countermeasure changed by C##BNA2
ACF2 command used to change GSO setting

   Alert id        2503
   Date and time   23Jan2003 12:13:34.58
   Rule key        C-GSO-CRM     PSWD
   Field/Old/New   WRNDAYS/5/10
   User            C##BNA2  NICK AFTERSOCK
   Job name        C##BNA2
   System id       DINO
```

The text message format of the alert is:

```
Subject: Alert 2503: Global security countermeasure changed by C##BNA2

Alert 2503: Global security countermeasure changed by C##BNA2: C-GSO-CRM     PSWD
```

The alert shows the GSO rule key, the GSO field and its old and new values, and the user that executed the command.

For SNMP, only one GSO rule key, GSO field, and value is sent with variable whatParm.

System alerts

The following alerts are for monitoring general system events.

SMF data loss started (2601)

This alert is generated when WTO reports that SMF data loss has started. It is reported in messages IEE351I, IEE979W, and IEE989I.

Note: You can choose to activate alert 2602 so that you are notified when the immediate exposure passes.

To receive this alert, you must receive WTO messages IEE351I, IEE979W, and IEE989I.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: SMF data loss started

Alert: SMF data loss started
System messages report that SMF data loss has started

   Alert id        2601
   Date and time   10Feb2003 16:36:27.07
   WTO message     IEE979W SMF DATA LOST - NO BUFFER SPACE
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2601: SMF data loss started. WTO msgid: IEE979W

Alert 2601: SMF data loss started. WTO msgid: IEE979W
```

The generated email contains only the issued WTO message.

SMF data loss started (2602)

This alert is generated when SMF data was lost due to full buffers, but the system has resumed logging.

Note: You can choose to activate this alert so that you are notified when the immediate exposure indicated by alert 2601 passes.

To receive this alert, you must log SMF record type 7.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: SMF logging resumed after failure

Alert: SMF logging resumed after failure
SMF data is lost, but the system has resumed logging

   Alert id        2602
   Start of loss   10Feb2003 17:35:58.97
   Date and time   10Feb2003 17:36:27.12
   #records lost   4121
   System ID       DINO
```

The text message format of the alert is:

```
Subject: Alert 2602: SMF logging resumed after failure.  4121 records lost.

Alert 2602: SMF logging resumed after failure. 4121 records lost.
```

The generated email contains the start time (`Start of loss`) and end time (`Resume time`) of the period when data was lost. It also shows the number of SMF records that were lost.

SVC definition changed (2603)

This alert is generated when a change is detected in the definition of an SVC in the SVC-table or the SVC ESR-table. Because this alert is based on a comparison of two system snapshots, it does not provide any information about how the change was accomplished.

The email format of the alert is:

```
From: C2POLICE at IDFX
Subject: Alert: SVC Definition changed: SVC/ESR 220/

Alert: SVC Definition changed: SVC/ESR 220/
A change in the definition of an SVC has been detected

   Alert id        2603
   SVC/ESR number  220/
   Address         00147080
   APF             Yes
   System ID       IDFX
```

The text message format of the alert is:

```
Subject: Alert 2603: SVC Definition changed: SVC/ESR 220/
Alert 2603: SVC Definition changed: SVC/ESR 220/ at address 00147080 APF
```

This alert shows the SVC and ESR number of the SVC that was changed. The current address of the SVC code is shown together with the current APF status. Because this alert is generated based on a comparison of two system snapshots, no information is available about how the change was accomplished.

IBM Health Checker found low severity problem (2604)

This alert is generated when WTO reports that IBM Health Checker found a low severity problem. It is reported in message HZS0001I.

To receive this alert, you must receive WTO message HZS0001I.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: IBM Health Checker found low severity problem

Alert: IBM Health Checker found low severity problem
Check found a problem that should be investigated

  Alert id       2604
  Date and time  10Feb2010 16:36:27.07
  System ID      DINO
  WTO message    HZS0001I CHECK(IBMGRS,GRS_SYNCHRES):


                 ISGH0305E Global Resource Serialization synchronous
                 RESERVE processing
                 is not active.
```

The text message format of the alert is:

```
Subject: Alert 2604: IBM Health Checker low severity: HZS0001I CHECK(IBMGRS,GRS_SYNCHRES):
Alert 2604:  IBM Health Checker low severity: HZS0001I CHECK(IBMGRS,GRS_SYNCHRES):
```

IBM Health Checker found medium severity problem (2605)

This alert is generated when WTO reports that IBM Health Checker found a medium severity problem. It is reported in message HZS0002E.

To receive this alert, you must receive WTO message HZS0002E,

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: IBM Health Checker found medium severity problem

Alert: IBM Health Checker found medium severity problem
Check found a problem that should be investigated

  Alert id       2605
  Date and time  10Feb2010 16:36:27.07
  System ID      DINO
  WTO message    HZS0002E CHECK(IBMASM,ASM_LOCAL_SLOT_USAGE):


                 ILRH0107E Page data set slot usage threshold met or
                 exceeded
```

The text message format of the alert is:

```
Subject: Alert 2605: IBM Health Checker medium severity: HZS0002E
CHECK(IBMASM,ASM_LOCAL_SLOT_USAGE):
Alert 2605: IBM Health Checker medium severity: HZS0002E
CHECK(IBMASM,ASM_LOCAL_SLOT_USAGE):
```

IBM Health Checker found high severity problem (2606)

This alert is generated when WTO reports that IBM Health Checker found a high severity problem. It is reported in message HZS0003E.

To receive this alert, you must receive WTO message HZS0003E,

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: IBM Health Checker found high severity problem

Alert: IBM Health Checker found high severity problem
Check found a problem that should be investigated

  Alert id       2606
  Date and time  10Feb2010 16:36:27.07
  System ID      DINO
  WTO message    HZS0003E CHECK(IBMXCF,XCF_CDS_SPOF):

                 IXCH0242E One or more couple data sets have a single
                 point of failure.
```

The text message format of the alert is:

```
Subject: Alert 2606: IBM Health Checker high severity: HZS0003E CHECK(IBMXCF,XCF_CDS_SPOF):
Alert 2606:  IBM Health Checker high severity: HZS0003E CHECK(IBMXCF,XCF_CDS_SPOF):
```

SMF record flood detected (2607)

This alert is generated when WTO reports that SMF record flood is detected. It is reported in message IFA780A.

To receive this alert, you must receive WTO message IFA780A.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: SMF record flood detected

Alert: SMF record flood detected
System messages report SMF record flood detected
   Alert id        2607
   Date and time   03May2010 17:50:05.46
   WTO message     IFA780A SMF RECORD FLOOD MSG FILTER FOR TYPE 40
                   EXCEEDED AT TIME=
   System ID       NMPIPL87
```

The text message format of the alert is:

```
Subject: Alert 2607: SMF record flood detected. WTO msgid:IFA780A SMF
RECORD FLOOD MSG FILTER FOR TYPE 40 EXCEEDED AT TIME=
Alert 2607:  SMF record flood detected. WTO msgid:IFA780A SMF RECORD FLOOD
MSG FILTER FOR TYPE 40 EXCEEDED AT TIME=
```

SMF record flood detected (2608)

This alert is generated when WTO reports that SMF record flood starts dropping records. It is reported in message IFA782A.

To receive this alert, you must receive WTO message IFA782A.

The email format of the alert is:

```
From: C2POLICE at DINO
Subject: Alert: SMF record flood starts dropping records

Alert: SMF record flood starts dropping records
System messages report SMF record flood starts dropping records
   Alert id        2608
   Date and time   03May2010 17:00:00.33
   WTO message     IFA782A SMF RECORD FLOOD DROP FILTER FOR TYPE 74
                   EXCEEDED AT TIME=
   System ID       NMPIPL87
```

The text message format of the alert is:

```
Subject: Alert 2608: SMF record flood starts dropping records. WTO
msgid:IFA782A SMF RECORD FLOOD DROP FILTER FOR TYPE 74 EXCEEDED AT TIME=
Alert 2608: SMF record flood starts dropping records. WTO msgid:IFA782A SMF
RECORD FLOOD DROP FILTER FOR TYPE 74 EXCEEDED AT TIME=
```

Attacks blocked by filter rules are no longer logged – audit trail incomplete (2609)

This alert is generated when logging for packet filtering is no longer enabled.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Attacks blocked by filter rules are no longer logged

Alert: Attacks blocked by filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP
   Alert id      2609
   Changed field IPSEC_LOGENABLE(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

The text message format of the alert is:

```
Subject: Alert 2609: Attacks blocked by filter rules are no longer logged - audit
trail incomplete in TCP/IP stack TCPIP

Alert 2609: Attacks blocked by filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP
```

The generated email shows that the IP_STACK field IPSEC_LOGENABLE indicates that logging is not enabled for packet filtering. The alert contains the name of the changed field (IPSEC_LOGENABLE), as well as the old value of the field (Yes), its new value (No), and the security direction (-).

Attacks blocked by default filter rules are no longer logged – audit trail incomplete (2610)

This alert is generated when logging for packets that are denied by the implicit default rules is no longer enabled.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Attacks blocked by default filter rules are no longer logged

Alert: Attacks blocked by default filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP
```

```
   Alert id      2610
   Changed field IPSEC_LOGIMPLICIT(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

The text message format of the alert is:

```
Subject: Alert 2610: Attacks blocked by default filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP

Alert 2610: Attacks blocked by default filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP
```

The generated email shows that the IP_STACK field IPSEC_LOGIMPLICIT indicates that logging is not enabled for packets that are denied by the implicit default rules.

SMF 119 subtype is no longer written - audit trail incomplete (2611)

This alert is generated when SMF 119 records are no longer written when any of the following actions occur:

- A user invokes the FTP client command (FTPCLIENT)
- Statistics related to LINK utilization become available (IFSTAT)
- A tunnel is added, removed, activated, or deactivated (IPSECURITY)
- Statistics related to reserved PORT utilization become available (PORTSTAT)
- A TCP connection is established (TCPINIT)
- A TCP/IP stack is activated or terminated (TCPIPSTACK)
- TCP/IP statistics become available (TCPIPSTAT)
- A TCP connection is terminated (TCPTERM)
- The TSO Telnet Client code starts or ends a connection (TN3270CLIENT)
- A UDP socket is closed (UDPTERM)

The e-mail format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: SMF 119 FTPCLIENT is no longer written by stack name

Alert: SMF 119 FTPCLIENT is no longer written -
audit trail incomplete in TCP/IP stack TCPIP
   Alert id      2611
   Changed field SMF119_FTPCLIENT(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

The text message format of the alert is:

```
Subject: Alert 2611: SMF 119 FTPCLIENT is no longer written - audit trail incomplete
in TCP/IP stack TCPIP

Alert 2611: SMF 119 FTPCLIENT is no longer written -
audit trail incomplete in TCP/IP stack TCPIP
```

The generated e-mail shows that the IP_STACK flag field corresponding with the associated SMF 119 subtype indicates that records of the given subtype will not be written.

IP filtering support and IPSec tunnel support deactivated (2612)

This alert is generated when IPv4 or IPv6 IP filtering support and IPSec tunnel support are no longer activated.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: IPv4 IP filtering support and IPsec tunnel support deactivated

Alert: IPv4 IP filtering support and IPsec tunnel support deactivated
in TCP/IP stack TCPIP
   Alert id      2612
   Changed field IPCONFIG_IPSECURITY(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

The text message format of the alert is:

```
Subject: Alert 2612: IPv4 IP filtering support and IPsec tunnel support deactivated
in TCP/IP stack TCPIP

Alert 2612: IPv4 IP filtering support and IPsec tunnel
support deactivated in TCP/IP stack TCPIP
```

The generated email shows that the IP_STACK field IPCONFIG_IPSECURITY indicates that IPv4 IP filtering and IPSec tunnel support are not activated, or that the IP_STACK field IPCONFIG6_IPSECURITY indicates that IPv6 IP filtering and IPSec tunnel support are not activated.

Ports below 1024 are not reserved anymore (2613)

This alert is generated when TCP or UDP ports 1 - 1023 are no longer reserved for users by the PORT and PORTRANGE statements.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: UDP ports below 1024 are not reserved anymore by stack name

Alert: UDP ports below 1024 are not reserved anymore in
TCP/IP stack TCPIP
   Alert id      2613
   Changed field UDP_RESTRICTLOWPORTS(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

The text message format of the alert is:

```
Subject: Alert 2613: UDP ports below 1024 are not reserved anymore in TCP/IP stack
TCPIP

Alert 2613: UDP ports below 1024 are not reserved anymore in TCP/IP stack TCPIP
```

The generated email shows that the IP_STACK field TCP_RESTRICTLOWPORTS indicates that TCP ports 1 - 1023 are not reserved for users by the PORT and PORTRANGE statements, or that the IP_STACK field UDP_RESTRICTLOWPORTS indicates that UDP ports 1 - 1023 are not reserved for users by the PORT and PORTRANGE statements.

Interface security class changed (2614)

This alert is generated when the security class used for IP filtering with this interface changes.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: Security class changed for interface interface

Alert: Interface EELINK security class has changed in
TCP/IP stack TCPIP
```

```
   Alert id       2614
   Changed field  SECCLASS(255->238)
   Interface      EELINK
   Security class 238
   Stack          TCPIP
   System ID      DINO
```

The text message format of the alert is:

```
Subject: Alert 2614: Interface EELINK           security class has changed in TCP/IP
stack TCPIP

Alert 2614: Interface EELINK security class has changed in TCP/IP stack TCPIP
```

The generated email contains the IPv4 or IPv6 interface name, and the security class used for IP filtering with this interface.

IP filter rules changed (2615)

This alert is generated when an IP filter rule is changed, added, or deleted.

The email format of the alert is:

```
From:    C2POLICE at DINO
Subject: Alert: IP filter rules changed in TCP/IP stack TCPIP

Alert: IP filter rules changed in TCP/IP stack TCPIP
   Alert id                     2615
   Kind of change               CHG-
   Changed fields               LOG(Yes->No)-
   Source IP
   Source prefix length         0
   Source port                  0
   Destination IP
   Destination prefix length    0
   Destination port             0
   Protocol
   Type                         64
   Code                         0
   Packet filter logging enabled No
   Routing                      LOCAL
   Security class               0
   Stack                        TCPIP
   System ID                    DINO
```

The text message format of the alert is:

```
Subject: Alert 2615: IP filter rules changed in TCP/IP stack TCPIP

Alert:2615: IP filter rules changed in TCP/IP stack TCPIP
```

The generated email contains several components of the changed, added, or deleted IP filter rule: the source IP address for the outbound rule, the prefix length for the source subnet address, the source port for the outbound rule (for TCP or UDP traffic), the destination IP address for the outbound rule, the destination subnet address prefix length, the destination port for the outbound rule (matching the source port for the generated inbound rule), the type of traffic that the rule applies to, the ICMP value (for ICMP traffic), an indication whether packet filter logging is enabled for the default filter rule, the type of packet routing that the rule applies to, and the security class of the rule.

Predefined alert configuration

This section explains how some of the predefined alerts can be configured with installation-specific names.

Alert definition - specify action

When you select **Specify action** on the alert definition panel, the following panel is displayed:

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

Specify action
_  TSO-RACF command
   _  Write TSO-RACF command to C2RCMD DD

   Specify command (Press Help key in this field for help)
   _____________________________________________________________________

Enter up to 5 EXCLUDE condition sets (use EGN masks)
X _____________________________________________________________________
X _____________________________________________________________________
X _____________________________________________________________________
X _____________________________________________________________________
X _____________________________________________________________________
```

Figure 18. Setup Alert panel: Specify action

The following fields are displayed:

TSO-RACF command
Select this field to generate a TSO-RACF command for this alert.

Write TSO-RACF command to C2RCMD DD
When both this field and **TSO-RACF command** are tagged, the generated commands are not issued, but written to the C2RCMD DD.

Specify command
Enter the command you want to issue for this alert. Enclose the fixed command string parts in single quotation marks ('). For example:

```
'ALU' USER(0) 'REVOKE'
```

Enter up to 5 EXCLUDE condition sets (use EGN masks)/(use ACF2 masks). In these fields, you can enter up to 5 exclude condition sets for which no commands should be generated. For example:

```
USER=(IBMUSER,SYS*)
```

Emergency user configuration (alerts 1102 and 2102)

The alert 1102 or 2102 means logon with emergency user. When it is selected, the following panel is displayed. You can enter up to 10 emergency users.

```
 Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
              zSecure - Setup - Alert
Command ===> ____________________________________________________________________
Enter emergency users
User 1  . . . . . . . IBMUSER
User 2  . . . . . . . ________
User 3  . . . . . . . ________
User 4  . . . . . . . ________
User 5  . . . . . . . ________
User 6  . . . . . . . ________
User 7  . . . . . . . ________
User 8  . . . . . . . ________
User 9  . . . . . . . ________
User 10 . . . . . . . ________
```

Figure 19. Setup Alert panel: Configuring emergency users (alerts 1102 and 2102) panel

Note: zSecure Alert expects at least one emergency user to be entered. If no input is provided, IBMUSER is used as default.

Revocation for excessive violations (1115) configuration

Alert 1115 means too many violations in addition to just sending the alert. This alert enables you to revoke the offending user.

To be able to take the requested corrective action, the user running the started task needs sufficient authorization for the following tasks:

- RACF revoke, RACF system-wide special, or group special, and so on. See RACF documentation.
- CKGRACF DISABLE command authorization. The users to be managed must fall in the CKGRACF scope of the started task user. See *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.

The following panel displays when you select this alert:

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

Configure alert 1115: Too many violations

Number of violations    10

_  Issue RACF ALTUSER REVOKE command
_  Disable user with CKGRACF revoke schedule  ________

Exclude the following users from revocation
User 1  . . . . . . . ________
User 2  . . . . . . . ________
User 3  . . . . . . . ________
User 4  . . . . . . . ________
User 5  . . . . . . . ________
User 6  . . . . . . . ________
User 7  . . . . . . . ________
User 8  . . . . . . . ________
User 9  . . . . . . . ________
User 10 . . . . . . . ________
```

Figure 20. Setup Alert panel: Configuring revocation for excessive violations (Alert 1115)

The following fields are displayed:

Number of violations
The minimum number of violations allowed in the history interval as specified on the Alert Configuration general settings panel by the field Average.

When the number of violations specified is exceeded, the started task might issue either a RACF or CKGRACF command to revoke the violating user.

Valid values are numbers in the range 1 - 999. When not specified, a default value of 10 is used.

Issue RACF ALTUSER REVOKE command
When this field is selected, a RACF ALTUSER REVOKE command is issued when the number of violations specified is exceeded.

Disable user with CKGRACF revoke schedule
If this field is selected, a CKGRACF USER DISABLE command is issued when the number of violations specified is exceeded.

This field is only available when a zSecure Admin license has been found. When this option is selected, you are required to specify the name of the revoke schedule as well.

This option is mutually exclusive with Issue RACF ALTUSER REVOKE command

User 1-10
These fields enable you to specify user IDs which must be excluded from revocation.

It is possible to use a filter to select more than one user ID. Filters can contain %, that is, any one character, and can end in *, that is, zero or more characters.

Important groups (1701) configuration

When alert 1701, which means connection to an important group, is selected, the following panel is displayed:

```
  Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                          zSecure - Setup - Alert
Command ===> ____________________________________________________________________
Specify important group(s)
Group  . . . . . . . . SYS1      ________  ________  ________  ________
                       ________  ________  ________  ________  ________
                       ________  ________  ________  ________  ________
                       ________  ________  ________  ________  ________
```

Figure 21. Setup Alert panel: Configuring important groups (Alert 1701)

This panel enables you to enter up to 20 important groups.

It is possible to use a filter pattern to select more than one group. Filter patterns can contain a percent sign %, that is, one character, or can end with an asterisk *, that is, zero or more characters.

Number of violations and logonids to exclude (2115) configuration

The following panel is displayed when you select this alert:

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

Configure alert 1115: Too many violations

Number of violations    10



Exclude the following users from revocation
User 1  . . . . . . . . ________
User 2  . . . . . . . . ________
User 3  . . . . . . . . ________
User 4  . . . . . . . . ________
User 5  . . . . . . . . ________
User 6  . . . . . . . . ________
User 7  . . . . . . . . ________
User 8  . . . . . . . . ________
User 9  . . . . . . . . ________
User 10 . . . . . . . . ________
```

Figure 22. Setup Alert panel: Configuring the number of violations and logonids to exclude (Alert 2115)

The following fields are displayed:

Number of violations

The minimum number of violations allowed in the history interval as specified on the Alert Configuration general settings panel by the field Average.

Valid values are numbers in the range 1 - 999. When not specified, a default value of 10 is used.

User 1-10

These fields enable you to specify the users that must be excluded from revocation.

It is possible to use a filter to select more than one user. Filters can contain *, that is, any one character, and can end in -, that is, zero or more characters.

Chapter 4. Periodical overview

A periodical overview can be sent as a reminder for the recipients and possibly served as a check on correct or changed settings. For this purpose, job C2PJRECI and procedure C2PCRECI are supplied. You must copy job C2PJRECI to a data set that is used by your job scheduling software and adapt it to your needs. Specifically, you must adapt the parameter ACONF to reflect your Alert configuration and the parameter CONFIG to reflect your zSecure Alert-enabled zSecure configuration.

For general instructions for customizing zSecure-supplied jobs, see *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.

Chapter 5. Problem determination guide

This chapter provides information to identify and troubleshoot problems with zSecure Alert. A general outline describes how to distinguish zSecure Collect and zSecure Alert problems from problems in zSecure Alert, and how to resolve the problems. It provides a reference for common zSecure Alert abend codes and an explanation on how to diagnose license problems. It also gives you some troubleshooting hints for situations when zSecure Alert does not generate the alerts.

Information for problem diagnosis

If you encounter a problem in the ISPF interface, see Chapter 2, "zSecure Alert configuration," on page 3, or see *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.

Information about CKF*nnn* messages from zSecure Collect and abends in the C2PCOLL started task (program CKFCOLL) can be found in the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.

For other problems, the first step is to look at the output of the zSecure Alert started task. You must decide whether you have a problem in zSecure Alert or in zSecure Audit. The zSecure Alert started task output is partially written to the spool and partially to data sets as specified in the JCL of the started task C2POLICE.

CKR*nnnn* messages are issued by zSecure Audit. They are documented in *IBM Security zSecure: Messages Guide*.

C2P*nnnn* messages are issued by zSecure Alert. They are documented in *IBM Security zSecure: Messages Guide*. Message numbers in the range 0 - 999 point to the zSecure Alert started task.

If the zSecure Alert started task abends, you have a zSecure Alert problem. If you get summary dumps for program C2POLICE, you have a zSecure Alert problem. If you get summary dumps for program CKRCARLA, you have a zSecure Audit problem.

zSecure Audit problem diagnosis

If you have a zSecure Audit problem, the next step is to figure out whether you have a problem in the `stage 1` preparation subtask or in the reporting subtask. A zSecure Audit run produces SYSPRINT output. The output for the most recent `stage 1` run is available in the data set allocated to the SYSPRST1 DD-name in the zSecure Alert JCL. Likewise the output for the most recent reporting run can be found from SYSPRRPT. Look at the JCL of the zSecure Alert started task to obtain the names of these data sets. Consider making a copy immediately, since these data sets are reused when zSecure Alert invokes zSecure Audit again. If zSecure Alert is still running, they might have been reused already. They might still reflect the previous completed run rather than the current one. In addition, the SYSPRINT output from any zSecure Audit invocation that ends in a nonzero Return Code is added to the C2PDEBUG file.

The SYSPRINT must contain the input commands sent to zSecure Audit and indicative CKR*nnnn* messages. For diagnosing a problem report, this information is always crucial.

- If the SYSPRINT for a reporting run contains an error that relates to an unresolved LIKELIST keyword reference, this points to a problem in the `stage 1` run.
- If the CKR messages indicate a syntax error, the most likely cause is an error in a skeleton member.

See *IBM Security zSecure Admin and Audit for RACF: User Reference Manual* for further information.

zSecure Alert problem diagnosis

If zSecure Alert abends, see "General problems and abends." If you get C2P messages that point to buffer size problems, see Chapter 2, "zSecure Alert configuration," on page 3.

For other problems, contact IBM software support and provide the following information:

- A description of the circumstances under which the problem occurred
- The C2POLICE message log or the relevant part of the SYSLOG
- The JCL used, and the listing of the input commands.

General problems and abends

This section is for abends that occur in zSecure Alert. If they occur in zSecure Collect or zSecure Audit, see *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.

The following section lists the most common system abend codes encountered with zSecure Alert and provides a suggestion for the possible cause and remedy. You must also first check the appropriate message manual for your operating system, which tells you the exact meaning of the abend and reason code.

001 Problems with blocksize. Look at the message in your joblog to determine the DD-name. If you used a concatenation for this DD-name, make sure that the largest blocksize comes first. Or, specify the larger blocksize on a DCB=BLKSIZE= parameter on the first DD statement.

047 Load module is started from a non-APF authorized library. Make sure that the C2POLICE STEPLIB is APF-authorized.

322 CPU time limit exceeded. Check the job log for prior abend messages with a different abend code. If a prior abend occurred, solve this abend.

722 Too many output lines.

80A878
GETMAIN error. Try to increase the REGION parameter on the EXEC statement. If you reached the maximum of your site, contact your system programmer.

913 Access denied to one of the data sets. Review the ICH408I or ACF99913 messages in the job log to determine which data set.

D37 B37
One of the output data sets was too small, or there was no space left on the volume to extend the data set. Look at the message in your job log to determine the DD-name.

EC6 An abend EC6 means that an abend occurred while in a UNIX service. You must have the reason code to know what it is about (like CPU time limit reached - reason FD1D).

For assistance with a problem by IBM Security zSecure, you must generally provide at least the SYSMDUMP, the JCL used, and the listing of the input commands.

License problems

zSecure Alert needs one of the zSecure Alert features to be installed and not disabled in z/OS PARMLIB member IFAPRDxx on the system where it runs. The features indicate the External Security Monitor and are represented by product codes ALERTRACF and ALERTACF2.

If you have a license problem with the zSecure Alert engine (C2POLICE), look in the C2PDEBUG file. Verify whether the information shown corresponds to what you expected.

Expected alerts do not show up

If the expected alerts do not show up, check for these possible configuration issues:

- zSecure Alert is configured to send the alert to a file, that is, option SE.A.A action R
- The alert is not in the active configuration. You can find the name of the active configuration from the operator command MODIFY C2POLICE,DISPLAY . You can look for C2P messages 127, 128 and 135. Recall that you *cannot* dynamically change *which* alert configuration is used: the Refresh action does *not* activate a different member. The member contents might have been changed since the last `stage 1` run. If you changed it, you must consider the following questions:
  - Did you Verify the alert configuration?
  - Did you issue a Refresh action to bring the configuration online?
  - Did the refresh succeed?

  You can verify it in the JESMSGLG file of the zSecure Alert started task C2POLICE, or in SYSLOG.
- The alert is in the active configuration but it is not selected
- The SMF logging required for the alert is not activated. You must check whether SMFPRM*xx* specifies that the needed SMF record types are written. For the requirements for a predefined alert, see its description in Chapter 3, “Predefined alerts,” on page 39. You can find the current SMF options from the operator command DISPLAY SMF,O. For an installation defined alert, you must check whether you specify correct filter criteria. You must also check whether the C2PCUST data set member <set name>VP contains the corresponding filter criteria.
- The WTOs required for the alert are not found. You must check whether the WTO is intercepted by MPFLSTxx or by one of the MPF-related exits. It can be either IEAVMXIT or an exit routine you name on the USEREXIT parameter in PARMLIB(MPFLSTxx). For more information, see MVS Init and Tuning Reference.

In the SYSPRINT output from a reporting run, which you can see “zSecure Audit problem diagnosis” on page 103, you can see whether the alert was issued. For a WTO, CKR1239 is issued. For an SNMP trap, CKR1227 is issued. If you find this message, check on the receiving end. For an email or text message, CKR1225 is issued. If you find this message, check if the email or text message is still on the spool in the C2REMAIL file of the zSecure Alert started task C2POLICE. If so, check the SMTP settings under option SE.7 and ask your system programmer for the correct parameters. If these settings are good, you might have an SMTP problem. If the email or text message is not on the spool, it was sent by SMTP. Check the SMTP log for further diagnosis.

If the SYSPRINT reveals that the alert was not issued, check for message CKR1240 (Could not resolve to any SNMP receivers). Check any messages on WTO with a nonzero Severity.

If no alert is being sent and you cannot find a reason, check in the SMF log or SYSLOG for WTOs. See whether the event you are looking for was logged. For a "moving window" alert, verify that the threshold was exceeded in the time window.

If none of these actions help, contact IBM software support with a description of the circumstances and the problem, the SYSPRINT from the reporting subtask, and if it seems applicable the SYSPRINT from the `Stage-1` subtask as well, the JCL used, and any unexpected results encountered in the preceding diagnosis steps.

Appendix A. SNMP output

You can define your own SNMP traps. To define your SNMP traps, the LIST/SORTLIST-output must have a special form. zSecure Alert can automatically process the LIST/SORTLIST-output using NEWLIST SNMP. The special form of the output must be:

specific-trap ['**-c** *community*'] ['**-g** *global-trap*'.] ['**-e** *enterprise*'] /,
variable_1 <contents to be assigned to variable_1> /,
variable_2 <contents to be assigned to variable_2> /,
...
variable_n <contents to be assigned to variable_n>

The CARLa output conforming to this template is a set of assignment statements. It is processed by NEWLIST SNMP when generating the SNMP trap. The assignments can use following predefined variables and in the Management Information Base SCKRCARL(C2PMIB)as well as integers that represent user-defined variables. The range 400000 - 699999 is reserved for user-defined variables. You must use the four digits of the SNMP trap number followed by two digits of your own choice. Your SNMP-generating code can contain:

```
'eventIntegral'  'short description of the specific trap at hand' /,
'eventWhen' datetime(datetimezone,0) /,
```

Here is an example of the CARLa that generates the required output:

```
)CM SNMP sortlist
)SEL &C2PERCTP = SNMP
  sortlist,
   recno(nd),
   '&c2pemem.' /,
   'eventIntegral',
    'Alert: APF list changed by SETPROG APF command' '-',
    'System messages report that SETPROG APF command is issued' /,
   'eventWhen' datetime(datetimezone,0) /,
   '&c2pemem.00' MsgTxt1(0,hor) /,
   'whereSYSTEM' system(0)
)ENDSEL
```

The variables in this example are `'eventIntegral'`, `'eventWhen'`, `'&c2pemem.00'`, and `'whereSYSTEM'`. The variables `'eventIntegral'`, `'eventWhen'`, and `'whereSYSTEM'` are predefined, while `'&c2pemem.00'` is an installation defined variable.

The contents of a variable must not contain line breaks. It might have to be enforced with a repeat group format modifier `firstonly`, or `hor`.

Between `'&c2pemem.'`, which is called the *specific-trap* field, and `/,` on the line after `recno(nd)`, you can insert the options `-c` *community*, `-g` *global-trap*, and `-e` *enterprise*. The default value of *community* is `public` while *global-trap* defaults to `6`, indicating an enterprise-specific trap, and *enterprise* defaults to `1.3.6.1.4.1.9399.1.2`, indicating enterprises.consul.software.zAlert. For information about the specific-trap, community, global-trap, and enterprise parameters, you must consult SNMP literature like RFC 1215.

The following predefined variables can appear in SNMP output.

Table 7. Predefined variables that can appear in SNMP output

Variable	Description
eventIntegral	Human-readable alert title. Mostly the same as the title of the email report.
eventWhen	Date and time.
fromWhereCONSOLE	The console from which the user entered the command.
fromWhereTERMINAL	Terminal ID.
onWhatACCESS	RACF allowed access.
onWhatALLOWED	The access level allowed by the security rules, except for access granted because of WARNING mode; see onWhatGRANTED.
onWhatAUTHORITY	System-level authority that is granted or removed.
onWhatCLASS	The class in which a general profile resides.
onWhatDSNAME	Depending on the alert, the data set that is updated, on which an access attempt is made, or that is the origin of a program.
onWhatGRANTED	The access level granted. It includes access granted because of WARNING mode; see onWhatALLOWED.
onWhatGROUP-AUTHORITY	Group-level authority that is granted or removed.
onWhatINTENT	The access level requested.
onWhatNEW-PERMISSIONS	The permissions of a UNIX file or directory after a **chmod** command.
onWhatOLD-PERMISSIONS	The permissions of a UNIX file or directory before a **chmod** command.
onWhatPATH1	Requested path name (corresponding with extended-length relocate section 263).
onWhatPROFILE	The general resource or data set profile that is used for access checks.
onWhatRACFCMD-AUTH	Connect authority used in a RACF command.
onWhatRACFCMD-GROUP	Group that is used in a RACF command.
onWhatRACFCMD-NAME	Programmer name of the user that is used in a RACF command.
onWhatRACFCMD-USER	User ID of the user that is used in a RACF or ACF2 command.
onWhatRESOURCE	The resource on which RACF or ACF2 makes access checks. This resource can be a general resource. It also can be the resource that is created from a data set name using the RACF Naming Convention Table. For SMF describing class PROGRAM, it is the name of the program that is run.
onWhatUNIX-ACCESS-ALLOWED	Allowed UNIX access.
onWhatUNIX-ACCESS-INTENT	Intended UNIX access.

Table 7. Predefined variables that can appear in SNMP output (continued)

Variable	Description
onWhatUNIX-PATHNAME	The absolute or relative path of a file or directory. If the CKFREEZE file used was made with UNIX=YES (and AUTOMOUNT=YES) and contains the file or directory, it is an absolute path name.
onWhatVOLUME	The volume on which a data set resides or <SMS MANAGED> if the data set is managed by SMS.
onWhatWORKTYPE	'TSO' or 'OMVS' depending on the type of logon.
whatATTEMPTS	The number of attempts made.
whatCOMPCODE	Job or step completion code.
whatCOMPSTAT	Job or step completion status.
whatCOUNT-SMF-LOST	The number of SMF records that were lost due to full buffers.
whatDESC	Depending on the status of the event, this field contains Success, Undefined user, Violation, or Warning, depending on the status of the event.
whatEVENT	Human readable event ID.
whatEVENTDESC	The name of the event, an indication of the result (Success, Warning, Failure, or Undefined), and a short explanation of the event qualifier (Invalid password, for example).
whatEVENTQUAL	Numeric event qualifier.
whatJOBID	Job ID of the job in which the event triggered or which is created because of the event.
whatJOBNAME	Job name of the job in which the event triggered or which is created because of the event (for example, in a logon).
whatJOBTAG	System ID, job name, reader date, and reader time.
whatLOGSTR	SAF log string.
whatPARM	ACF2 GSO field, old value, and new value
whatPROGRAM	Program name.
whatPWDCHANGES	The number of password changes made in the last measurement interval
whatRACFCMD	RACF command that triggered the alert. Ignored (because of insufficient authority) keywords are labeled <IGNORED>.
whatRECORDDESC	A descriptive string that summarizes the record.
whatRULE	ACF2 rule
whatSTC	The name of a started task procedure.
whatSTEPNAME	Step name.
whatSUBTYPE	SMF record subtype.
whatTYPE	SMF numeric record type.

Table 7. Predefined variables that can appear in SNMP output (continued)

Variable	Description
whatUACC	The UACC set on a profile.
whatVIOLATIONS	Number of violations.
whatWTO-MESSAGE	The first line of output of a WTO. This line starts with the WTO message ID.
whenSMF-FAILURE	The start date and time of the period in which SMF data was lost due to full buffers. The end date and time can be found in the eventWhen field.
whenStart	Start date and start time.
whereSYSTEM	System name.
whereSYSTYPE	Operating system type.
whoNAME	Programmer name of the user in whoUSERID.
whoUSERID	User ID of the user that caused the SMF or WTO record to be written.

Appendix B. Tivoli Enterprise Console and NetView configuration

Use the information in this appendix to:

- Configure the Tivoli Enterprise Console
- Configure NetView on AIX and Windows for zSecure Alert
- Add a user-defined alert to a Management Information Base
- Create a user-defined BAROC file with Tivoli Enterprise Console classes
- Create addtrap commands for AIX and Windows systems

Configuring Tivoli Enterprise Console

About this task

This section explains how Tivoli Enterprise Console can be configured to properly display zSecure Alert traps and user-defined zSecure Alert traps. It involves carrying out a shell script to import certain trap aspects into an SNMP trap configuration file, and importing a Basic Representation of Object in C (BAROC) Tivoli Enterprise Console configuration file into a Tivoli rule base. While you can find detailed explanation in IBM-supplied Tivoli Enterprise Console documentation at publib.boulder.ibm.com/tividd/td/EnterpriseConsole3.9.html. Some of the necessary steps are highlighted for you. Tivoli Enterprise Console version 3.9 was employed on AIX 5.2.

It is assumed that you already created and activated a rule base, which is called `crm_rb` in this text. It is also assumed that a NetView Server Daemon (`nvserverd`) is running, and that the NetView trap configuration file (`/usr/OV/conf/tecint.conf`) indicates that the NetView Server Daemon must forward events to Tivoli Enterprise Console. Older Tivoli Enterprise Console setups might not include a nvserverd adapter. They might require some OID and CDS configuration files in addition to those scripts mentioned in this text. Such setups are not discussed here.

In this text, `zSecure-Alert-addtraps.sh` is used as a shorthand for the IBM-supplied trap configuration shell script. Similarly, `user-addtraps.sh` is used as a shorthand for a user-defined trap configuration script. The Windows versions of these files are called `zSecure-Alert-addtraps.bat` and `user-addtraps.bat`. Furthermore, `zSecure-Alert.baroc` is a shorthand for the IBM-supplied BAROC file, while `user-Alert.baroc` is a shorthand for a user-defined BAROC file. Creation of `user-Alert.baroc` is discussed in “User-defined BAROC files with Tivoli Enterprise Console classes” on page 117 and creation of `user-addtraps.sh` is discussed in “Addtrap commands for AIX” on page 118. You can download the most recent versions of the IBM-supplied files in the zSecure Information Center available online at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_1.13/samples.html. You can also download them from the latest *IBM Security zSecure: Documentation CD*. The files are accessible from the "Sample (Tivoli Enterprise Console and NetView Configuration, XSLT)" entry under **zSecure** in the Contents panel.

Most of the commands in the following steps require superuser privileges. It is also necessary to have the `wrb` and `addtrap` commands in your $PATH. It can be achieved by carrying out the following command, which starts with a dot and a space:

```
. /etc/Tivoli/setup_env.sh
```

The following commands pertain to IBM-supplied and user-defined traps. When you have no user-defined traps, you can ignore any steps that involve `user-addtraps.sh` and `user-Alert.baroc`.

Procedure

1. Stop the Tivoli Enterprise Console if it is running.
2. Locate a directory with the latest version of the `zSecure-Alert-addtraps.sh` file.

   You can download this file and other configuration files to a local directory from the IBM Security zSecure information center available online. Or, you can download it from the latest *IBM Security zSecure: Documentation CD*.
3. Locate a directory with the latest version of the `user-addtraps.sh` file.
4. From the folder which contains the `zSecure-Alert-addtraps.sh` file, carry out `sh zSecure-Alert-addtraps.sh`. It puts IBM-supplied zSecure Alert definitions in the NetView trap configuration file (`/usr/OV/conf/C/trapd.conf`). If you carried out this step before, it replaces older IBM-supplied zSecure Alert definitions with new ones.
5. From the folder which contains the `user-addtraps.sh` file, carry out `sh user-addtraps.sh`. It puts user-defined zSecure Alert definitions in the NetView trap configuration file (`/usr/OV/conf/C/trapd.conf`). If you carried out this step before, it replaces older user-defined definitions with new ones.
6. Remove existing user-defined Tivoli Enterprise Console classes; this step is necessary only if you have imported `user-Alert.baroc` before. You must remove these classes before the next step is carried out.

   ```
   wrb -delrbclass user-Alert.baroc crm_rb
   ```
7. Remove existing zSecure Alert Tivoli Enterprise Console classes; this step is necessary only if you imported `zSecure-Alert.baroc` before:

   ```
   wrb -delrbclass zSecure-Alert.baroc crm_rb
   ```
8. Check whether `netview.baroc` has been imported. The file must be imported before the next steps can be carried out. Using the Tivoli Enterprise Console Server, you can check whether `netview.baroc` has been imported. In the Tivoli Enterprise Console Server Desktop for Administrator window, double-click the Event Server icon. Then in the Event Server Rule Bases window, right click the `crm_rb` icon, and select **Import**. In the Import Into Rule Bases window, the imported classes are listed below the **Position to insert imported class file** text. The `netview.baroc` file must be listed there. If it is not listed, you must import the file.
9. Import the zSecure Alert BAROC file `zSecure-Alert.baroc` into Tivoli:

   ```
   wrb -imprbclass zSecure-Alert.baroc crm_rb
   ```
10. Import the user-defined BAROC file `user-Alert.baroc` into Tivoli. Importing succeeds only if the previous step has been carried out.

    ```
    wrb -imprbclass user-Alert.baroc crm_rb
    ```
11. Compile and load the `crm_rb` rule base:

    ```
    wrb -comprules crm_rb wrb -loadrb crm_rb
    ```
12. Run the following commands to stop and restart the Tivoli Enterprise Console Event Server:

```
wstopesvr
wstartesvr
```

13. Start the Tivoli Enterprise Console. To check whether the Tivoli Enterprise Console server is running again, issue the `wstatesvr` command.
14. You can send a sample trap using the `snmptrap` command, in which you must replace `10.10.3.52` with the IP number of your computer.

```
/usr/OV/bin/snmptrap -p 162 10.10.3.52 \
  .1.3.6.1.4.1.9399.1.2 "" 6 1601 "" \
  .1.3.6.1.4.1.9399.1.2.1 OctetString "Variable eventIntegral sample" \
  .1.3.6.1.4.1.9399.1.2.2 OctetString "Variable eventWhen sample" \
  .1.3.6.1.4.1.9399.1.2.31 OctetString "Variable whatWTO-MESSAGE sample" \
  .1.3.6.1.4.1.9399.1.2.6 OctetString "Variable whereSYSTEM sample"
```

15. You can check whether the trap was correctly processed. You can issue the `wtdumprl` command and view the last few lines of its output. You can also check this using the Tivoli Enterprise Console.

Configuring NetView on AIX and Windows

About this task

To configure NetView on AIX for zSecure Alert, you must load the (possibly user-extended) zSecure Alert MIB into NetView. Then you must carry out the `sh zSecure-Alert-addtraps.sh` and `sh user-addtraps.sh` commands. These commands are discussed in "Configuring Tivoli Enterprise Console" on page 111. It put some zSecure Alert definitions in the NetView trap configuration file `/usr/OV/conf/C/trapd.conf`. If you carried out these commands before, existing zSecure Alert trap definitions are replaced with new ones. Tivoli NetView version 7.1.5 was employed on AIX 5.2 to carry out the NetView configuration. You must use NetView version 7.1.5 or above.

To configure NetView on Windows for zSecure Alert, you must load the (possibly user-extended) zSecure Alert MIB into NetView. Then you must perform the following steps. If you have no user-defined traps, you can ignore the steps that involve `user-addtraps.bat`.

1. Locate a directory with the latest version of the `zSecure-Alert-addtraps.bat` file. One such directory is `samples` on the latest *IBM Security zSecure: Documentation CD*.
2. Locate a directory with the latest version of the `user-addtraps.bat` file.
3. From the folder which contains the `zSecure-Alert-addtraps.bat` file, carry out `zSecure-Alert-addtraps.bat`. It puts the zSecure Alert definitions in the right place. If you carried out this step before, it replaces older zSecure Alert definitions with new ones.
4. From the folder which contains the `user-addtraps.bat` file, carry out `user-addtraps.bat`. It puts user-defined zSecure Alert definitions in the right place. If you carried out this step before, it replaces older user-defined definitions with new ones.

To carry out these steps, NetView version 7.1.5 was employed on Microsoft Windows 2000 (Service Pack 4).

If you want NetView on Windows to forward events to Tivoli Enterprise Console, you need additional configuration. To add the zSecure Alert events, you must add entries for them in the `tecad_nv6k.cds` and `tecad_nv6k.oid` files. Then rerun the configurator again or edit the conf file to include them. See *IBM Tivoli Enterprise*

Console Adapters Guide for details on how to edit the CDS, OID, and CONF files for NetView for Windows.

Add a user-defined alert to an MIB

This section describes the extension of a Management Information Base (MIB) with a user-defined alert, also called a trap. An MIB can be imported by using NetView running on AIX or Windows. It is discussed in "Configuring NetView on AIX and Windows" on page 113.

zSecure Alert supplies the original MIB file that is going to be extended. Its name looks like *zSecure-Alert-v113.mib.*

The main components of a trap are variables. Although you can define a trap by using only variables defined in the zSecure Alert MIB, it is also possible to define and use additional variables. In "Variables," it shows how variables can be defined in an MIB. These variables can be used in traps, whose definition is discussed in "TRAPS" on page 115. "Add a user-defined alert to an MIB" indicates how several MIB files can be merged. This is necessary if you have a zSecure Alert-supplied but user-extended MIB, and then receive a new zSecure Alert MIB.

Variables

You can choose the variables that are part of a trap from the variables already defined in the zSecure Alert-supplied MIB, but you can also define new variables, add them to the MIB, and use them in a trap. The full variable definition syntax can be found in RFC 1212 (`www.faqs.org/rfcs`). The following example presents you a simplified variable definition syntax and a variable definition:

```
name OBJECT-TYPE          | user-whatATTEMPTS OBJECT-TYPE
   SYNTAX syntax          |     SYNTAX DisplayString (SIZE (0..1023))
   ACCESS access          |     ACCESS read-only
   STATUS status          |     STATUS mandatory
   DESCRIPTION            |     DESCRIPTION
          description     |           "Number of password attempts"
   ::= { Alert number }   |     ::= { Alert 400047 }
```

A variable has the following components:

name The *name* must start with a lowercase letter. It must consist of lowercase letters, uppercase letters, digits, and dashes (-) only. An example variable name is

```
user-whatATTEMPTS
```

The variable names already defined by zSecure Alert are short descriptions of alert aspects. If there are several words in a variable name, each word except the first starts with an uppercase letter `justLikeThis`. You can use these conventions as well. To avoid clashes with any future zSecure Alert-supplied variable names, you can put `user` or `user-` in front of each user-defined variable name, as in the sample variable `user-whatATTEMPTS`.

Most zSecure Alert-supplied variable names contain `who`, `what`, `onWhat`, `when`, `where`, `whereTo`, or `fromWhere`, giving an indication of the aspect domain. Also, if there is a direct correspondence between a variable and a CARLa, or CARLa Auditing and Reporting Language, field, the variable name ends with the field name written in uppercase letters.

syntax The *syntax* can have several forms but it typically is

```
DisplayString (SIZE (0..1023))
```

With this form, the variable can contain 1023 characters at most.

access The *access* can have several forms but it typically is

```
read-only
```

status The *status* can have several forms but it typically is

```
mandatory
```

description
The *description* is a quoted string like

```
"this description"
```

number
The *number* is a positive integer like

```
432100
```

The variable name and number must be unique in the MIB you want to extend. The MIB defines several variables with OBJECT-TYPE statements. Each statement starts with

name OBJECT-TYPE

and ends with

`::= { Alert` *number* `}`

The new variable must get a name which does not yet occur in front of any OBJECT-TYPE keyword in the MIB. The new variable must get a number which does not yet occur in a `::= { Alert` *number* `}` in the MIB. You must use the four digits of the trap number followed by two digits of your own choice. As indicated in "TRAPS," a user-defined trap number must be in the range 4000-6999. Therefore, the number of a user-defined variable must be in the range 400000-699999, which is the range reserved for user-defined variables. Variable numbers outside of this range are reserved for IBM.

Note: These reservations pertain to enterprise tree iso.org.dod.internet.private.enterprises.consul.software.zAlert, coded as 1.3.6.1.4.1.9399.1.2.

When you determine the components of a variable definition, you add the definition to the MIB by inserting it right after an existing variable definition. The definition ends with `::= { Alert` *n* `}`, in the MIB.

For your convenience, sort variable definitions so their variable numbers appear in increasing order. Sorting makes it easy to see which variable numbers are already reserved. The sorting order is not mandatory.

For detailed information about variables, see RFC 1212 at `www.faqs.org/rfcs`.

TRAPS

The full trap definition syntax can be found in RFC 1215 (`www.faqs.org/rfcs`). A simplified trap definition syntax and a sample trap definition look like this example:

```
name TRAP-TYPE          | smfDataLost TRAP-TYPE
   ENTERPRISE Alert     |     ENTERPRISE Alert
   VARIABLES {          |     VARIABLES {
               v1,      |                 eventIntegral,
```

```
                v2,   |                 eventWhen,
                ...   |                 whatWTO-MESSAGE,
                vm    |                 whereSYSTEM
              }       |               }
   DESCRIPTION        |    DESCRIPTION
         description  |          "SMF data is lost"
   ::= number         |    ::= 1601
```

As in the trap definition syntax, a trap definition has several components:

name The name of a trap must start with a lowercase letter. It must consist of lowercase letters, uppercase letters, digits, and dashes (-) only. An example trap name is

```
smfDataLost
```

list of variables

Variables v_1, v_2, . . ., v_m to be sent as part of the trap. Each variable listed in the VARIABLES section of a trap must have been defined as an OBJECT-TYPE. You can read about variable definitions in "Variables" on page 114.

Note: according to the MIB syntax rules, a trap with zero variables cannot have a VARIABLES { ... } section.

description

The trap names already defined by zSecure Alert are short descriptions of alerts. If there are several words in a trap name, each word except the first starts with an uppercase letter `justLikeThis`. You can use these trap naming conventions as well. The description is a quoted string like

```
"this description"
```

number

The number is a positive integer such as:

```
1601
```

The trap name and number must not yet occur in the MIB you want to extend.

To create a user-defined trap, you can simply copy a zSecure Alert-supplied trap definition. Keep the variable names and overwrite the name, description, and number with unique values. Take the following zSecure Alert-supplied trap as a starting point.

```
smfDataLost TRAP-TYPE
    ENTERPRISE Alert
    VARIABLES {
                eventIntegral,
                eventWhen,
                whatWTO-MESSAGE,
                whereSYSTEM
              }
   DESCRIPTION
          "System messages report that SMF data is lost (5)"
   ::= 1601
```

The italic parts of the trap definition can be changed to obtain the following definition:

```
mirrorGroupConnected TRAP-TYPE
    ENTERPRISE Alert
    VARIABLES {
                eventIntegral,
                eventWhen,
                user-whatMirrorGroup
```

```
          }
DESCRIPTION
       "Connect to mirror group defined"
::= 4001
```

As you can see, two zSecure Alert-supplied variables have been retained and the other variables have been replaced by a user-defined variable `user-whatMirrorGroup`. Each user-defined variable must have been defined as an OBJECT-TYPE see “Variables” on page 114.

The trap name and number must be unique across the zSecure Alert-defined and user-extended MIB. A new trap must get a name which does not yet occur in front of any TRAP-TYPE keyword in the MIB. The new trap must get a number which does not yet occur after any TRAP-TYPE ... ::= in the MIB.

The number must be in the range 4000-6999, which is the range reserved for user-defined traps. Trap numbers outside of this range are reserved for IBM. (These reservations pertain to enterprise tree iso.org.dod.internet.private.enterprises.consul.software.zAlert, coded as 1.3.6.1.4.1.9399.1.2.) The trap number must be the same as the alert number which you see in the ISPF zSecure Alert interface. The range 4000 - 4999 is intended for RACF alerts. The range 5000 - 5999 is intended for ACF2 alerts. The range 6000 - 6999 is intended for ACF2 alerts.

A new trap can be added to an MIB by inserting its definition after some trap ending with ::= *n*, where *n* is the trap number, which is already present in the MIB.

You can sort trap definitions so their numbers appear in increasing order. Sorting makes it easy to see which trap numbers are already reserved. The sorting order is not mandatory.

For detailed information about traps, refer to RFC 1215, which can be found on `www.faqs.org/rfcs`.

MIB file merging

When you add some traps and variables to an MIB and get a replacement or upgrade MIB from IBM, you must copy the customer defined traps in the range 4000-6999 and variables in the range 400000- 699999 from the old MIB to the new MIB. That ensures that the customer defined traps and variables are still recognized when you unload the old MIB file and load the new MIB file.

User-defined BAROC files with Tivoli Enterprise Console classes

This section describes the creation of a user-defined BAROC file. This file can be imported by Tivoli Enterprise Console as discussed in “Configuring Tivoli Enterprise Console” on page 111.

While it is possible to extend the zSecure Alert BAROC file (`zSecure-Alert.baroc`) with classes and variables, you must create a separate BAROC file instead. You can call that file `user-Alert.baroc` here, but you must give it another specific name. Users must keep the zSecure Alert-supplied and the user-defined BAROC files as separate entities.

You must take the definitions of the following sample `user-Alert.baroc` file as a starting point. Here, v_1, v_2, ..., v_m is a list of all user-defined variables. Each # character starts a comment which runs to the end of the line. Occurrences of

USER_DEFINED_ALERT can be replaced with some more appropriate phrase, like MY_COMPANY_ALERT. It is important to note that the user-defined `user-Alert.baroc` file depends on the `zSecure-Alert.baroc` file, which provides several zSecure Alert BAROC classes.

```
TEC CLASS: USER_DEFINED_ALERT ISA ZSECURE_ALERT
     DEFINES {
                v1: STRING; # e.g. user-whatATTEMPTS: STRING;
                v2: STRING; # e.g. user-whatMirrorGroup: STRING;
                ...
                vm: STRING; # e.g. user-whoManager: STRING;
     };
END

TEC CLASS: USER_DEFINED_ALERT_HARMLESS ISA USER_DEFINED_ALERT
     DEFINES {
                severity: default = HARMLESS;
     };
END

TEC CLASS: USER_DEFINED_ALERT_UNKNOWN ISA USER_DEFINED_ALERT
     DEFINES {
                severity: default = UNKNOWN;
     };
END

TEC CLASS: USER_DEFINED_ALERT_WARNING ISA USER_DEFINED_ALERT
     DEFINES {
                severity: default = WARNING;
     };
END

TEC CLASS: USER_DEFINED_ALERT_MINOR ISA USER_DEFINED_ALERT
     DEFINES {
                severity: default = MINOR; };
END

TEC CLASS: USER_DEFINED_ALERT_CRITICAL ISA USER_DEFINED_ALERT
     DEFINES {
                severity: default = CRITICAL;
     };
END

TEC CLASS: USER_DEFINED_ALERT_FATAL ISA USER_DEFINED_ALERT
     DEFINES {
                severity: default = FATAL;
     };
END
```

Addtrap commands for AIX

This section describes the creation of a shell script with user-defined addtrap commands. The script is intended for execution on an AIX computer that runs Tivoli Enterprise Console or NetView, as discussed in "Configuring Tivoli Enterprise Console" on page 111. "Addtrap commands for Windows" on page 120 describes the creation of a script with user-defined `addtrap` commands for Windows computers.

Each `addtrap` command corresponds with a single user-defined trap present in the zSecure Alert-supplied and user-extended MIB. It is discussed in "Add a user-defined alert to an MIB" on page 114. You must put the list of `addtrap` commands in a script separate from the zSecure Alert-supplied script. Your list of `addtrap` commands cannot then be accidentally lost when IBM provides a new

script version. The script to be created can be called `user-addtraps.sh` in this text but you must give it another specific name.

Suppose the trap numbers (to be found right after ::= operators) in the MIB are n_1, n_2, ..., and n_m. Each of these numbers should lie in the range of 4000-6999 reserved for user-defined traps. Trap numbers outside of this range, like 1601, are reserved for IBM.

Suppose the corresponding user-defined trap names, which can be found right before TRAP-TYPE keywords, in the MIB are $name_1$, $name_2$, ..., and $name_m$.

First assign a severity s_i to each user-defined trap i. A severity can be any of the following codes:

0 harmless/cleared

1 indeterminate or unknown

2 warning

3 minor

4 critical

5 major or fatal

Suppose that you assign the severities s_1, s_2, ..., and s_m to the user-defined traps. Each severity s_i corresponds with a class name cn_i:

Table 8. Severity levels assigned to class names

Severity	Description	Class name
0	harmless/cleared	USER_DEFINED_ALERT_HARMLESS
1	indeterminate/unknown	USER_DEFINED_ALERT_UNKNOWN
2	warning	USER_DEFINED_ALERT_WARNING
3	minor	USER_DEFINED_ALERT_MINOR
4	critical	USER_DEFINED_ALERT_CRITICAL
5	major/fatal	USER_DEFINED_ALERT_FATAL

The correspondence between severities and class names is specified in the BAROC file, whose creation is described in "User-defined BAROC files with Tivoli Enterprise Console classes" on page 117.

Next, devise a succinct description d_i of the trap. You can use the MIB description of the trap. Finally, make a list of names of variables of the traps in the order in which they occur in the MIB: $v_{i,1}$, $v_{i,2}$, ..., $v_{i,j}$.

Then for each name $name_i$, corresponding trap number n_i, severity s_i, class name c_i, description d_i, and variables $v_{i,1}$, $v_{i,2}$, ..., $v_{i,j}$, add the following lines to `user-addtraps.sh`:

```
addtrap -l name_i -s n_i -S s_i -g 6 -n Alert \
        -i 1.3.6.1.4.1.9399.1.2 -o A \
        -c "Status Events" -e c_i \
        -D d_i \
        -E 'v_i,1' -V '$V1' \
```

```
        -E 'v_i,2' -V '$V2' \
        ...
        -E 'v_i,j' -V '$Vj' \
        -t 0 -f - -F '$S $1'
```

Here is an example of an addtrap command, derived from the sample user-defined mirrorGroupConnected trap presented in "TRAPS" on page 115. The trap has severity 3 (-S 3), which corresponds with the USER_DEFINED_ALERT_MINOR class.

```
addtrap -l mirrorGroupConnected -s 4001 -S 3 -g 6 -n Alert \
        -i 1.3.6.1.4.1.9399.1.2 -o A \
        -c "Status Events" -e USER_DEFINED_ALERT_MINOR \
        -D "Connect to mirror group defined" \
        -E 'eventIntegral' -V '$V1' \
        -E 'eventWhen' -V '$V2' \
        -E 'user-whatMirrorGroup' -V '$V3' \
        -t 0 -f - -F '$S $1'
```

For other sample addtrap commands, you can look at the zSecure-Alert-addtraps.sh script.

Note:

1. The addtrap command and its options are case-sensitive.
2. Each backslash in the command indicates that the command is continued on the next line.
3. Each variable name in that script starts with an underscore (_), unlike the variable names in the zSecure Alert-supplied MIB. The underscores ensure that the variables are grouped in trap displays. You can also put underscores in front of variable names in user-addtraps.sh.

When you already have a user-addtraps.sh script and have added a number of new traps to your MIB file, you must extend user-addtraps.sh by appending lines corresponding with the new user-defined traps. Similarly, after removing a trap from the MIB, you must also remove the corresponding addtrap line from user-addtraps.sh. Finally, when you want to change some aspects of a trap such as severity, you can change the corresponding addtrap line.

After creating or changing user-addtraps.sh, you must run the script to notify Tivoli Enterprise Console of new or changed traps. If you have changed aspects of user-defined traps in the Tivoli Enterprise Console user interface, you can rerun the user-addtraps.sh file to revert these aspects to the user-addtraps.sh-provided values. If you do not want to change the aspects of a certain trap (for example, with name *namei*), you must remove the addtrap -l *name*$_i$ ... lines from the user-addtraps.sh file before you rerun it. Even better, do not remove the addtrap command but adjust it to reflect the current trap aspects.

Addtrap commands for Windows

This section describes the creation and use of a file with addtrap commands corresponding with user-defined traps in an MIB. The file is intended to be executed on a Windows computer running NetView. It is discussed in "Configuring NetView on AIX and Windows" on page 113. "Addtrap commands for AIX" on page 118 describes the creation of a script with user-defined addtrap commands for AIX computers.

You must create a file user-addtraps.bat other than the zSecure Alert-supplied zSecure-Alert-addtraps.bat file with addtrap commands. This way, your

user-defined addtrap commands cannot be lost when IBM provides a new version of zSecure-Alert-addtraps.bat. Although the file to be created can be called user-addtraps.bat in this text, you can give it another more specific name.

Suppose the user-defined trap numbers, which can be found right after ::= operators, in the zSecure Alert-supplied and user-extended MIB (for example, zSecure-Alert-v113.mib) are n_1, n_2, ..., and n_m. Each of these numbers must lie in the range of 4000-6999 reserved for user-defined traps. Trap numbers outside of this range are reserved for IBM.

First assign a severity to each user-defined trap. A severity can be 0 (harmless or cleared), 1 (indeterminate or unknown), 2 (warning), 3 (minor), 4 (critical), or 5 (major or fatal). Suppose severities s_1, s_2, ..., and s_m are assigned to the traps corresponding with trap numbers n_1, n_2, ..., and n_m.

Suppose the corresponding user-defined trap names (to be found right before TRAP-TYPE keywords) in the MIB are $name_1$, $name_2$, ..., and $name_m$.

Next, for each name $name_i$, corresponding trap number n_i, and corresponding severity s_i, add the following line to user-addtraps.bat:

```
addtrap -l name_i -s n_i -S s_i -g 6 -n Alert
    -i 1.3.6.1.4.1.9399.1.2 -o A
        -c "Status Events" -t 0 -f - -F "$S $1\n$# args: $*"
```

Here is an example of an addtrap command, derived from the sample user-defined mirrorGroupConnected trap presented in "TRAPS" on page 115. The trap has severity 3 (minor).

```
addtrap -l mirrorGroupConnected -s 4001 -S 3 -g 6 -n Alert
    -i 1.3.6.1.4.1.9399.1.2 -o A
        -c "Status Events" -t 0 -f - -F "$S $1\n$# args: $*"
```

For other sample addtrap commands, you can look at the zSecure-Alert-addtraps.bat script. The addtrap command and its options are case-sensitive.

After loading the MIB, you must run user-addtraps.bat to notify NetView of certain aspects (like severity) of the user-defined traps. When you already have a file called user-addtraps.bat and a number of new user-defined traps, you can extend the user-addtraps.bat file with lines corresponding with the new user-defined traps. When you remove a user-defined trap from the MIB, you must also remove the corresponding addtrap line from the user-addtraps.bat file. Finally, when you want to change some aspects of a user-defined trap, you can change the corresponding addtrap line.

After changing user-addtraps.bat, you must rerun the file to notify NetView of new or changed user-defined trap aspects.

Note: If you have changed aspects of user-defined traps in NetView, you can rerun the user-addtraps.bat file to revert these aspects to the user-addtraps.bat file-provided values. If you do not want to change the aspects of a certain trap, (for example, with name $name_i$), you must remove the addtrap -l *name*$_i$ ... line from the user-addtraps.bat file before you rerun it.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web

sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not

been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, Acrobat, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Z

Printed in USA

SC22-5467-00