IBM InfoSphere Guardium S-TAP for VSAM on z/OS
Version 9 Release 0

User's Guide

SC19-4085-01

IBM InfoSphere Guardium S-TAP for VSAM on z/OS
Version 9 Release 0

User's Guide

SC19-4085-01

Note:
Before using this information and the product it supports, read the information in "Notices" on page 53.

This edition applies to Version 9 Release 0 of IBM InfoSphere Guardium S-TAP for VSAM on z/OS (product number 5655-STY) and to all subsequent releases and modifications until otherwise indicated in new editions.

©Copyright Rocket Software Inc., 2013. All Rights Reserved.

Contents

Tables v

About this information vii
Who should read this book vii
Service updates and support information vii
Highlighting conventions. vii
How to read syntax diagrams viii
How to look up message explanations ix
Searching an information center. ix
Using a Web search ix
Using LookAt. ix
How to send your comments x

Chapter 1. Welcome to IBM InfoSphere Guardium S-TAP for VSAM on z/OS . . . 1
InfoSphere Guardium S-TAP for VSAM components 1

Chapter 2. Installation requirements for IBM InfoSphere Guardium S-TAP for VSAM on z/OS V9.0 3
Software prerequisites 3
User ID authorities required for installation 3

Chapter 3. Configuring InfoSphere Guardium S-TAP for VSAM agent 5
Security 5
APF authorizing the load library 5
Authorizing the z/OS agent started task for the control data set 6
OMVS segment definition 6
Planning your configuration 6
Job cards for the sample JCL in the sample library 6
Allocating auxiliary storage 6
Configuring the SMFPRMxx parameter library member 7
IAM and ACF2 collection considerations 7
Creating the control data set 8
Specifying subsystem options. 9
Configuring the started task JCL 12
Starting the product 13
Starting and stopping the agent started task . . 13
Sample library members 13

Chapter 4. InfoSphere Guardium S-TAP for VSAM administration 15
Communicating with the InfoSphere Guardium system 15
Communicating with the InfoSphere Guardium S-TAP for VSAM started task 15
InfoSphere Guardium S-TAP for VSAM started task commands 15
Record level and SMF data set monitoring options 16
Data collection 18
Policy pushdown 21

Chapter 5. Reference information . . . 31
VSAM data set types 31
SMF record types and contexts 32

Chapter 6. Troubleshooting 35
Messages and codes for IBM InfoSphere Guardium S-TAP for VSAM on z/OS 35
Error messages 35

Notices 53
Trademarks 55

Index 57

Tables

1. Sample library members, types, and descriptions 13
2. SMF record types, subtypes, and contexts 32
3. Error message severity codes. 35

About this information

This document contains information about IBM® InfoSphere® Guardium® S-TAP® for VSAM on z/OS®. Its purpose is to provide an overview of IBM InfoSphere Guardium S-TAP for VSAM on z/OS and its functions, as well as tasks for installing, configuring, and using IBM InfoSphere Guardium S-TAP for VSAM on z/OS. This book includes:

- Steps for installing and configuring IBM InfoSphere Guardium S-TAP for VSAM on z/OS
- System requirements and prerequisites
- Processes for the effective use of IBM InfoSphere Guardium S-TAP for VSAM on z/OS

This book is designed to help database administrators, system programmers, and application programmers perform these tasks:

- Plan for the installation of IBM InfoSphere Guardium S-TAP for VSAM on z/OS
- Install and operate IBM InfoSphere Guardium S-TAP for VSAM on z/OS
- Configure the IBM InfoSphere Guardium S-TAP for VSAM on z/OS
- Diagnose and recover from IBM InfoSphere Guardium S-TAP for VSAM on z/OS problems

Specific changes since the previous edition of this book are indicated by a vertical bar (|) to the left of a change. Editorial changes that have no technical significance are not noted.

Always check the publications web page for the most current version of this publication:

http://www-01.ibm.com/software/data/guardium/library.html

Who should read this book

This book is intended for those persons responsible for installing, customizing, and using IBM InfoSphere Guardium S-TAP for VSAM on z/OS.

Service updates and support information

To find service updates and support information, including software fix packs, PTFs, Frequently Asked Question (FAQs), technical notes, troubleshooting information, and downloads, refer to the following Web page:

http://www-947.ibm.com/support/entry/portal/Overview/Software/Information_Management/InfoSphere_Guardium

Highlighting conventions

This information uses the following highlighting conventions:

- **Boldface** type indicates commands or user interface controls such as names of fields, folders, icons, or menu choices.
- `Monospace` type indicates examples of text that you enter exactly as shown.

- *Italic* type indicates variables that you should replace with a value, to indicate the titles of other publication, and to emphasize significant terms.

How to read syntax diagrams

The following rules apply to the syntax diagrams that are used in this information:

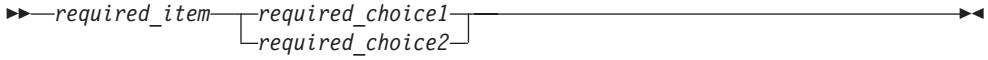
- Read the syntax diagrams from left to right, from top to bottom, following the path of the line. The following conventions are used:
  - The >>--- symbol indicates the beginning of a syntax diagram.
  - The ---> symbol indicates that the syntax diagram is continued on the next line.
  - The >--- symbol indicates that a syntax diagram is continued from the previous line.
  - The --->< symbol indicates the end of a syntax diagram.
- Required items appear on the horizontal line (the main path).

- Optional items appear below the main path.

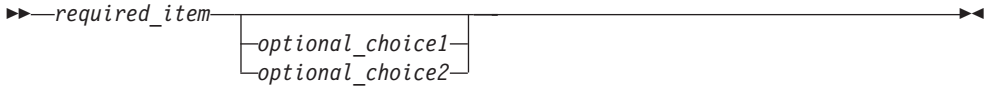
  If an optional item appears above the main path, that item has no effect on the execution of the syntax element and is used only for readability.

- If you can choose from two or more items, they appear vertically, in a stack.

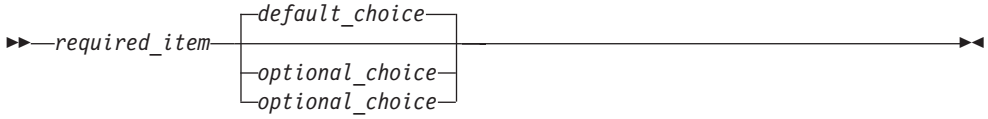
  If you *must* choose one of the items, one item of the stack appears on the main path.



  If choosing one of the items is optional, the entire stack appears below the main path.



  If one of the items is the default, it appears above the main path, and the remaining choices are shown below.



- An arrow returning to the left, above the main line, indicates an item that can be repeated.

If the repeat arrow contains a comma, you must separate repeated items with a comma.

A repeat arrow above a stack indicates that you can repeat the items in the stack.

- Keywords, and their minimum abbreviations if applicable, appear in uppercase. They must be spelled exactly as shown. Variables appear in all lowercase italic letters (for example, *column-name*). They represent user-supplied names or values.
- Separate keywords and parameters by at least one space if no intervening punctuation is shown in the diagram.
- Enter punctuation marks, parentheses, arithmetic operators, and other symbols, exactly as shown in the diagram.
- Footnotes are shown by a number in parentheses, for example (1).

How to look up message explanations

You can use any of the following methods to search for messages and codes:

Searching an information center

In the search box that is located in the top left toolbar of any Eclipse help system, such as the IBM Information Management Software for z/OS Solutions Information Center, enter the number of the message that you want to locate. For example, you can enter DFS1065A in the search field.

Use the following tips to help you improve your message searches:

- You can search for information on codes by entering the code; for example, enter -327.
- Enter the complete or partial message number. You can use wild cards (* or ?) in the message number to broaden your search; for example, DFS20??I.

The information center contains the latest message information for all of the information management products that are included in the information center.

Using a Web search

You can use any of the popular search engines that are available on the Web to search for message explanations. When you type the specific message number or code into the search engine, you will be presented with links to the message information in IBM information centers.

Using LookAt

LookAt is an online facility that you can use to look up explanations for most of the IBM messages you encounter, as well as for some system abends and codes. Using LookAt to find information is faster than a conventional search because in most cases LookAt goes directly to the message explanation.

You can use LookAt from the following locations to find IBM message explanations for z/OS elements and features, z/VM®, VSE/ESA, and Clusters for AIX® and Linux:

- The Internet. You can access IBM message explanations directly from the LookAt Web site at http://www.ibm.com/eserver/zseries/zos/bkserv/lookat/.
- Your z/OS TSO/E host system. You can install code on your z/OS or z/OSe systems to access IBM message explanations, using LookAt from a TSO/E command line (for example, TSO/E prompt, ISPF, or z/OS UNIX System Services running OMVS).
- Your Microsoft Windows workstation. You can install code to access IBM message explanations on the z/OS Collection (SK3T-4269) using LookAt from a Microsoft Windows command prompt (also known as the DOS command line).
- Your wireless handheld device. You can use the LookAt Mobile Edition with a handheld device that has wireless access and an Internet browser (for example, Internet Explorer for Pocket PCs, Blazer, or Eudora for Palm OS, or Opera for Linux handheld devices). Link to the LookAt Mobile Edition from the LookAt Web site.

You can obtain code to install LookAt on your host system or Microsoft Windows workstation from a disk on your z/OS Collection (SK3T-4269) or from the LookAt Web site (click **Download**, and select the platform, release, collection, and location that suit your needs). More information is available in the LOOKAT.ME files available during the download process.

How to send your comments

Your feedback is important in helping to provide the most accurate and high-quality information. If you have any comments about this book or any other IBM InfoSphere Guardium S-TAP for VSAM on z/OS documentation:

- Use the online reader comment form, which is located at:

  www.ibm.com/software/data/rcf/
- Send your comments by e-mail to comments@us.ibm.com. Be sure to include the name of the book, the part number of the book, the version of IBM InfoSphere Guardium S-TAP for VSAM on z/OS, and, if applicable, the specific location of the text you are commenting on (for example, a page number or table number).

Chapter 1. Welcome to IBM InfoSphere Guardium S-TAP for VSAM on z/OS

IBM InfoSphere Guardium S-TAP for VSAM on z/OS(also referred to as InfoSphere Guardium S-TAP) is a tool that collects and correlates data access information from System Management Facility (SMF) records to produce a comprehensive view of business activity for auditors.

InfoSphere Guardium S-TAP provides the following features and functions:

- Data collection— InfoSphere Guardium S-TAP can collect and correlate many different types of information:
  - Access to VSAM data sets and security violations as recorded by SMF.
  - Data set operations performed against VSAM data sets such as deletes or renames as recorded by SMF.

InfoSphere Guardium S-TAP for VSAM components

The product consists of the InfoSphere Guardium system, and the InfoSphere Guardium S-TAP for VSAM agent. The Guardium system is a server-based component that provides the product's user interface. The agent collects VSAM-related information that is obtained from the SMF record exit interface and VSAM I/O activities.

Guardium system and S-TAP agent communication

Communication between the Guardium system and the agent uses a TCP/IP connection. The policies you create, using the Guardium system user interface, tell the agent what data to collect. The policy specifies filter information, such as which jobs and data sets to be monitored for data accesses.

Guardium system

The Guardium system can gather, and report on, information from multiple agents running on multiple z/OS systems. The Guardium system:

- Provides the user interface, which accepts requests and displays the resulting information.
- Enables you to create collection policies, which specify the types of data to be collected by the agent.
- Stores the collected data.

Agent

The agent collects data from a single z/OS system. Monitoring can be performed at the both the data set and record level:

- For data set level monitoring, data is collected directly from SMF records as presented to various SMF exits with which the agent interfaces.
- For record level monitoring, data is collected when VSAM records are read or written.

Related reference:

"SMF record types and contexts" on page 32
SMF records are correlated to InfoSphere Guardium S-TAP for VSAM context as shown in the SMF record types context table.

Chapter 2. Installation requirements for IBM InfoSphere Guardium S-TAP for VSAM on z/OS V9.0

Review the software and authorization prerequisites before installing IBM InfoSphere Guardium S-TAP for VSAM on z/OS V9.0.

Software prerequisites

InfoSphere Guardium S-TAP for VSAM requires z/OS Version 1 Release 11 or higher.

User ID authorities required for installation

If you are the installing the product, you must have the necessary z/OS user ID authorities to install IBM InfoSphere Guardium S-TAP for VSAM on z/OS V9.0.

Your z/OS user ID must have the authority to:

- Define the appropriate SMF record collection parameters in the SMFPRMxx PARMLIB member and APF authorize the load library for the product.
- Update the appropriate procedure library to include the agent started task.

If necessary, contact your system administrator to obtain the required authority.

Chapter 3. Configuring InfoSphere Guardium S-TAP for VSAM agent

You must configure InfoSphere Guardium S-TAP for VSAM agent.

Configuration overview

Use this section of the user's guide to:

- Review the required resource authorizations, planning steps, and required information.
- Configure the z/OS system PARMLIB member SMFPRMxx to collect required SMF record types.
- Allocate and initially populate the control data set.
- Review the subsystem changes you can make to the options member in the control data set.
- Determine the location of the started task JCL (control job language), and follow configuration steps and tips.

Once you have completed the required configuration steps, learn how to stop and start the InfoSphere Guardium S-TAP for VSAM agent, which runs as a started task. A list of sample library members is also provided for your reference.

Security

InfoSphere Guardium S-TAP for VSAM requires access to various z/OS data sets and system components. You must set up access controls in your security product in order to create, authorize, or update the various data sets that are necessary for product configuration.

To provide InfoSphere Guardium S-TAP for VSAM with access to the necessary z/OS data sets and system components, you must APF authorize the load library, authorize the z/OS started task for the control data set, and define an OMVS segment to your security product.

In this user's guide, security products refer to the various software tools currently available, including IBM Resource Access Control Facility (RACF), Innovation Access Method (IAM) from Innovation Data Processing, and Access Control Facility (ACF2) from Computer Associates International.

APF authorizing the load library

InfoSphere Guardium S-TAP for VSAM requires certain data sets be accessible and APF authorized on the system in which the started task agent will run, and SMF data will be collected by the agent.

The product data set SAUVLOAD, which contains the product's load modules required for operation, must be APF authorized on the system on which InfoSphere Guardium S-TAP for VSAM will be run.

Refer to the z/OS MVS Programming Authorized Assembler Services Guide for guidelines and instructions on using APF.

Authorizing the z/OS agent started task for the control data set

The z/OS agent started task must be authorized to read and update the control data set. The control data set is a partitioned data set that contains various members that define options and operating parameters for the product. InfoSphere Guardium S-TAP for VSAM uses a control data set that is defined in the agent started task.

Refer to your security product's documentation for more information on authorizing the agent started task.

OMVS segment definition

You must define an OMVS segment to your security product in order to make use of TCP/IP connectivity and UNIX System Services. An OMVS segment specifies the user ID to be used, the home directory, and the shell program name.

If you are using IBM RACF, refer to z/OS V1R12.0 UNIX System Services Planning for guidelines and instructions on OMVS segment definitions. If you are using a security product other than RACF, refer to your product's instructions on how to define an OMVS segment.

Planning your configuration

Use this planning list to determine necessary information before continuing. Then, provide a valid job card, and allocate auxiliary storage if necessary, as described in the following sections.

Prior to configuration, you must determine:

- The user who will configure the product
- The user ID that will be used to run the agent
- Where the InfoSphere Guardium system and the agent will run

Job cards for the sample JCL in the sample library

Some JCL members included with the product SAMPLIB have a sample card for the job card.

Provide a valid job card that conforms to the JCL standards of your site before submitting any of the JCL members.

Allocating auxiliary storage

z/OS auxiliary storage consists of DASD space allocated to the local page data sets. It is used as a temporary backing storage for programs and data located in virtual and physical memory. InfoSphere Guardium S-TAP for VSAM can allocate auxiliary storage space if the SPILL_BUFFER_SIZE parameter is set in accordance with the following requirements.

The SPILL_BUFFER_SIZE parameter option instructs the address space to allocate a data space equal in size to the value you set for SPILL_BUFFER_SIZE.

Verify that the current local page space can accommodate a new data space.

Example

Specifying "SPILL_BUFFER_SIZE=64" instructs the address space to allocate 64 MB of data space.

Refer to the z/OS MVS™ Initialization and Tuning guide for more information on sizing local page data sets.

Configuring the SMFPRMxx parameter library member

To ensure a complete audit, you must configure the active SMFPRMxx member of the z/OS system PARMLIB to collect the required SMF record types needed by InfoSphere Guardium S-TAP for VSAM.

The record types can be collected at the subsystem or system level. Maximum auditing of VSAM data set activity can be achieved by ensuring that all defined subsystems record all of the SMF record types required by the product.

The defaults used at the system level for those subsystems not explicitly defined should also specify collection of the required SMF record types. The required SMF record types are 30, 42, 60, 61, 62, 64, 65, 66, 80 and 89.

The IEFU83, IEFU84, and IEFU85 SMF exits should be specified at either the subsystem or system level in a manner consistent with the SMF record type specifications.

For more information about setting up and managing SMF, refer to the z/OS MVS System Management Facility (SMF) manual.

Related reference:

"SMF record types and contexts" on page 32
SMF records are correlated to InfoSphere Guardium S-TAP for VSAM context as shown in the SMF record types context table.

IAM and ACF2 collection considerations

InfoSphere Guardium S-TAP for VSAM can capture IAM data set activity and ACF2 access failures. Learn how to enable InfoSphere Guardium S-TAP for VSAM to collect this information, and be aware of the following collection considerations. These products implement the collection of SMF data in a nonstandard way and require special consideration.

Innovations Data Processing IAM considerations

Innovation Access Method (IAM) from Innovation Data Processing provides capabilities beyond standard VSAM. IAM replaces VSAM access with a proprietary non-VSAM access that simulates VSAM. Since the underlying data sets are non-VSAM, accesses to the IAM-simulated VSAM data sets do not generate VSAM SMF records, such as the SMF type 62 (VSAM OPEN) and SMF type 64 (VSAM CLOSE).

IAM provides a unique, user-specified record ID, which is written during CLOSE processing. For Guardium S-TAP for VSAM to report this access:

1. Determine the user SMF record ID selected for IAM
2. Specify that value in the Guardium S-TAP for VSAM control data set IAM_SMF_RECORD_ID option.

For IAM data sets, InfoSphere Guardium S-TAP for VSAM does not report the following:

- Context records for OPEN and UPDATE for IAM data sets (due to the lack of the SMF type 62 records).
- IAM simulation of alternate index and path processing (due to the lack of an IAM SMF CLOSE record).

The CLOSE record counters will report IAM data sets differently than native VSAM processing. Although the IAM CLOSE SMF record offers an extensive array of counters, those corresponding to the VSAM SMF Type 64 record are included in the accumulated counts within the CLOSE context record.

Computer Associates International ACF2 considerations

Access Control Facility (ACF2) from Computer Associates International records access failures to a unique, user-specified record ID. For Guardium S-TAP for VSAM to report these failures:

1. Determine the user SMF record ID selected for ACF2.
2. Specify that value in the Guardium S-TAP for VSAM control data set ACF_SMF_RECORD_ID option.

Unlike some security products, ACF2 does not offer a unique authorization failure code to identify a CONTROL access failure. Instead, it reports these as UPDATE access failures. In ACF2 facilities, no CONTROL context records will be reported.

Creating the control data set

Complete these steps to create the control data set and generate the initial PDS members. These members contain required information, and must be added to the newly created data set for the agent to work properly.

Before you begin

Refer to the high-level qualifier that you specified when configuring the started task JCL. The same high-level qualifier must be used in step 1 of the control data set creation procedure.

About this task

The options and definitions that determine how InfoSphere Guardium S-TAP for VSAM performs processing in your environment are contained in the control data set.

Procedure

1. The JCL to create the control data set is located in the AUVJCNTL member of the SAUVSAMP library. Configure the AUVJCNTL member by replacing AUV.V9R0 with the high-level qualifier of the installed InfoSphere Guardium S-TAP for VSAM load library.
2. Submit the JCL to create the control data set. The JCL creates the control data set and populates the data set with these initial members: subsystem options (OPTIONS) and policy rule definition members (RULEDEFS and RULEDEFB).

   Important:

   - Do not modify the contents of the RULEDEFS or RULEDEFB member.

- Do not modify the value of the default INITIAL_RULEDEF option in the RULEDEFS or RULEDEFB members.

3. Specify the TCP/IP_ADDRESS, AGENT_NAME, and PORT parameters in the OPTIONS member to enable the product to function properly.
4. Optional: Consider whether allocating the control data set as an extended partitioned data set (PDSE) it appropriate for your environment. A PDSE dynamically manages internal space, drastically reducing the need to perform the space compressions that are required for a nonextended partitioned data set (PDS). The AUVJCNTL member includes statements that can be used to change the allocation to a PDSE.

Specifying subsystem options

To configure InfoSphere Guardium S-TAP for VSAM, you must specify a four-character InfoSphere Guardium S-TAP for VSAM subsystem ID (SSID) to associate with this particular instance of InfoSphere Guardium S-TAP for VSAM. The SSID identifies the InfoSphere Guardium S-TAP for VSAM subsystem in messages that are generated by the product.

The InfoSphere Guardium S-TAP for VSAM subsystem options are in the OPTIONS member of the InfoSphere Guardium S-TAP for VSAM control data set that is generated by the AUVJCNTL member JCL. These options are the global definitions and general operation options that determine where and how InfoSphere Guardium S-TAP for VSAM performs its functions.

To specify InfoSphere Guardium S-TAP for VSAM subsystem options, modify the contents of the OPTIONS member as described.

ACF_SMF_RECORD_ID

If you are using Access Control Facility (ACF2) from Computer Associates International, you must provide product-specific information for your SMF data to be processed in a compatibly. ACF2 records access failures to a unique record ID. For Guardium S-TAP for VSAM to report these failures, determine the user SMF record ID selected for ACF2, and specify that ID in the Guardium S-TAP for VSAM CONTROL data set ACF_SMF_RECORD_ID option.

ACF2 writes SMF access failure data to a user-defined SMF record ID. Specify a numerical value that identifies the SMF record identification number used by ACF2.

For ACF2 installations, contact your ACF2 administrator to determine the appropriate numeric value to include with this parameter.

Valid values are 128-255. There is no product default value, however, the SAMPLIB member AUVSOPTS includes a default specification of 230.

AGENT_NAME

Specify a character string from one through 26 characters that defines the name of this InfoSphere Guardium S-TAP for VSAM agent.

There is no default.

IAM_SMF_RECORD_ID

If you are using Innovation Access Method (IAM) from Innovation Data Processing, you must provide product-specific information for your SMF data to be processed in a compatibly. IAM provides a unique user-specified record ID, which it writes during CLOSE processing. For Guardium S-TAP

for VSAM to report this access, determine the user SMF record ID for IAM, and specify that value in the Guardium S-TAP for VSAM CONTROL data set IAM_SMF_RECORD_ID option.

IAM writes SMF statistical data to a user defined SMF record ID. Specify a numeric value that identifies the SMF record identification number used by IAM.

For IAM installations, consult your IAM administrator to determine the appropriate numeric value to include with this parameter.

Valid values are 128-255. There is no product default value; however, the SAMPLIB member AUVSOPTS includes a default specification of 201.

INTERNAL_BUFFER_SIZE

Specify the size of the internal buffer used.

To improve performance, data is stored in an internal buffer that is sent when the buffer is full or during a ping request. If the buffer reaches the INTERNAL_BUFFER_SIZE, data is sent without waiting for the next ping request.

Specifying an INTERNAL_BUFFER_SIZE value that is too large for your environment can cause connection problems due to timing out while trying to send a large amount of data. Specifying too small a value might can cause unnecessary I/O requests.

Tip: Performance varies based on system load, network load, and the load on the Guardium system, so the correct value for your environment cannot be predetermined. Begin with the default value, and make minor, incremental adjustments to improve performance, if necessary.

Valid values are 0-2047 megabytes. The default is 8.

INITIAL_RULEDEF

You must not change this subsystem option unless IBM Software Support instructs you to do so. If instructed to modify this subsystem option, specify the name of the rule definitions member to use at startup. The default rule definitions member name is RULEDEFS.

PING_RATE

Specify a numeric value that defines the number of seconds between pings to the InfoSphere Guardium system. The ping signals the InfoSphere Guardium system that the S-TAP is active and available for communications.

Valid values are 1-65535. The default value, in seconds, is 5.

PORT

Specify a numeric value that defines the TCP/IP port number for communication with the InfoSphere Guardium system by InfoSphere Guardium S-TAP for VSAM. Use port 16022 for the V9 system protocol.

Valid values are 0-99999. The default value is 16022.

RETRY_COUNT

Specify a numeric value that defines the number of times to retry communicating with the InfoSphere Guardium system when an error is encountered during initialization. If the communication is still not successful after the number of retries as specified by this value have been

completed, the communication is abandoned and no data is sent. The process also terminates if the number of retries specified is reached with no successful connection.

Valid values are 0-65535. The default value is 20.

RETRY_INTERVAL
Specify a numeric value that defines the number of seconds between retries when an error is encountered while initially attempting to connect to the InfoSphere Guardium system.

Valid values are 0-65535. The default value, in seconds, is 10.

SECONDARY_IPADDR_PORT
Specify the secondary TCP/IP addresses to use for failover and recovery processing. The product supports up to five alternate TCP/IP address. To specify one or more secondary entries, include this parameter up to five times, each time providing a unique TCP/IP address.

The option syntax is as follows:
`SECONDARY_IPADDR_PORT=(`*`addr`*`)`

Valid values are any valid TCP/IP address. There are no default values. If initialization does not detect this parameter, it does not activate the failover process.

SOCKET_CONNECT_TIMEOUT
Specify the length of time for socket connection attempts before failure or timeout.

Setting this value too low results in connection failures when the Guardium system is slow to respond. Setting this value too high causes problems in failover scenarios.

Tip: Performance varies based on system load, network load, and the load on the Guardium system, so the correct value for your environment cannot be predetermined. Begin with the default value, and make minor, incremental adjustments to improve performance, if necessary.

Valid values are 1-65535. The default value, in seconds, is 3.

SOCKET_TIMEOUT
Specify a numeric value that defines the number of seconds that must transpire before a timeout is recognized.

Valid values are 0-65535. The default value, in seconds, is 0.

SPILL_BUFFER_SIZE
Specify the size of the spill file to be used when no connection can be made.

If the product includes a spill file and no secondary TCP/IP and port pairs is specified, or none of the secondary TCP/IP address and port pairs responds, it writes to the spill file. The spill file is meant for short term outages only, because once a connection is restored to any Guardium system, it clears the spill file content before continuing to send data.

Valid values are 0-1024 megabytes. If a valid value is not specified, a spill file is not created.

SSID Choose any four-character alphanumeric subsystem ID to identify this particular instance of InfoSphere Guardium S-TAP for VSAM. For example, “AUV1”, “AUV2” and so on.

Choose a unique SSID for each agent.

The default subsystem ID is “VTAP”.

TCP/IP_ADDRESS

Specify the TCP/IP address for the InfoSphere Guardium system with which InfoSphere Guardium S-TAP for VSAM is to communicate.

The address can be specified as a host name (*infosphere.guardiumvsam.net*) or as four numeric digits separated by periods (for example, 188.128.6.42).

Maximum length is 57 characters. There is no default.

Configuring the started task JCL

The started task JCL is a group of statements that provide information to the system. You must configure the started task JCL with values that are specific to your environment. Follow these steps to configure the started task JCL.

About this task

The InfoSphere Guardium S-TAP for VSAM started task JCL is located in the AUVJSTC member of the InfoSphere Guardium S-TAP for VSAM sample library (SAUVSAMP).

Note: Do not start the started task until you finish configuring InfoSphere Guardium S-TAP for VSAM. Attempting to initiate the started task prior to completing configuration could cause the started task to fail.

Procedure

1. Copy the InfoSphere Guardium S-TAP for VSAM started task JCL from sample data set member AUVJSTC to your system PROCLIB.

   Tip: Name the InfoSphere Guardium S-TAP for VSAM started task member AUVSTAPV. This name is easily identifiable with the InfoSphere Guardium S-TAP for VSAM product.
2. Verify that the statement://AUVSTAPV PROC OPTSMBR=OPTIONS points to the default member name OPTIONS. The default member name OPTIONS was created during creation of the control data set.
3. Configure the started task JCL that you copied to your system PROCLIB by replacing AUV.V9R0 with the high-level qualifier of the installed InfoSphere Guardium S-TAP for VSAM load library.

   Note: For operation of the product, policy activation, and correct processing of data, the following conditions must be met:
   - A DD statement with the DDNAME OPTIONS must be in the InfoSphere Guardium S-TAP for VSAM started task. This DD statement points to the subsystem OPTIONS member of the InfoSphere Guardium S-TAP for VSAM control data set, which contains the global settings for the product. When the started task is initiated, it references the data in the subsystem options member to establish global settings, including the subsystem identifier for this specific instance of InfoSphere Guardium S-TAP for VSAM.
   - A DD statement with a DDNAME of CONTROL must be in the InfoSphere Guardium S-TAP for VSAM started task. For example: //CONTROL DD DSN=AUV.V9R0.CONTROL,DISP=SHR. This DD

statement points to the InfoSphere Guardium S-TAP for VSAM control data set that contains the collection policy in the RULEDEFS member.

- The two DD statements with the DDNAMES RULEDEFS and RULEDEFB must be present and must point to the same control data set name that was specified in the OPTIONS and CONTROL DD statements. The member names RULEDEFS and RULEDEFB must not be changed. If DDNAMES RULEDEFS and RULEDEFB are not present, are changed, or do not point to the correct data set name, then the agent does not initiate properly and is unable to collect data.
- The high-level qualifier you specify for the control data set JCL when allocating the control data set must match the high-level qualifier you specify in the started task JCL.
- The started task must have the authority to read and update the control data set and load library.

4. After you configure the started task JCL, add it to the z/OS proclib data set for started task initiation.

Starting the product

Start InfoSphere Guardium S-TAP for VSAM prior to starting products that perform similar functions.

Product initialization errors might occur if other products, which are known to intercept processing at the point of open, close, or record management functions for VSAM data sets, are started before InfoSphere Guardium S-TAP for VSAM. Message AUV1196E will warn you of a product initialization order conflict. If you receive this error at start up, shut down InfoSphere Guardium S-TAP for VSAM and any similar products, and start InfoSphere Guardium S-TAP for VSAM first.

Starting and stopping the agent started task

Follow these steps to start and stop the InfoSphere Guardium S-TAP for VSAM agent started task.

1. Start the agent started task by issuing the START command from the operator console. For example: **START AUVSTAPV**
2. Stop the agent started task by issuing the STOP command from the operator console. For example: **STOP AUVSTAPV**

You can configure the agent started task to start automatically during the z/OS initial program load (IPL). To set automatic startup, add the appropriate command to the COMMNDxx member in SYS1.PARMLIB, or contact your system administrator.

Sample library members

The following sample library members are included for your use in installing and configuring InfoSphere Guardium S-TAP for VSAM. The sample library members table lists them by type and description.

Table 1. Sample library members, types, and descriptions

Member	Type	Description
AUVJCNTL	JCL	Sample JCL to allocate and initially populate the control data set.
AUVJSTC	JCL	Sample PROC to start the InfoSphere Guardium S-TAP for VSAM agent address space.

Table 1. Sample library members, types, and descriptions (continued)

Member	Type	Description
AUVSOPTS	Data	Initial data used to populate the control data set OPTIONS member.
AUVSRDEF	Data	Initial data used to populate the control data set RULEDEFS and RULEDEFB members.

Chapter 4. InfoSphere Guardium S-TAP for VSAM administration

You must configure the InfoSphere Guardium system to communicate with the InfoSphere Guardium S-TAP for VSAM agent.

Communicating with the InfoSphere Guardium system

The InfoSphere Guardium system and the S-TAP for VSAM agent need to communicate policy rules and collected data using a TCP/IP connections. For the InfoSphere Guardium S-TAP for VSAM to communicate with the Guardium system, the following conditions must be met:

- The InfoSphere Guardium S-TAP for VSAM TCP/IP connection must be configured.
- At least one agent per z/OS image must be specified. When configuring an agent instance:
  - Specify the host name or IP address and the port number on which the Guardium system is running. These values are specified by the TCP/IP_ADDRESS and PORT configuration elements in the agent configuration file. The complete name of this CONTROL member is OPTIONS.

  When the agent is started, it uses the specified configuration information to connect to the InfoSphere Guardium system.

Communicating with the InfoSphere Guardium S-TAP for VSAM started task

InfoSphere Guardium S-TAP for VSAM operator commands enable authorized users to perform selected operations. Several types of operator commands can be used to display the status of InfoSphere Guardium S-TAP for VSAM, to enable and disable certain functions, and to dynamically alter processing without stopping or quiescing the product.

InfoSphere Guardium S-TAP for VSAM started task commands

If you are an authorized user, you can enter commands to display the status of InfoSphere Guardium S-TAP for VSAM, enable and disable certain functions, and dynamically alter processing without shutting down or quiescing the system.

Commands

You enter operator commands from an MVS operator console or by using a facility that issues MVS commands, such as SDSF. The command format is **MODIFY***stcname*, where *stcname* is the name of the started task, followed by the display command. For example, to monitor Record level monitoring, you can enter**MODIFY***stcname*,**DISPLAY RLM**. You can also use the shorthand for **MODIFY**, which is **F**, for example: **F***stcname*,**DISPLAY RLM**. The following table summarizes the commands for displaying monitoring status and for enabling or disabling monitoring.

Command	Description
DISPLAY RLM	Indicates whether Record level monitoring is enabled or disabled.
DISPLAY SMFM	Indicates whether SMF Monitoring is enabled or disabled.
ENABLE RLM	Enables Record level monitoring
DISABLE RLM	Disables Record level monitoring
ENABLE SMFM	Enables SMF Monitoring
DISABLE SMFM	Disables SMF Monitoring

Record level and SMF data set monitoring options

You can reduce z/OS CPU and storage usage by setting options for Record level and SMF data set monitoring.

Record level monitoring performance

During Record level monitoring, data is collected when VSAM records are read or written. Record level monitoring can affect performance, TCP/IP traffic, and system load. Record level monitoring intercepts VSAM accesses at the record level, so excessive monitoring of logical record requests can result in large volumes of data being transferred to the InfoSphere Guardium system from the TCP/IP telecommunications link, along with a corresponding increase in CPU and storage use within z/OS. Even in a moderately sized installation that uses VSAM files, hundreds of millions, if not billions, of logical record requests can be made to VSAM daily. Attempting to monitor and report on all VSAM requests can result in huge volumes of data that can potentially increase system load on z/OS and data traffic on communication links.

To provide flexibility in controlling the impact of Record level monitoring, policy options can be used to limit the scope of monitoring. Carefully consider these options with the goal of limiting Record level monitoring to the logical record requests in specific data sets that must be monitored in your environment.

Record level monitoring filter options

You can use the Record Level Monitoring to filter based on:

- Program name
- SYSPLEX name
- SMF system identification

You can also limit the monitoring of records to particular keys or key ranges:

VSAM KSDS and RRDS data sets

For KSDS data sets, the key used is defined when the data set is created through an IDCAMS DEFINE.

For RRDS data sets the key is a relative record number within the data set.

For individual keys a list of keys is permitted with which a comparison operator can be used. In situations where the key contains unprintable characters, you can define the keys or key ranges using hexadecimal notation.

Limit the monitoring of record level requests by the type of logical requests, including:

- Record read events
- Update write events
- Insertions
- Deletions

Remember: Each monitored record that matches the various policy filters results in the processing, creation, and transmission of a record monitoring data element to the InfoSphere Guardium system. Use the InfoSphere Guardium system interface to establish as restrictive a set of policy filters as possible. InfoSphere Guardium S-TAP for VSAM dynamically tunes and minimizes processing based on the filtering criteria chosen. Effectively chosen filters allows for maximum efficiency of Record level monitoring processing.

Activating Record level monitoring

You must define a policy that includes rules that specify one or more of the record level request filters (reads, update writes, insertions, or deletions) in order to activate Record level monitoring.

- If a policy does not contain any of these filters, no additional overhead occurs at the logical record request level.
- If a particular policy rule contains one or more of these filters, only the specific data set defined in the rule (or data sets associated with other policy filters defined in the rule) incurs any additional monitoring overhead.

SMF data set monitoring performance and filtering

Use filtering criteria to limit the amount of VSAM data set monitoring to only particular events. Using policy filters, SMF data set monitoring performance is enhanced by reducing CPU usage, storage usage, and TCP/IP traffic to the InfoSphere Guardium system.

Filter down to each specific VSAM data set events with the following filters:

- Data Set Open
- Data Set Update
- Data Set Close
- Data Set Delete
- Data Set Rename
- Data Set Create
- Data Set Alter
- Data Set RACF® Alter
- Data Set RACF Update
- Data Set RACF Read

You can achieve optimal Record level monitoring and SMF data set monitoring performance when you create and use a policy that defines only those events that are required by your organization.

Data collection

InfoSphere Guardium S-TAP for VSAM collects data from multiple sources. This section describes the data collection process, stages of filtering performance, and their performance impacts.

SMF event and Record level monitoring

Event information is gathered at run time through SMF event and Record level monitoring. For both SMF event monitoring and Record level monitoring, you can specify filtering options to minimize overhead and control the performance of the data collection and reporting phases of processing. InfoSphere Guardium S-TAP for VSAM uses the filtering criteria you define to dynamically tune its processing path for optimal performance.

With few exceptions, you can use the same filtering criteria for both SMF event and Record level monitoring.

- Specify the minimal filtering criteria necessary for your policy. Filtering only on the data you require minimizes:
  - Data collection overhead
  - Event processing
  - Event reporting
  - CPU time
  - Memory usage

  Record level monitoring creates the potential for the collection and reporting of large amounts of data. When constructing a policy and specifying filtering criteria, carefully consider the potential amount of data to be collected and processed.
- You can specify lists of elements for some filters, and use generic characters (wildcards) to create more flexibility in your filtering criteria. Generic characters act as placeholders in the specification of a character-based operand, representative of one or more valid characters for the entity on which an operation is performed.
- The use of generic characters can reduce the total number of policy rules required, but be aware that an overly inclusive set of selected entities can ultimately reduce efficiency. Excessive use of generic characters can increase the scope of selectivity during the qualification of records for processing, and dramatically reduce efficiency and increase overhead.
- SMF event monitoring can be controlled at a higher level through the specifications in the SMFPRMxx z/OS system PARMLIB member.

Filtering stages

Both SMF event and Record level monitoring are performed in stages. If a collected event does not pass the lowest filtering stage (0), further processing of that event is not performed. Otherwise, the event is reevaluated during the next stage of filter processing, and InfoSphere Guardium S-TAP for VSAM determines whether the event should be auditing and reporting.

Stage 0 filtering
: Stage 0 filtering should only be used by advanced users. An understanding of each SMF record type is required.

Stage 0 filtering can be performed for SMF event monitoring only. Only SMF events being recorded by SMF can be monitored for processing.

SMF record types to be monitored must be defined in the SMFPRMxx z/OS System Initialization PARMLIB member. If one or more SMF record types to be monitored is not specified, data collection cannot be performed. See the "SMF record types collected by InfoSphere Guardium S-TAP for VSAM" section of this user's guide for details on the record types and the associated data collected with each record type.

Stage 1 filtering

Stage 1 filtering can be performed with both SMF event and Record level monitoring.

Filter out as much data as possible to achieve the best possible performance.

The filtering criteria specified in the policy associated with this level of filtering include:

- Data Set Name
- Job Name
- Program Name
- Security System User ID
- Security System Group ID
- Sysplex Name
- SMF System ID
- Subsystem ID
- Job Type
- VSAM Record Organization*

*VSAM Record Organization is only available as a filtering criterion for Record level monitoring. Only key-sequenced data set (KSDS) and relative record data set (RRDS) organizations are supported.

Some of the possible filtering criteria for Stage 1 filtering include a wider scope of data than others. For example, a user ID can require a much larger subset of data for processing than a data set name requires. You can define the minimum amount of data to be monitored, collected, and reported on by including or excluding selection criteria, creating lists of elements, and specifying relational operators for most criteria.

Stage 1 filtering for SMF event monitoring: For SMF event monitoring, Stage 1 filtering occurs in the InfoSphere Guardium S-TAP for VSAM address space immediately after a monitored SMF record type is obtained by the collector, located at the SMF User Exit collection point.

Stage 1 filtering for Record level monitoring: For Record level monitoring, Stage 1 filtering occurs at OPEN time for KSDS and RRDS VSAM data sets.

Stage 2 filtering

Stage 2 filtering for SMF event and Record level monitoring applies to the following event types:

- Data Set Open
- Data Set Close
- Data Set Update
- Data Set Delete

- Data Set Rename
- Data Set Create
- Data Set Alter
- Data Set RACF Alter
- Data Set RACF Control
- Data Set RACF Read
- Data Set RACF Update

Default or specified event types are collected and passed on to the InfoSphere Guardium system.

Stage 2 filtering for Record level monitoring can be based on the type of logical record access as well as one or more values for the key of the VSAM data set. The types of record level access that can filtered on in Stage 2 are:

- Record Insert
- Record Delete
- Record Update
- Record Read

You can use a key value or list of key values, as well as a key range or list of key ranges, to further limit the amount and scope of data collected. The key data can be specified in normal printable characters or in hexadecimal by using the EBCDIC character set.

For key values, you can use generic characters in the specification of the keys. Only those records that pass Stage 2 filtering are collected and passed on to the InfoSphere Guardium system.

Stage 3 filtering

Stage 3 filtering is performed by InfoSphere Guardium S-TAP for VSAM based on Stage 2 filtering criteria that you define. During policy pushdown and activation, an analysis of the policy's filtering criteria is performed. This analysis enables pre-filtering processing determinations that can be performed across the product. Stage 3 pre-filtering can be very efficient in eliminating certain types of data collection, and ultimately reducing the path length through the product to provide optimal processing performance.

Examples:

- **SMF event monitoring:** The exclusion of certain SMF event monitoring types from your filtering criteria allows InfoSphere Guardium S-TAP for VSAM to bypass collection very early in the SMF User Exit data collection, and eliminates all downstream processing for that SMF record type.
- **Record level monitoring:** If no Record level monitoring event types are specified in the policy, Stage 2 filtering is eliminated, which reduces overhead significantly.

Exclusions

InfoSphere Guardium S-TAP for VSAM does not collect information on the following types of activities:

On DB2® subsystems

Activity within address spaces whose STC names have the following endings:

- MSTR (example: QA1XMSTR)
- DIST (example: QA1XDIST)
- IRLM (example: QA1XIRLM)
- DBM1 (example: QA1XDBM1)

On IMS™ subsystems

Accesses performed by the following program names:

- DFSMVRC0
- CQSINIT0
- HWSHWS00

Policy pushdown

Policy pushdown is a method of controlling the data collected by the InfoSphere Guardium S-TAP for VSAM agent. Policy pushdown enables the agent to evaluate the filtering criteria that you specified.

Evaluating a match

When searching for a match for the filtering criteria you have specified, an evaluation is performed through each data set level. Access rules are used for processing a data set when the filtering criteria of the following access types match the data:

- Job Name
- Program
- Dataset Name
- User ID
- Group ID
- SYSPLEX
- SSID
- SYS ID
- RECORG
- Job Type

The following values are not used to evaluate for a match on an access rule. They are used as sub-filtering criteria after a match on a data set is found:

- Key
- Key Range
- Data Set Event
- RLM Event

Multiple values are allowed in an access rule, as shown in the following example with two access rules:

Access Rule 1

Rule Type = INCLUDE

Job Name = JOBA

Key = "111111"

RLM Event = ALL

Access Rule 2

Rule Type = INCLUDE

Job Name = JOBA

Key = "222222"

RLM Event = ALL

When a match is found on Access Rule 1 for job JOBA, no further scanning of the Access Rules occurs. The keyword *Key* is not used as part of the Access Rule match. To filter on keys "111111" and "222222" for a job named JOBA, code the Access Rules as follows:

Access Rule 1

Rule Type = INCLUDE

Job Name = JOBA

Key = "111111","222222"

RLM Event = ALL

This rule searches for a match on the job name JOBA. If a match on JOBA is found, the RLM Event and Key values will be matched.

VSAM collection filtering parameters

All the fields are optional and most will have a default behavior as described.

Rule Type

Indicates whether this rule indicates inclusion or exclusion for events matching the criteria.

Allowed values are: INCLUDE | EXCLUDE: Include collects events satisfying the criteria specified, exclude does not collect those events. If nothing is specified, then INCLUDE is used.

Job Type

Indicates the type of jobs that should be considered for a match.

Should contain zero or more of the following values separated by a comma (,): JOB | STC | TSU | APPC, where:

JOB Jobs

STC Started Task

TSU Time Sharing User

APPC

Advanced Program-To-Program Communication

Note: If nothing is specified, then all types are collected.

SYS ID

Indicates the SMF System IDs to use when searching for a match.

1-4 character SMF System ID to match.

Can be optionally followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.

Valid wildcards are supported at any position. They are:

- Percent sign (%) for zero or more characters
- Question mark (?) for a single character match

If left blank, then all SMF System IDs are considered a match.

Examples:

SS01 Matches events occurring on SS01

SS01,EQ
Matches events occurring on SS01

SS%,EQ
Matches events occurring on systems with SS as the first two characters in the SMF System ID

RECORG
Indicates the record organization type to match.

Only affects RLM collection.

Can contain zero or more of the following values separated by a comma (,): KSDS|RRDS, where:

KSDS Key-sequenced data set

RRDS Relative record data set

If left blank, all record organization types for RLM are considered a match.

Examples:

KSDS Matches key-sequenced data set events

KSDS,RRDS
Matches key-sequenced data set and relative record data set events

User ID
Indicates the user ID to use when searching for a match.

1-8 character user ID to match.

Can be optionally followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.

Wildcards are supported.

If left blank, then activities for all user IDs are considered a match.

Examples:

PDUSER01
Matches events caused by user PDUSER01

PDUSER01,EQ
Matches events caused by user PDUSER01

PDUSER%,EQ
Matches events caused by users with the prefix PDUSER.

SSID Indicates the AUV ID to use when searching for a match.

1-4 character AUV ID optionally followed by a comma (,) and a relational operator. If no relational operator is provided EQ is assumed.

Wildcards are supported.

If left blank, activities for all SSID are considered a match.

Examples:

AUV1 Matches events from systems with AUV ID of AUV1

AUV1,EQ
Matches events from systems with AUV ID of AUV1

AUV%,EQ
Matches events from systems with AUV ID prefix of AUV

SYSPLEX
Indicates the z/OS sysplex name to use when searching for a match.

The specific 1-8 character z/OS sysplex name, optionally followed by a comma (,) and a relational operator. If no relational operator is provided, EQ is assumed.

Wildcards are supported.

If left blank, then activities for all SYSPLEX are considered a match.

Examples:

SYSPLEX1
Matches events from systems on SYSPLEX1

SYSPLEX1,EQ
Matches events from systems on SYSPLEX1

SYSPLEX%,EQ
Matches events from systems on a plex beginning with SYSPLEX

Program
Indicates the program name to use when searching for a match.

1-8 character program name, optionally followed by a comma (,) and a relational operator. If no relational operator is provided, EQ is assumed.

Wildcards are supported.

If left blank, activities from all programs are considered a match.

Examples:

IDCAMS
Matches events accessed via IDCAMS

IDCAMS,EQ
Matches events accessed via IDCAMS

IDCAM%,EQ
Matches events accessed via program beginning with IDCAM

Group ID
Indicates the group ID to use when searching for a match.

1-8 character representing the security system group ID optionally followed by a comma (,) and a relational operator. If no relational operator is provided EQ is assumed.

Wildcards are supported.

If left blank, then activities from all groups are considered a match.

Examples:

GROUP1
Matches events caused by someone within GROUP1

GROUP1,EQ
Matches events caused by someone within GROUP1

GROUP%,EQ
Matches events caused by someone within a group ID beginning with GROUP

Data Set Name
Indicates the data set name to use when searching for a match.

1-44 character representing the data set name for which activity is to be collected, optionally followed by the comma character (,) and a relational operator. If no relational operator is provided EQ is assumed.

Wildcards are supported.

If left blank, then all data set names are considered a match.

Examples:

HLQ1.MLQ1.LLQ1
Matches events on HLQ1.MLQ1.LLQ1

HLQ1.MLQ1.LLQ1,EQ
Matches events on HLQ1.MLQ1.LLQ1

HLQ%.MLQ%.LLQ%.EQ
Matches events with the data set name mask HLQ%.MLQ%.LLQ%

%.%%,EQ
Matches all data sets with more than one qualifier

%,EQ Matches all data sets with one qualifier

Job Name
Indicates the job name to use when searching for a match.

1-8 character representing the job name for which activity should be collected on, optionally followed by the comma character (,) and a relational operator. If no relational operator is provided, EQ is assumed.

Wildcards are supported.

If left blank, then activities from all jobs are considered a match.

Examples:

AUVJOB01
Matches events resulting from a job name AUVJOB01

AUVJOB01,EQ
Matches events resulting from a job name AUVJOB01

AUVJOB%,EQ
Matches events resulting from any job beginning with AUVJOB

Key Indicates the keys to consider when searching for a match.

One or more keys in plain text or hexadecimal format, representing the key for which to match event data during RLM processing.

Multiple keys should be delimited by a comma (,) optionally followed by the comma character (,) and a relational operator. If no relational operator is provided, EQ is assumed.

Plain text keys can be between 1-255 characters long.

Hexadecimal keys can be between 2-510 characters long and should always have an even number of characters.

An individual key should be surrounded in double quotes ("").

If the key is in hexadecimal format, then it should be prefixed with x' and suffixed with a single quotation mark ('). It should be placed inside double quotation marks, for example: "x'F0F0F1'"

A backslash (\) can precede any character to escape the character. For example:

"\x'0123"'
: Matches the plain text key "x'0123"' instead of a hexadecimal key. Both types can be supplied together.

Wildcards are supported. If a wildcard is to be supplied with a hexadecimal key, the wildcard should be in hexadecimal (6C for '%', 6E for '?').

If a provided key is greater than the actual length of the VSAM key, the key will be truncated. If the key provided is shorter than the VSAM key, it will be padded with hex zeroes.

If the Key and Key Range fields are blank, activities for all keys are considered a match.

Examples:

"KEY01"
: Matches RLM events with a key of KEY01

"KEY01","KEY02"
: Matches RLM events with a key of KEY01 or KEY02

"x'F0F0"'
: Matches RLM events with a key containing the hexadecimal value F0F0

"x'F0F0"',"x'F0F1"'
: Matches RLM events with a key containing the hexadecimal value of F0F0 or F0F1

"KEY01","x'F0F1"'
: Matches RLM events with a key of KEY01 or a key with the hexadecimal value of F0F1

"KEY0%"
: Matches RLM events with a key beginning with KEY0.

"x'F06C'"
: Matches RLM events with a key with a hexadecimal value beginning with F0

"\x'F06C'"
: Matches RLM events with a key of x'F06C'

Key Range
: Indicates the range of keys to consider when searching for a match.

  A pair of keys in plain text, or a pair of keys in hexadecimal, representing the range to match for record level monitoring. This should be specified as <key1>,<key2>.

A pair of keys must both be in plain text or both be in hexadecimal. Each plain text key in a plain text key pair can be 1-255 characters long. Each hexadecimal key in a hexadecimal key pair can be between 2-510 characters long and should have an even number of characters.

If the keys are in hexadecimal they should begin with x' and end with a single quotation mark ('). All keys should be enclosed in double quotes.

A backslash (\) can precede any characters to escape the character.

There should be an even number of keys in this field.

All key pairs should have the smaller key in the first value and the larger key in the second value, otherwise it will be rejected.

Wildcards are not supported in this field.

If the provided key is greater than the actual length of the VSAM key, the provided key will be truncated. If the key provided is shorter than the VSAM key, it will be padded with hex zeroes.

If the Key Range and Key fields are blank, activities for all keys are considered a match.

Examples:

"KEY01","KEY09″
Matches RLM events where the key is between KEY01 and KEY09

"KEY01","KEY09","KEY11","KEY19″
Matches RLM events where the key is between KEY01 and KEY09 or between KEY11 and KEY19

"x'F0F0'","x'F0F9'″
Matches RLM events where the key has a hexadecimal value between F0F0 and F0F9

"x'F0F0'","x'F0F9'","x'F1F0'","x'F1F9'"
Matches RLM events where the key has a hexadecimal value between F0F0 and F0F9 or between F1F0 and F1F9

"\x'F0F0'","\x'F0F9'″
Matches RLM events where the key is between x'F0F0' and x'F0F9'

RLM Event
Indicates what type of Record Level Monitoring events should be considered for a match.

Must contain zero or more of the following values separated by a comma (,): RINS | RDEL | RWRT | RGET | ALL | SKIP, where:

RINS A record insert within a data set of a supported type

RDEL
A record delete within a data set of a supported type

RWRT
A record level update within a record of a supported type

RGET
A record level read within a data set of a supported type

ALL

Returns all record level events

SKIP Returns no record level events

If left blank, then SKIP is the default and nothing is considered a match

Examples:

RINS Matches RLM events where the operation was a record insert

RINS,RDEL
Matches RLM events where the operation was a record insert or a record delete

Data Set Event
Indicates what type of SMF Data Set Events should be considered for a match.

Should contain zero or more of the following values separated by a comma (,):
DSOP | DSCL | DSUP | DSDL | DSRN | DSCR | DSALT | DSRAL | DSRCN | DSRRD | DSRUP | ALL
where:

DSOP
An OPEN event against a supported data set type

DSCL
A CLOSE event against a supported data set type

DSUP
An UPDATE event against a supported data set type

DSDL
A DELETE event against a supported data set type

DSRN
A RENAME event against a supported data set type

DSCR
A DEFINE or NEW ALLOCATION event of a supported data set type

DSALT
An ALTER of the attributes of a supported data set type

DSRAL
A security facility ALTER access of a supported data set type

DSRCN
A security facility CONTROL access of a supported data set type

DSRRD
A security facility READ access of a supported data set type

DSRUP
A security facility UPDATE access of a supported data set type

ALL Returns all data set level events

SKIP Returns no data set level events

If left blank, ALL is the default and all types are considered a match.

Examples:

DSOP Matches data set events where an open occurred.

DSOP,DSCL
Matches data set events where an open or a close occurred.

Valid relational operators are:

- EQ (Equals)
- NE (Does not equal)
- GE (Greater than or equal to)
- LE (Less than or equal to)
- GT (Greater than)
- LT (Less than)

Note:

- If you are using a relational operator with the **Group of Values** list, you must ensure that the operator is appended to the last field in the list, otherwise it will be treated as an additional value for that field.
- To use individual values along with those listed in the **Group of Values** list, the relational operator should be appended to the last field in the **Group of Values** list, rather than to the individual field.

String comparisons are performed in lexicographical order. Because the strings are in EBCDIC, the order is lowercase, uppercase, and then numeric. Special character positions depend on the hexadecimal value of the special character itself in relation to the other characters.

Chapter 5. Reference information

This section describes IBM InfoSphere Guardium S-TAP for VSAM reference information.

VSAM data set types

For data set level monitoring, the InfoSphere Guardium S-TAP for VSAM agent collects SMF data for the following VSAM data set types:

ESDS Entry sequence data set

KSDS Key-sequenced data set

RRDS Relative record data set

VRRDS
Variable length relative record data set

LDS Linear data set

The agent audits these data set types by correlating data from a combination of SMF record types to construct one of the following audit events.

DATA SET OPEN
An OPEN event against a supported data set type

DATA SET CLOSE
A CLOSE event against a supported data set type

DATA SET UPDATE
An UPDATE event against a supported data set type

DATA SET DELETE
A DELETE event of a supported data set type

DATA SET RENAME
A RENAME event of a supported data set type

DATA SET CREATE
A DEFINE or New Allocation event of a supported data set type

DATA SET ALTER
An ALTER of the attributes of a supported data set type

RACF ALTER
A security facility ALTER access of a supported data set type

RACF CONTROL
A security facility CONTROL access of a supported data set type

RACF UPDATE
A security facility UPDATE access of a supported data set type

RACF READ
A security facility READ access of a supported data set type

For Record level monitoring, the InfoSphere Guardium S-TAP for VSAM agent collects record access information for the following VSAM data set types:

KSDS Key-sequenced data set

RRDS Relative record data set

VRRDS
Variable length relative record data sets

The agent audits these Record level monitoring events:

RECORD INSERT
A record insert within a data set of a supported type.

RECORD DELETE
A record delete within a data set of a supported type.

RECORD READ
A record read within a data set of a supported type.

RECORD UPDATE
A record update within a data set of a supported type.

SMF record types and contexts

SMF records are correlated to InfoSphere Guardium S-TAP for VSAM context as shown in the SMF record types context table.

Table 2. SMF record types, subtypes, and contexts

Record number	Record subtype	SMF context
30		Accounting
42	I/O Statistics	Accounting
60	Insert	Created
61	DEFINE/CATLG	Created
62	Update	OPEN Update
64		CLOSE
65		Deleted
66*	Rename	Rename, ALTER
80		Security Access

*Some records have multiple subtypes.

Note:

- There is not a one-to-one correlation between SMF records and context events reported. If more than one SMF record is encountered within a step for a single event, then subsequent records are considered duplicates.
- Audit records for data set events are produced after the job that is generating the events has completed. SMF context events are stored in a temporary area until a closure event is received.
- Type 30 records are closure records for a job. When the type 30 end-of-job is encountered, SMF data is collected and saved, closed, and sent to the InfoSphere Guardium system. For long running tasks, such as a CICS task, this process might require significant time.

Related reference:

"InfoSphere Guardium S-TAP for VSAM components" on page 1
The product consists of the InfoSphere Guardium system, and the InfoSphere Guardium S-TAP for VSAM agent. The Guardium system is a server-based component that provides the product's user interface. The agent collects VSAM-related information that is obtained from the SMF record exit interface and VSAM I/O activities.

"Configuring the SMFPRMxx parameter library member" on page 7
To ensure a complete audit, you must configure the active SMFPRMxx member of the z/OS system PARMLIB to collect the required SMF record types needed by InfoSphere Guardium S-TAP for VSAM.

Chapter 6. Troubleshooting

Use these topics to diagnose and correct problems that you might experience with InfoSphere Guardium S-TAP for VSAM.

Messages and codes for IBM InfoSphere Guardium S-TAP for VSAM on z/OS

This information documents the messages and error codes issued by IBM InfoSphere Guardium S-TAP for VSAM. Messages are presented in ascending alphabetical and numerical order.

Error messages

InfoSphere Guardium S-TAP for VSAM error messages adhere to the following format: AUV*nnnx*

Where:

AUV Indicates that the messages was issued by InfoSphere Guardium S-TAP for VSAM.

nnn Indicates the message identification number.

x Indicates the severity of the message:

Table 3. Error message severity codes

Severity Code	Description
A	Indicates that operator intervention is required before processing can continue.
E	Indicates that an error occurred, which might or might not require operator intervention.
I	Indicates that the message is informational only.
W	Indicates that the message is a warning to alert you to a possible error condition.

AUV1000E INSUFFICIENT OPERATING SYSTEM LEVEL; OS/390 R2.10 (SP6.10) OR HIGHER REQUIRED

Explanation: Product initialization has determined that the level of the operating system is not at a level high enough to support the product.

User response: Run the product on a system with OS/390® at the 2.10 level or above.

AUV1001I RULEDEFS ACTIVATION SUCCESSFUL –*ssss*

Explanation: This message is issued to the operator console following successful activation of rule definitions using the ACTIVATE RULEDEFS operator command.

User response: No action is required.

AUV1002E INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING

Explanation: Product initialization was unable to obtain the required above-the-line storage.

User response: Increase the amount of available above-the-line storage and attempt to restart the product. If this is not successful, contact IBM Support.

AUV1003E INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING

Explanation: Product initialization was unable to obtain the required below-the-line storage.

User response: Increase the amount of available

below-the-line storage and attempt to restart the product. If this is not successful, contact IBM Support.

AUV1004E UNABLE TO LOCATE REQUIRED DDNAME - CONTROL

Explanation: During product initialization, the CONTROL DD statement was unable to be located in the product started task procedure.

User response: The CONTROL DD statement is required. Add the CONTROL DD statement to the product started task procedure and retry.

AUV1005E ERROR OCCURRED DURING SWAREQ PROCESSING FOR JFCB FOR DDNAME CONTROL, RC=*rrrrrrrr*

Explanation: An internal error (*rrrrrrrr*) occurred while processing the CONTROL DD statement during product initialization.

User response: Make sure that the CONTROL DD statement points to a valid partitioned data set and retry. If the error persists, contact IBM Support.

AUV1006E UNABLE TO LOCATE REQUIRED DDNAME - OPTIONS

Explanation: During product initialization, the OPTIONS DD statement was unable to be located in the product started task procedure.

User response: The OPTIONS DD statement is required. Add the OPTIONS DD statement to the product started task procedure and retry.

AUV1007E ERROR OCCURRED DURING SWAREQ PROCESSING FOR JFCB FOR DDNAME OPTIONS, RC=*rrrrrrrr*

Explanation: An internal error (*rrrrrrrr*) occurred while processing the OPTIONS DD statement during product initialization.

User response: Make sure that the OPTIONS DD statement points to a valid data set and retry. If the error persists, contact IBM Support.

AUV1008I RULEDEFS NOT ACTIVATED –*ssss*

Explanation: This message is issued in response to the **DISPLAY RULEDEFS** operator command when no rule definitions have been activated.

User response: No action is required.

AUV1009E OPEN FAILED FOR PROCESSING OPTIONS MEMBER; DEFAULT OPTIONS USED

Explanation: Open processing was unsuccessful for the OPTIONS member so the default options were used.

User response: Make sure that the OPTIONS DD statement points to a valid data set and retry. If the error continues, contact IBM Support.

AUV1012E ATTACH FOR AUVMAIN FAILED, RC=*rrrrrrrr*

Explanation: During product initialization, the startup of an internal task failed. The value *rrrrrrrr* identifies the internal error code.

User response: Examine other error messages that might have occurred at the same time as this message to aid in determining the cause of the failure. If no cause can be determined, contact IBM Support.

AUV1013I PRODUCT TERMINATION IS COMPLETE

Explanation: This message is issued in response to the product shutdown command at completion of termination processing.

User response: No action is required.

AUV1014E INVALID START PARAMETERS SPECIFIED; IGNORED

Explanation: An invalidly constructed parameter was specified on the START command for the started task; it will be ignored.

User response: Correct the START command parameter and restart the started task.

AUV1015E INVALID PARM SPECIFIED - *parm*

Explanation: An unrecognized parameter was specified on the START command for the started task where parm is the unrecognized parameter.

User response: Correct the START command parameter and restart the started task.

AUV1016E DELIMITER "=" IS MISSING - *parm*

Explanation: The START parameter specified by parm requires an equal sign followed by a keyword value; no equal sign was found.

User response: Correct the START command parameter and restart the started task.

AUV1017I START PARAMETER SPECIFIED - *parm*

Explanation: The TRACING START parameter specified by parm was successfully recognized and processed.

User response: No action is necessary.

AUV1018E INVALID VALUE SPECIFIED FOR PARAMETER - *parm*

Explanation: The TRACING START parameter keyword value for the parameter specified by *parm* was invalid.

User response: Correct the START parameter keyword value and restart the started task.

AUV1019I START PARAMETER SPECIFIED - *parm*

Explanation: The KEY START parameter specified by parm was successfully recognized and processed.

User response: No action is necessary.

AUV1020E VALUE SPECIFIED FOR PARAMETER - *parm*

Explanation: The KEY START parameter keyword value for the parameter specified by parm was invalid.

User response: Correct the START parameter keyword value and restart the started task.

AUV1021E INVALID OPTION SPECIFIED - *pppppppp*

Explanation: During product initialization, an invalid keyword was encountered when processing the subsystem options in the OPTIONS member. The value *pppppppp* is the invalid option encountered — or the value "(NONE)" if blank options were specified.

User response: Correct the specified option keyword and restart the product.

AUV1021E INVALID OPTION SPECIFIED - *pppppppp*

Explanation: During product initialization, an invalid keyword was encountered when processing the subsystem options in the OPTIONS member. The value *pppppppp* is the invalid option encountered — or the value "(NONE)" if blank options were specified.

User response: Correct the specified option keyword and restart the product.

AUV1022E REQUIRED DELIMITER "=" IS MISSING - *pppppppp*

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, a keyword was encountered which required an equal sign (=) but it was found to be missing. The value *pppppppp* indicates the associated keyword.

User response: Correct the specified option keyword and restart the product.

AUV1023E INVALID VALUE SPECIFIED FOR OPTION - *pppppppp*

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, a keyword was encountered with an invalid value. The value *pppppppp* indicates the option with the incorrect value.

User response: Correct the specified option keyword and restart the product.

AUV1024I PROCESSING OPTION SET - SSID=*ssss*

Explanation: This message is issued during product initialization to display the value (*ssss*) set for the SSID keyword in the OPTIONS member.

User response: No action is required.

AUV1025E INVALID VALUE SPECIFIED FOR OPTION - SSID=*ssss*

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the SSID option. The value *ssss* indicates the invalid value.

User response: Correct the specified option keyword and restart the product.

AUV1026I PROCESSING OPTION SET - INITIAL_RULEDEF=*rrrrrrrr*

Explanation: This message is issued during product initialization to display the value (*rrrrrrrr*) specified for the INITIAL_RULEDEF keyword in the OPTIONS member.

User response: No action is required.

AUV1027E INVALID VALUE SPECIFIED FOR OPTION -INITIAL_RULEDEF=*rrrrrrrr*

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the INITIAL_RULEDEF option. The value *rrrrrrrr* indicates the invalid value.

User response: Correct the specified option keyword and restart the product.

AUV1028I PROCESSING OPTION SET - PORT=*nnnnn*

Explanation: This message is issued during product initialization to display the value (*nnnnn*) specified for the PORT keyword in the OPTIONS member.

User response: No action is required.

AUV1029E INVALID VALUE SPECIFIED FOR OPTION - PORT=*nnnnn*

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the PORT option. The value *nnnnn* indicates the invalid value.

User response: Correct the specified option keyword and restart the product.

AUV1030I PROCESSING OPTION SET – PING_RATE=*nnnnn*

Explanation: This message is issued during product initialization to display the value (*nnnnn*) specified for the PING_RATE keyword in the OPTIONS member.

User response: No action is required.

AUV1031E INVALID VALUE SPECIFIED FOR OPTION – PING_RATE=*nnnnn*

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the PING_RATE option. The value *nnnnn* indicates the invalid value.

User response: Correct the specified option keyword and restart the product.

AUV1032I PROCESSING OPTION SET – RETRY_INTERVAL=*nnnnn*

Explanation: This message is issued during product initialization to display the value (*nnnnn*) specified for the RETRY_INTERVAL keyword in the OPTIONS member.

User response: No action is required.

AUV1033E VALUE SPECIFIED FOR OPTION – RETRY_INTERVAL=*nnnnn*

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the RETRY_INTERVAL option. The value *nnnnn* indicates the invalid value.

User response: Correct the specified option keyword and restart the product.

AUV1034E ERROR IN NAME/TOKEN RETRIEVAL PROCESSING, RC=*rrrrrrrr*

Explanation: During product initialization, an internal system error (*rrrrrrrr*) was encountered in establishing the product.

User response: Please contact IBM Support.

AUV1035E NAME/TOKEN ALREADY EXISTS, BUT TOKEN IS ZERO

Explanation: During product initialization, an internal system error was encountered in establishing the product.

User response: Please contact IBM Support.

AUV1036E NAME/TOKEN ALREADY EXISTS, BUT TOKEN DOES NOT POINT TO A VALID PRODUCT BLOCK

User response: IPL the system before starting the product. If this does not resolve the problem, contact IBM Support.

AUV1038E UNABLE TO OBTAIN STORAGE FOR PRODUCT CONTROL BLOCK, RC=*rrrrrrrr*

Explanation: During product initialization, above-the-line CSA storage was unable to be obtained a product control block as indicated by the internal return code *rrrrrrrr*.

User response: Investigate and correct the shortage of above-the-line CSA storage and restart the product. If the problem persists, contact IBM Support.

AUV1040E ERROR IN NAME/TOKEN CREATE PROCESSING, RC=*rrrrrrrr*

Explanation: During product initialization, an internal system error (*rrrrrrrr*) was encountered in establishing the product.

User response: Please contact IBM Support.

AUV1041I PRODUCT INTERCEPTS HAVE BEEN ESTABLISHED

Explanation: This message is issued when all intercepts have been successfully established.

User response: No action is required.

AUV1042E UNABLE TO OBTAIN STORAGE FOR COMMON AREA ROUTINE, RC=*rrrrrrrr*

Explanation: During product initialization, above-the-line CSA storage was unable to be obtained for loading a required product routine as detailed by the internal return code *rrrrrrrr*.

User response: Investigate and correct the shortage of above-the-line CSA storage and restart the product. If the problem persists, contact IBM Support.

AUV1043E BLDL FAILED FOR *mmmmmmmm*, RC=*rrrrrrrr*

Explanation: During product initialization, a required load module was unable to be successfully located. The value *mmmmmmmm* identifies the load module and the value *rrrrrrrr* specifies the internal return code in error.

User response: Verify that the load modules for the product are accessible either in a STEPLIB in the product started task, or in the system LINKLIST concatenation and then restart the product.

AUV1044E UNABLE TO DETERMINE ORIGIN OF *mmmmmmmm*

Explanation: During product initialization while processing the product load module *mmmmmmmm* an error was encountered.

User response: Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and restart the product.

AUV1046E PRIVATE LOAD FAILED FOR *mmmmmmmm*

Explanation: During product initialization, the processing of a product load module *(mmmmmmm*) to be located in above-the-line private storage failed.

User response: Verify that the load modules for the product are accessible either in a STEPLIB in the product started task, or in the system LINKLIST concatenation and then restart the product. In addition, check the available amount of above-the-line private storage available for the product started task. After correcting the problem, restart the product. If the error cannot be determined, contact IBM Support.

AUV1047E COMMON LOAD FAILED FOR *mmmmmmmm*

Explanation: During product initialization, the processing of a product load module (*mmmmmmm*) to be located in above-the-line common storage, failed.

User response: Verify that the load modules for the product are accessible either in a STEPLIB in the product started task, or in the system LINKLIST concatenation and then restart the product. In addition, check the available amount of above-the-line common storage available for the product started task. After correcting the problem, restart the product. If the error cannot be determined, contact IBM Support.

AUV1048I PROCESSING OPTION SET – RETRY_COUNT=*nnnnn*

Explanation: This message is issued during product initialization to display the value (*nnnnn*) specified for the RETRY_COUNT keyword in the OPTIONS member.

User response: No action is required.

AUV1049E INVALID VALUE SPECIFIED FOR OPTION – RETRY_COUNT=*nnnnn*

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the RETRY_COUNT option. The value *nnnnn* indicates the invalid value.

User response: Correct the specified option keyword and restart the product.

AUV1050E UNABLE TO ESTABLISH *NNNNNNNNNNNNNNN* EXIT, RC=*RRRRRRRR*, RS=*SSSSSSSS*

Explanation: During started task initialization or as a result of the ENABLE SMFEXIT1 operator command, an error was encountered attempting to establish the SMF exit named *NNNNNNNNNNNNNNN*. The return code encountered is specified by *RRRRRRRR* and the reason code is specified by *SSSSSSSS*.

This message might be caused by having more than one agent active on a single z/OS image. Only one agent per z/OS image is required.

User response: Verify that no more than one agent is active per z/OS image. If that does not resolve the error, contact IBM Support.

AUV1052E UNABLE TO DELETE *NNNNNNNNNNNNNNN* EXIT, RC=*RRRRRRRR*, RS=*SSSSSSSS*

Explanation: During started task termination or as a result of the DISABLE SMFEXIT1 operator command, an error was encountered attempting to delete the SMF exit named *NNNNNNNNNNNNNNN*. The return code encountered is specified by *RRRRRRRR* and the reason code is specified by *SSSSSSSS*.

User response: Contact IBM Support.

AUV1054E GSSB IS NOT PRESENT

Explanation: During activation of a policy RULEDEFS member, a necessary InfoSphere Guardium S-TAP for VSAM on z/OS control block could not be located.

User response: Ensure that the InfoSphere Guardium S-TAP for VSAM on z/OS started task has been successfully started. If no error was encountered during the initialization of the started task, contact IBM technical support.

AUV1055E GSSB CONTROL BLOCK ID IS INVALID

Explanation: During activation of a policy RULEDEFS member, a necessary InfoSphere Guardium S-TAP for VSAM on z/OS control block was located but it is not valid.

User response: Ensure that the InfoSphere Guardium S-TAP for VSAM on z/OS started task has been successfully started. If no error was encountered during the initialization of the started task, contact IBM technical support.

AUV1056I PROCESSING OPTION SET – SOCKET_TIMEOUT=*nnnnn*

Explanation: This message is issued during product initialization to display the value (*nnnnn*) specified for the SOCKET_TIMEOUT keyword in the OPTIONS member.

User response: No action is required.

AUV1058E UNABLE TO LOCATE LPDE FOR IGC0005E

Explanation: During product initialization, a required pointer to an operating system module could not be located.

User response: Contact IBM Support.

AUV1058I PROCESSING OPTION SET – TCP/IP_ADDRESS=*a

Explanation: This message is issued during product initialization to display the value (*a**) specified for the TCP/IP_ADDRESS keyword in the OPTIONS member.

User response: No action is required.

AUV1059E INVALID VALUE SPECIFIED FOR OPTION - TCP/IP_ADDRESS=*a

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the TCP/IP_ADDRESS option. The value *a** indicates the invalid value.

User response: Correct the specified option keyword and restart the product.

AUV1060I PROCESSING OPTION SET – AGENT_NAME=*a

Explanation: This message is issued during product initialization to display the value (*a**) specified for the AGENT_NAME keyword in the OPTIONS member.

User response: No action is required.

AUV1061E VALUE SPECIFIED FOR OPTION – AGENT_NAME=*a

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the AGENT_NAME option. The value *a** indicates the invalid value.

User response: Correct the specified option keyword and restart the product.

AUV1065E UNABLE TO LOCATE LPDE FOR IDA0192A

Explanation: During Record Level Monitoring initialization, a required pointer to an operating system module could not be located.

User response: Contact IBM Support.

AUV1066E UNABLE TO LOCATE IDA0192A

Explanation: During Record Level Monitoring initialization, a required operating system module could not be located.

User response: Contact IBM Support.

AUV1067E PAGE SERVICE LIST EXHAUSTED FOR *xx* INTERCEPT

Explanation: During Record-Level Monitoring initialization, an unexpected internal error occurred during an attempt to establish a product intercept. The intercept, identified by *xx*, is "O1" for open-intercept one, or "C1" for close-intercept one.

User response: Contact IBM Support.

AUV1068E UNABLE TO OBTAIN STORAGE FOR *xx* INTERCEPT, RC=*rrrrrrrr*

Explanation: During Record-Level Monitoring initialization, an error specified as *rrrrrrrr* was encountered during an attempt to obtain common storage for a product control block. The intercept, identified by *xx*, is "O1" for open-intercept one, or "C1" for close-intercept one.

User response: Investigate a potential shortage of common storage and restart the product. If the problem continues, contact IBM Support.

AUV1069E UNABLE TO LOCATE IDA0200T

Explanation: During Record-Level Monitoring initialization, a required operating system module could not be located.

User response: Contact IBM Support.

AUV1073W MAXIMUM ACTIVE SUBSYSTEMS EXCEEDED (1)

Explanation: The current iteration of the product being started would exceed the limit of one concurrently active subsystems on a single z/OS system. Startup for the current iteration is terminated.

User response: If the current iteration of the product is needed, shut down one of the already active subsystems and then restart the current iteration. To display all currently active subsystems use the "`display,subsystems,all`" command.

AUV1074E DUPLICATE SUBSYSTEM FOUND FOR SSID=*ssss*

Explanation: During product initialization, a duplicate product control block was encountered for the subsystem ID *ssss*.

User response: Contact IBM Support.

AUV1080E ERROR IN NAME/TOKEN DELETE PROCESSING, RC=*rrrrrrrr*

Explanation: During product initialization, an error occurred that required product termination. During termination, an attempt was made to delete the product's NAME/TOKEN, but the NAME/TOKEN DELETE service encountered an error. *rrrrrrrr* contains the value returned in register 15.

System action: Product termination continues.

User response: Contact IBM Support.

AUV1081E GETMAIN FAILED FOR JSPB VECTOR TABLE, RC=*rrrrrrrr*

Explanation: During product initialization, the specified error *rrrrrrrr* occurred while attempting to obtain common storage for a product control block.

User response: Investigate a potential shortage of above-the-line common storage and restart the product. If the problem continues, contact IBM Support.

AUV1100E ACRONYM CHECK FAILED FOR GSSB

Explanation: An internal error occurred within the product during product initialization.

User response: Contact IBM Support.

AUV1101E INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING

Explanation: Main task startup was unable to obtain enough above-the-line private storage to initialize.

User response: Increase the amount of above-the-line private storage. If the problem persists, contact IBM Support.

AUV1102E ERROR OCCURRED IN CROSS-MEMORY INITIALIZATION

Explanation: An internal error occurred during main task startup.

User response: Contact IBM Support.

AUV1103E ATTACH FOR AUVPING FAILED, RC=*rrrrrrrr -ssss*

Explanation: During initialization of the InfoSphere Guardium S-TAP for VSAM started task, an error was encountered during the attach of the subtask named AUVPING for the subsystem *SSSS*. The return code encountered is specified by *RRRRRRRR*.

User response: Ensure that the STEPLIB for the started task contains all of the load modules included with InfoSphere Guardium S-TAP for VSAM on z/OS. If the STEPLIB appears to correctly contain all of the product load modules, contact IBM Support.

AUV1105E ATTACH FOR AUVSSRP FAILED, RC=*rrrrrrrr -ssss*

Explanation: During initialization of the InfoSphere Guardium S-TAP for VSAM started task, an error was encountered during the attach of the subtask named AUVSSRP for the subsystem *SSSS*. The return code encountered is specified by *RRRRRRRR*.

User response: Ensure that the STEPLIB for the started task contains all of the load modules Included with the InfoSphere Guardium S-TAP for VSAM for VSAM on z/OS product. If the STEPLIB appears to correctly contain all of the product load modules, contact IBM technical support.

AUV1105I SUBSYSTEM IS ACTIVE AND ENABLED

Explanation: This message indicates that the main product task has successfully started and is now active.

User response: No action is required.

AUV1106I SUBSYSTEM INITIALIZATION IS COMPLETE

Explanation: This message is issued when the main product task has successfully completed initialization processing.

User response: No action is required.

AUV1107I PRODUCT TERMINATION HAS BEEN REQUESTED

Explanation: This message is issued when the main product task has initiated subsystem shutdown processing, either due to a command request or because of an unrecoverable error condition.

User response: No action is required if this is due to a command request. If this is due to an unrecoverable error, restart the subsystem address space. Contact IBM Technical Support if problems persist.

AUV1111E UNABLE TO OBTAIN STORAGE FOR COMMON AREA ROUTINE, RC=*rrrrrrrr*

Explanation: Product subsystem initialization was unable to obtain a sufficient amount of storage to load a required module.

User response: Check and increase the amount available above- and below-the-line storage and restart the product. If the error persists, contact IBM Support.

AUV1112E BLDL FAILED FOR *mmmmmmmm*, RC=*rrrrrrrr*

Explanation: During product subsystem initialization, a required load module was unable to be successfully located. The value *mmmmmmmm* identifies the load module and the value *rrrrrrrr* specifies the internal return code in error.

User response: Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and then restart the product.

AUV1113E UNABLE TO DETERMINE ORIGIN OF *mmmmmmmm*

Explanation: An error was encountered during product subsystem initialization while processing the product load module *mmmmmmmm*.

User response: Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and then restart the product

AUV1115E INITIAL LOAD FAILED FOR *mmmmmmmm*

Explanation: During product subsystem initialization, a required load module (*mmmmmmmm*) did not load successfully.

User response: Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and then restart the product. In addition, check the available amount of above-the-line private storage available for the product started task. After correcting the problem restart the product. If the error cannot be determined, contact IBM Support.

AUV1116E DIRECTED LOAD FAILED FOR *mmmmmmmm*

Explanation: During product subsystem initialization, a required load module (*mmmmmmmm*) did not load successfully.

User response: Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and then restart the product.

AUV1117E NON-ZERO RETURN CODE FROM SYSEVENT, RC=*rrrrrrrr* -*ssss*

Explanation: During product subsystem initialization, an error (*rrrrrrrr*) was encountered when attempting to make the product started task address space non-swappable for subsystem *ssss*.

User response: Contact IBM Support.

AUV1122E INVALID COMMAND SPECIFIED - *cccccccc* -*ssss*

Explanation: The product subsystem command parser received an error while processing the command (*cccccccc*) issued to the started task for subsystem ID *ssss*.

User response: Correct and re-issue the command.

AUV1123E INVALID COMMAND SPECIFIED - *cccccccc* -*ssss*

Explanation: An invalid or null product subsystem command (*cccccccc*) was issued to the started task for subsystem ID *ssss*.

User response: Correct and re-issue the command.

AUV1123W ACTIVE SUBSYSTEM DETECTED; PRODUCT-LEVEL MODULE NOT RE-INITIALIZED

Explanation: While a version of the product subsystem was active, an attempt was made to initiate the same product subsystem. The subsequent attempt to start the subsystem fails. Only one instance of the subsystem is allowed on a z/OS image at a time.

User response: No action required. If you are attempting to initiate a new version of the subsystem, first shut down the currently executing version of the subsystem.

AUV1124E EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc* **-***ssss*

Explanation: More operands than are allowed were specified for the **DISPLAY** command issued (*cccccccc*) to the product started task for subsystem ID *ssss*.

User response: Re-issue the command using the correct number of operands.

AUV1125E INSUFFICIENT OPERANDS SPECIFIED FOR COMMAND - *cccccccc* **-***ssss*

Explanation: The command entered contains fewer operands than the minimum required. The command entered is *cccccccc*. The subsystem ID is *ssss*.

User response: Re-issue the command using the correct number of operands.

AUV1126E INVALID OPERAND SPECIFIED FOR COMMAND - *cccccccc* **-***ssss*

Explanation: The command entered contains an invalid operand. The command entered is *cccccccc*. The subsystem ID is *ssss*.

User response: Correct the invalid operand and re-issue the command.

AUV1127I SUBSYSTEM IS ACTIVE | INACTIVE AND ENABLED | DISABLED -*ssss*

Explanation: This message is issued in response to the **DISPLAY SUBSYSTEM** or **DISPLAY ALL** operator command and shows the ACTIVE or INACTIVE status of the product subsystem and whether or not the subsystem is ENABLED or DISABLED for the subsystem *ssss*.

User response: No action is required.

AUV1128E INVALID COMMAND SPECIFIED - *command*

Explanation: An unrecognized InfoSphere Guardium S-TAP for VSAM operator command was issued to the started task where command is the unrecognized command.

User response: Issue a valid operator command to the started task.

AUV1129I THERE ARE CURRENTLY NO SUBSYSTEMS -*ssss*

Explanation: This message is issued in response to the product operator command **DISPLAY SUBSYSTEM ALL** when no subsystems are located.

User response: No action is required.

AUV1130I SUBSYSTEM xxxx IS ACTIVE | INACTIVE AND ENABLED | DISABLED -*ssss*

Explanation: This message is issued in response to the **DISPLAY SUBSYSTEM ALL** operator command issued to subsystem *ssss* and shows the ACTIVE or INACTIVE status of each product subsystem as identified by *xxxx* and whether or not the subsystem is ENABLED or DISABLED.

User response: No action is required.

AUV1131I RULEDEFS ACTIVATED ON *mm/dd/yyyy* **AT** *hh:mm:ss* **FROM MEMBER** *mmmmmmmm* **-***ssss*

Explanation: This message is issued in response to the **DISPLAY RULEDEFS** operator command to subsystem ID *ssss* and shows the date *mm/dd/yyyy* and time *hh:mm:ss* at which the active set of RULEDEFS was last activated as well as the member name (*mmmmmmmm*) from which they were activated.

User response: No action is required.

AUV1132I RULEDEFS NOT ACTIVATED -*ssss*

Explanation: This message is issued in response to the **DISPLAY RULEDEFS** operator command to subsystem ID *ssss* when no RULEDEFS were found to have been activated.

User response: No action is required.

AUV1136I PRODUCT-LEVEL TRACING IS ENABLED | DISABLED -*ssss*

Explanation: This message is issued in response to the **DISPLAY TRACING** operator command to subsystem ID *ssss* and shows whether or not the product tracing facility is ENABLED or DISABLED.

User response: No action is required.

AUV1137I SUBSYSTEM-LEVEL TRACING IS ENABLED | DISABLED -*ssss*

Explanation: This message is issued in response to the **DISPLAY TRACING** operator command to subsystem ID *ssss* and shows whether or not the subsystem tracing facility is ENABLED or DISABLED.

User response: No action is required.

AUV1138E EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc* **-***ssss*

Explanation: More operands than are allowed were specified for the **ENABLE** command issued (*cccccccc*) to the product started task for subsystem ID *ssss*.

User response: Re-issue the command using the

correct number of operands.

AUV1140I SMF MONITORING SUCCESSFULLY ENABLED – *SSSS*

Explanation: The **ENABLE SMFM** command was processed for the specified subsystem *SSSS*. The required SMF monitoring exits have been loaded and enabled.

User response: No response is required.

AUV1141I SUBSYSTEM IS NOW ENABLED -*ssss*

Explanation: This message is issued in response to the **ENABLE SUBSYSTEM** operator command and indicates that the subsystem *ssss* was successfully enabled.

User response: No action is required.

AUV1143I SMF MONITORING SUCCESSFULLY DISABLED –*SSSS*

Explanation: The **DISABLE SMFM** command was processed for the specified subsystem *SSSS*. The required SMF monitoring exits have been disabled and unloaded.

User response: No response is required.

AUV1144I TRACING FOR PRODUCT IS NOW ENABLED -*ssss*

Explanation: This message is issued in response to the **ENABLE TRACING** or **ENABLE TRACING ALL** operator command for subsystem ID *ssss* and indicates that product level tracing is now enabled.

User response: No action is required.

AUV1145I TRACING FOR SUBSYSTEM IS NOW ENABLED -*ssss*

Explanation: This message is issued in response to the **ENABLE TRACING ALL** operator command for subsystem ID *ssss* and indicates that subsystem level tracing is now enabled.

User response: No action is required.

AUV1146E EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc* **-***ssss*

Explanation: More operands than are allowed were specified for the **DISABLE** command issued (*cccccccc*) to the product started task for subsystem ID *ssss*.

User response: Re-issue the command using the correct number of operands.

AUV1149I SUBSYSTEM IS NOW DISABLED -*ssss*

Explanation: This message is issued in response to the **DISABLE SUBSYSTEM** operator command and indicates that the subsystem *ssss* was successfully disabled.

User response: No action is required.

AUV1151E SMF MONITORING DISABLE NOT SUCCESSFUL –*SSSS*

Explanation: The **DISABLE SMFM** command could not be processed for the specified subsystem *SSSS*. The SMF monitoring exits are still loaded and enabled.

User response: Contact IBM Support.

AUV1152I TRACING FOR PRODUCT IS NOW DISABLED -*ssss*

Explanation: This message is issued in response to the **DISABLE TRACING** or **DISABLE TRACING ALL** operator command for subsystem ID *ssss* and indicates that product level tracing is now disabled.

User response: No action is required.

AUV1153I TRACING FOR SUBSYSTEM IS NOW DISABLED -*ssss*

Explanation: This message is issued in response to the **DISABLE TRACING ALL** operator command for subsystem ID *ssss* and indicates that subsystem level tracing is now disabled.

User response: No action is required.

AUV1154E EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc* **-***ssss*

Explanation: More operands than are allowed were specified for the **ACTIVATE** command issued (*cccccccc*) to the product started task for subsystem ID *ssss*.

User response: Re-issue the command using the correct number of operands.

AUV1155E SMF MONITORING ENABLE FAILED –*SSSS*

Explanation: The **ENABLE SMFM** command failed to process for the specified *SSSS*. The SMF monitoring exits are not loaded or enabled.

User response: Ensure that the STEPLIB for the started task contains all of the load modules required for the product. If no error can be found, contact IBM Support.

AUV1156E SMF MONITORING ALREADY ENABLED –*SSSS*

Explanation: The **ENABLE SMFM** command was issued for the specified subsystem *SSSS* but the SMFEXIT1 exits are already enabled. The SMF exits are still loaded and enabled.

User response: No response is required.

AUV1157E OPERANDS SPECIFIED FOR COMMAND - *command*

Explanation: An operator command as identified by command was issued to the started task for subsystem *SSSS*, but more operands were specified than are permitted for the particular command.

User response: Correct and reissue the operator command.

AUV1158E SMF MONITORING ALREADY DISABLED –*SSSS*

Explanation: The **DISABLE SMFM** command was issued for the specified subsystem *SSSS* but the SMF monitoring exits are already disabled.

User response: No response is required.

AUV1175I *DDDDDDDD* MEMBER ACTIVATION SUCCESSFUL –*SSSS*

Explanation: A policy member as identified by DDDDDDDD for subsystem SSSS was successfully activated.

User response: No action is required.

AUV1176E *DDDDDDDD* MEMBER ACTIVATION FAILED – SEE JESYSMSG FOR DETAILS –*SSSS*

Explanation: A policy member as identified by *DDDDDDDD* for subsystem *SSSS* could not be successfully activated. The JESYSMSG output data set for the started task contains details of the error(s) encountered.

User response: Contact IBM Technical Support.

AUV1176I *dddddddd* MEMBER *mmmmmmmm* ACTIVATION FAILED - SEE JESYSMSG FOR DETAILS -*ssss*

Explanation: This message is issued in response to the **ACTIVATE RULEDEFS** operator command or the initial RULEDEFS activation (as indicated from the OPTIONS member for subsystem ID *ssss*) to show that the activation of the RULEDEFS from member *mmmmmmmm* was not successful due to syntax errors.

User response: Review the error messages in the JES SYSMSG output for the product started task, and then correct the errors and re-activate the RULEDEFS.

AUV1177I *dddddddd* MEMBER *mmmmmmmm* ACTIVATION FAILED - FAILURE CODE *cccc* -*ssss*

Explanation: This message is issued in response to the **ACTIVATE RULEDEFS** operator command, or the initial RULEDEFS activation (as indicated from the OPTIONS member for subsystem ID *ssss)* to show that the activation of the RULEDEFS from member *mmmmmmmm* was not successful due to an internal error as denoted by *cccc*.

User response: Review any error messages in the JES SYSMSG output or the console log for the product started task to determine the possible cause of the error, then correct the errors and re-activate the RULEDEFS. If the problem persists, contact IBM Support.

AUV1179E *DDDDDDDD* MEMBER ACTIVATION FAILED - FAILURE CODE *CCCCCCCC* –*SSSS*

Explanation: A policy member as identified by *DDDDDDDD* for subsystem *SSSS* could not be successfully activated. The failure code is identified by *CCCCCCCC*.

User response: Contact IBM Technical Support.

AUV1184E COMMAND VERB NOT UNIQUE - cccccccc -ssss

Explanation: More than one command exists that matches the abbreviation specified (*cccccccc*) for the command verb. The product subsystem processing the command was *ssss*.

User response: Re-issue the command, using a command verb abbreviation that more uniquely specifies the intended command.

AUV1185E INVALID COMMAND SYNTAX SPECIFIED - *ssss*

Explanation: The command entered contains invalid syntax. The product subsystem processing the command was *ssss*.

User response: Review the command entered and correct the syntax.

AUV1191E INVALID MODULE NAME SPECIFIED - *cccccccc*

Explanation: The command entered specifies an invalid module name. The command entered is *cccccccc*.

User response: Re-issue the command with a correct module name.

AUV1192I MODULE *mmmmmmmm vvvv ffffffff dddddddd ttttt*

Explanation: Module header information is displayed, where *mmmmmmmm* is the name of the module, *vvvv* is the version, *ffffffff* is the FMID *dddddddd* is the assembly date and *ttttt* is the assembly time.

User response: None.

AUV1193I MODULE *mmmmmmmm* **LOCATED AT** *aaaaaaaa* **(***stgloc***)**

Explanation: The module address (with offset if specified) is displayed, where *mmmmmmmm* is the name of the module, *aaaaaaaa* is the virtual storage address, and *stgloc* is the storage location ("PRIVATE" or "COMMON").

User response: None.

AUV1195E ERROR OCCURRED DURING FREEMAIN FOR GPB, RC=*rrrrrrrr*

Explanation: During initialization, the product encountered an error and determined that termination was necessary. As part of termination, an attempt was made to freemain the product control block, but the FREEMAIN service encountered an error. *rrrrrrrr* contains the value returned in register 15. Product termination continues.

User response: Contact IBM Support.

AUV1196E UNEXPECTED VCON COUNT FOR *xx* **INTERCEPT; EXPECTED=***eee***, FOUND=***fff*

Explanation: While setting product intercept *xx*, An unexpected VCON count was encountered for a particular csect. The expected VCON count is *eee* and the actual VCON count is *fff*. This does not necessarily indicate a problem, but a problem is possible.

System action: An SVC dump is taken. Depending upon the particular intercept, product initialization may continue or terminate.

User response: Contact IBM Support.

AUV1200E UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA

Explanation: A service task of the main product started task was unable to obtain the required amount of above-the-line storage.

User response: Increase the amount of above-the-line storage for the product task. If the problem persists, contact IBM Support.

AUV1202E UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA

Explanation: A service task of the main product started task was unable to obtain the required amount of above-the-line storage.

User response: Increase the amount of above-the-line storage for the product task. If the problem persists, contact IBM Support.

AUV1203E UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA

Explanation: A product module was unable to obtain the required amount of above-the-line virtual storage.

User response: Increase the amount of above-the-line storage for the InfoSphere Guardium S-TAP for VSAM started task and restart. If the problem persists, contact IBM Support.

AUV1204E UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA

Explanation: A service task of the main product started task was unable to obtain the required amount of above-the-line storage.

User response: Increase the amount of above-the-line storage for the InfoSphere Guardium S-TAP for VSAM started task. If the problem persists, contact IBM Support.

AUV1213E ERROR RETRIEVING SSRE

Explanation: An internal error was encountered.

User response: Contact IBM Technical support.

AUV1214E UNEXPECTED SSRE QUEUE ERROR

Explanation: An internal error was encountered.

User response: Contact IBM Technical support.

AUV1215E UNEXPECTED SSRE QUEUE ERROR

Explanation: An internal error was encountered.

User response: Contact IBM Technical support.

AUV1400I RECORD LEVEL MONITORING IS *EEEEEEEE* **-***SSSS*

Explanation: This message is issued in response to the InfoSphere Guardium S-TAP for VSAM operator command **`DISPLAY RLM`** for subsystem *SSSS*. The value *EEEEEEEE* indicates *ENABLED* or *DISABLED*.

User response: No response is required.

AUV1401I RECORD LEVEL MONITORING INTERCEPTS ARE *EEEEEEEE* -*SSSS*

Explanation: This message is issued in response to the InfoSphere Guardium S-TAP for VSAM operator command **DISPLAY RLM** for subsystem *SSSS*. The value *EEEEEEEE* indicates ENABLED or DISABLED.

User response: No response is required.

AUV1402I CURRENT POLICY *EEE* -*SSSS*

Explanation: This message is issued in response to the InfoSphere Guardium S-TAP for VSAM operator command **DISPLAY RLM** for subsystem *SSSS*. The value *EEE* indicates either "CONTAINS RLM FILTERS" or "DOES NOT CONTAIN RLM FILTERS".

User response: No response is required.

AUV1405I RECORD LEVEL MONITORING SUCCESSFULLY ENABLED -*SSSS*

Explanation: This message is issued in response to the InfoSphere Guardium S-TAP for VSAM operator command **ENABLE RLM** for subsystem *SSSS*.

User response: No response is required.

AUV1406W RECORD LEVEL MONITORING SUCCESSFULLY ENABLED, BUT NO RLM FILTERS EXIST IN CURRENT POLICY -*SSSS*

Explanation: This message is issued in response to the InfoSphere Guardium S-TAP for VSAM operator command **ENABLE RLM** for subsystem *SSSS*. The enable was successful, but no filters specifying RLM processing exist in the currently activated policy.

System action: Record Level Monitoring will not be performed.

User response: To perform Record Level Monitoring, add RLM definitions to the policy and activate it.

AUV1408W POLICY CONTAINING RECORD LEVEL MONITORING FILTERS ACTIVATED, BUT RLM IS CURRENTLY DISABLED -*SSSS*

Explanation: This message is issued in response to the InfoSphere Guardium S-TAP for VSAM operator command **ENABLE RLM** for subsystem SSSS. The policy activation containing RLM filters was successful, but RLM processing is currently disabled.

System action: Record Level Monitoring will not be performed.

User response: To perform Record Level Monitoring, issue the **ENABLE RLM** command for subsystem *SSSS*.

AUV1410I PROCESSING OPTION SET - SOCKET_CONNECT_TIMEOUT=*nnnnn*

Explanation: This message is issued during product initialization to display the value (nnnnn) specified for the SOCKET_CONNECT_TIMEOUT keyword in the OPTIONS member.

User response: No action required.

AUV1411E INVALID VALUE SPECIFIED FOR OPTION - SOCKET_CONNECT_TIMEOUT=*nnnnn*

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the SOCKET_CONNECT_TIMEOUT option. The value *nnnnn* indicates the invalid value.

User response: Correct the specified option keyword and restart.

AUV1412I PROCESSING OPTION SET - SPILL_BUFFER_SIZE=*nnnnnnn*

Explanation: This message is issued during product initialization to display the value (nnnnnnn) specified for the SPILL_BUFFER_SIZE keyword in the OPTIONS member.

User response: No action required.

AUV1413E INVALID VALUE SPECIFIED FOR OPTION – SPILL_BUFFER_SIZE=*nnnnnnn*

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the SPILL_BUFFER_SIZE option. The value *nnnnnnn* indicates the invalid value.

User response: Correct the specified option keyword and restart.

AUV1414I PROCESSING OPTION SET - INTERNAL_BUFFER_SIZE=*nnnnnnn*

Explanation: This message is issued during product initialization to display the value (*nnnnnnn*) specified for the INTERNAL_BUFFER_SIZE keyword in the OPTIONS member.

User response: No action required.

AUV1415E INVALID VALUE SPECIFIED FOR OPTION INTERNAL_BUFFER_SIZE=*nnnnnnn*

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the

INTERNAL_BUFFER_SIZE option. The value *nnnnnnn* indicates the invalid value.

User response: Correct the specified option keyword and restart.

AUV1416I PROCESSING OPTION SET - SECONDARY_IPADDR_PORT=(a*,*nnnnn*)

Explanation: This message is issued during product initialization to display the values (a* and *nnnnn*) specified for the SECONDARY_IPADDR_PORT keyword in the OPTIONS member.

User response: No action required.

AUV1417E INVALID VALUE SPECIFIED FOR OPTION - SECONDARY_IPADDR_PORT=(a*,*nnnnn*)

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the SECONDARY_IPADDR_PORT option. The values *a** and *nnnnn* indicate the invalid values.

User response: Correct the specified option keyword and restart.

AUV1419E INVALID VALUE SPECIFIED FOR OPTION - IAM_SMF_RECORD_ID = *nnn*

Explanation: While processing the subsystem options in the OPTIONS member during product initialization, an incorrect value was encountered for the IAM_SMF_RECORD_ID option. The value *nnn* indicates the invalid value.

User response: Correct the specified option keyword and restart.

AUV1420I PROCESSING OPTION SET - ACF_SMF_RECORD_ID = *nnn*

Explanation: This message is issued during product initialization to display the value specified for the ACF_SMF_RECORD_ID keyword in the OPTIONS member. This keyword identifies the SMF record ID for the ACF2 records.

User response: For Guardium S-TAP for VSAM to report access failures to a unique record ID, specify the value *nnn* in the Guardium S-TAP for VSAM CONTROL data set ACF_SMF_RECORD_ID option.

AUV1421E INVALID VALUE SPECIFIED FOR OPTION - ACF_SMF_RECORD_ID = *nnn*

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the ACF_SMF_RECORD_ID option. The value nnn indicates the invalid value.

User response: Correct the specified option keyword and restart.

AUV1438I SMF MONITORING IS *EEEEEEEE* -*SSSS*

Explanation: This message is issued in response to the InfoSphere Guardium S-TAP for VSAM operator command **DISPLAY SMFEXIT1** for subsystem *SSSS*. The value *EEEEEEEE* indicates *ENABLED* or *DISABLED*.

User response: No response is required.

AUV1439I SMF MONITORING EXITS ARE *EEE* -*SSSS*

Explanation: This message is issued in response to the InfoSphere Guardium S-TAP for VSAM operator command **DISPLAY SMFM** for subsystem *SSSS*. The value *EEE* indicates “ACTIVE/LOADED” or “NOT ACTIVE/LOADLED”.

User response: No response is required.

AUV1747E SUBSYSTEM IS NOT ACTIVE OR ENABLED

Explanation: This message is issued when, during the activation of a policy, the InfoSphere Guardium S-TAP for VSAM subsystem is found to be disabled or inactive. The policy is not activated.

User response: Ensure that the InfoSphere Guardium S-TAP for VSAM for VSAM started task has been started and that the subsystem is enabled and the hooks are active. If the problem persists, contact IBM Technical Support.

AUV1748W POLICY CONTAINING RECORD LEVEL MONITORING FILTERS ACTIVATED, BUT RLM IS CURRENTLY DISABLED -*SSSS*

Explanation: This message is issued in response to the InfoSphere Guardium S-TAP for VSAM policy pushdown operation for subsystem *SSSS*. The policy pushdown containing RLM filters was successful, but RLM processing is currently disabled.

System action: Record Level Monitoring will not be performed.

User response: To perform Record Level Monitoring, issue the **ENABLE RLM** command for subsystem *SSSS*.

AUV1418I PROCESSING OPTION SET - IAM_SMF_RECORD_ID = *nnn*

Explanation: This message is issued during product initialization to display the value *nnn* that is specified for the IAM_SMF_RECORD_ID keyword in the OPTIONS member. This keyword identifies the SMF record ID for the IAM records.

User response: For Guardium S-TAP for VSAM to report IAM access, specify the value *nnn* in the Guardium S-TAP for VSAM CONTROL data set IAM_SMF_RECORD_ID option.

AUV2000E INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING

Explanation: During an attempt to intercept an OPEN/CLOSE event, InfoSphere Guardium S-TAP for VSAM was unable to obtain enough virtual storage to perform processing.

User response: Increase the amount of virtual storage for the job. If the error persists, contact IBM Support.

AUV2030E UNRECOGNIZED INTERCEPT ID ENCOUNTERED (*XX***)**

Explanation: InfoSphere Guardium S-TAP for VSAM received control with unexpected intercept parameters.

User response: This is an unexpected internal condition. If product maintenance was recently applied, ensure that all steps in the HOLDDATA were performed. If they were, record the ID *XX* and contact IBM support.

AUV2040E ERROR OCCURRED DURING SWAREQ PROCESSING FOR JCT, RC=*rrrrrrrr*

Explanation: During interception of an OPEN or CLOSE event, an internal error specified as *rrrrrrrr* occurred while attempting to access a system control block.

User response: Contact IBM Support.

AUV2041E ERROR OCCURRED DURING SWAREQ PROCESSING FOR SCT, RC=*rrrrrrrr*

Explanation: During interception of an OPEN or CLOSE event, an internal error specified as *rrrrrrrr* was encountered while attempting to access a system control block.

User response: Contact IBM Support.

AUV2042E ERROR OCCURRED DURING SWAREQ PROCESSING FOR JMR, RC=*rrrrrrrr*

Explanation: During interception of an OPEN or CLOSE event, an internal error specified as *rrrrrrrr* occurred while attempting to access a system control block.

User response: Contact IBM Support.

AUV2097I JCT UNAVAILABLE FOR JSPB LOOK-UP FOR ASID *xxxx*

Explanation: During interception of an OPEN or CLOSE event, InfoSphere Guardium S-TAP for VSAM was unable to locate a product control block for the address space who's ASID is *xxxx*.

System action: Processing is bypassed for the current job.

User response: Contact IBM support.

AUV2098I ASID *xxxx* **EXCEEDS GJVT MAX; ASVTMAXU=***xxxxxxxx*

Explanation: During interception of an OPEN or CLOSE event, InfoSphere Guardium S-TAP for VSAM detected an unexpected error for the address space with the ASID *xxxx*. The system value for ASVTMAX *xxxxxxxx* is also displayed.

System action: Processing is bypassed for the current job.

User response: Contact IBM support.

AUV2104E ERROR OCCURRED IN FREEMAIN OF AUVSMFX1, RC=*RRRRRRRR*

Explanation: During termination processing of the InfoSphere Guardium S-TAP for VSAM started task or during the DISABLE of the SMFEXIT1 exits, the storage occupied by the module AUVSMFX1 could not be successfully freed. The error code encountered is specified by *RRRRRRRR*.

User response: No noticeable effect on system operations should be noticed as, although the module is located in Extended CSA, it consumes only a few kilobytes of storage. However, the cause of the error should be investigated by contacting IBM Technical support.

AUV2170I ATTEMPTING TO CONNECT TO THE GUARDIUM APPLIANCE

Explanation: This is an informational message issued during product initialization indicating initialization progress.

User response: None required.

AUV2171I CALL TO GUARDIUM APPLIANCE SUCCESSFUL

Explanation: This is an informational message issued during product initialization indicating that the z/OS host component of successfully connected to InfoSphere Guardium appliance.

User response: None required.

AUV2172E *function* **CALL TO GUARDIUM APPLICANCE FAILED**

Explanation: An attempt to communicate with the Guardium appliance failed. Before reporting the failure, the agent retried the request the number of times specified on the RETRY_INTERVAL parameter for the number of iterations specified on the RETRY_COUNT parameter. The *function* will be one of the following:

INIT Appliance initialization, which occurs when the started task initializes.

PING Cyclical pings to the appliance that report the agent's status.

SEND-SMF
Agent transmission of the audit records to the appliance.

If any one of these service requests fail, the agent address space is terminated.

User response: Correct any communications issue causing this failure and restart the agent started task. Contact IBM Support for further assistance.

AUV2173E *function* **CALL TO GUARDIUM S-TAP APPLIANCE FAILED, RC =** *rc* **RC_STP=** *rc* **RS_STP=** *rs* **RC_GDM=** *rc* **RC_PB =** *rc* **RC_LST=** *rc* **RS_LST=** *rs*

Explanation: An attempt to communicate with the Guardium appliance failed. Before reporting the failure, the agent retried the request the number of times specified on the RETRY_INTERVAL parameter for the number of iterations specified on the RETRY_COUNT parameter. The function will be one of the following:

INIT Appliance initialization, which occurs at started task initialization.

PING Cyclical pings to the appliance that reports the agent's status.

SEND-SMF
Agent transmission of the audit records to the appliance. If any one of these service requests fail, the agent address space is terminated.

The *"rc"* and *"rs"* text is replaced with numeric values that can assist IBM Technical Support with problem diagnosis, if the problem persists.

User response: Correct any communications issue causing this failure and restart the agent started task. Contact IBM Support for further assistance.

AUV2174E SPILL FILE FULL, DATA LOSS MIGHT OCCUR

Explanation: Connection to the Guardium appliance has unexpectedly terminated and the spill file with SPILL_BUFFER size is now full. Data loss can occur if this condition continues.

User response: Ensure that the Guardium appliance is communicating. Increase the SPILL_BUFFER value to increase the amount of data that can be written to the spill file.

AUV2175E CONNECTION LOST WITH NO SPILL FILE, DATA LOSS MIGHT OCCUR

Explanation: The connection to the Guardium appliance has unexpectedly terminated. SPILL_BUFFER was not specified in the configuration member.

User response: Ensure that the Guardium appliance is communicating. To minimize data loss, specify a SPILL_BUFFER.

AUV2176E UNABLE TO OBTAIN STORAGE, DATA LOSS MIGHT OCCUR

Explanation: An attempt to allocate storage for additional data failed.

User response: Ensure that a sufficient region size is provided in the started task JCL.

AUV2177E RULEDEF NOT ACTIVATED - CHECK SYSPRINT FOR REASON

Explanation: An attempt to process a policy pushdown failed. No RULEDEF was activated as a result.

User response: Check the SYSPRINT for the detailed reason on what caused the failure. Correct the issue, and reissue a policy pushdown.

AUV2900E INVALID STORAGE REQUEST FOR CONTROL BLOCK *nnnn -ssss*

Explanation: An internal error occurred while attempting to obtain a control block identified by *nnnn* subsystem ID *ssss*.

User response: Contact IBM Support.

AUV2901E INSUFFICIENT VIRTUAL STORAGE FOR CONTROL BLOCK *nnnn -ssss*

Explanation: Sufficient storage was not available to obtain a required control block identified by *nnnn* subsystem ID *ssss*.

User response: Attempt to increase above-the-line or below-the-line storage for the job receiving the error message. If the error persists, contact IBM Support.

AUV2902E ACRONYM CHECK FAILED WHILE ATTEMPTING TO FREE *nnnn*, **DATA=***dddd* **-***ssss*

Explanation: An internal error occurred while attempting to free a control block identified by *nnnn* with the invalid data identified by *dddd* for subsystem ID *ssss*.

User response: Contact IBM Support.

AUV2903E FAILURE OCCURRED DURING FREEMAIN FOR *nnnn* **-***ssss*

Explanation: An internal error occurred while attempting to free a control block identified by *nnnn* subsystem ID *ssss*.

User response: Contact IBM Support.

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 may 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
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
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 information 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 measurements 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. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

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 http://www.ibm.com/legal/copytrade.shtml.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Index

A

AFC2 7
agent 1
auxiliary storage requirements 6

C

commands
  display 15
  operator 15
comments
  methods for providing x
compatibility 13
components
  agent 1
  Guardium system 1
conventions
  highlighting vii

D

data collection
  exclusions 20
  filtering
    filtering stages 18
  SMF event and Record level
    monitoring 18
display commands
  entering 15

F

feedback
  methods for providing x

H

highlighting conventions vii

I

IAM 7
InfoSphere Guardium S-TAP
  introduction 1
initialization requirements 13
installation requirements 3

L

LOAD library
  APF authorizing 5
LookAt ix

M

message retrieval tool
  LookAt ix
messages
  methods for accessing ix
Messages and codes 35
monitoring
  enabling 15

O

OMVS segment definition 6
operator commands
  entering 15

P

Policy pushdown 21

R

Record level monitoring
  best practices and performance 16

S

sample library members 13
security 5
security considerations
  control data set 6
service information vii
SMF data set monitoring
  best practices and performance 16
started task
  communication 15
support information vii
syntax diagrams
  how to read viii

V

VSAM data set types 31

Product Number: 5655-STY

Printed in USA

SC19-4085-01