Version 10 Release 0

IBM Security Guardium S-TAP for Data Sets on z/OS User's Guide

SC27-8021-00

Version 10 Release 0

IBM Security Guardium S-TAP for Data Sets on z/OS User's Guide

SC27-8021-00

Note:
Before using this information and the product it supports, read the "Notices" topic at the end of this information.

Second Edition (April 2017)

This edition applies to Version 10 Release 0 of IBM Security Guardium S-TAP for Data Sets on z/OS (product number 5655-STZ) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this information

IBM® Security Guardium® S-TAP® for Data Sets on z/OS® (also referred to as IBM Guardium S-TAP for Data Sets) collects and correlates data access information from a variety of resources to produce a comprehensive view of business activity for auditors.

These topics provide instructions for installing, configuring, and using IBM Guardium S-TAP for Data Sets to help database administrators, appliance programmers, and application programmers perform these tasks:

- Plan for the installation of IBM Guardium S-TAP for Data Sets
- Install and operate IBM Guardium S-TAP for Data Sets
- Configure the IBM Guardium S-TAP for Data Sets environment
- Diagnose and recover from IBM Guardium S-TAP for Data Sets problems

Always check the Security Guardium Knowledge Center for the most current version of this information:

http://www.ibm.com/support/knowledgecenter/SSMPHH_10.0.0/com.ibm.guardium.doc.zos/z_plugin-gentopic1.html

Chapter 1. IBM Security Guardium S-TAP for Data Sets on z/OS overview

IBM Security Guardium S-TAP for Data Sets on z/OS (also referred to as IBM Guardium S-TAP for Data Sets) collects and correlates data access information from System Management Facilities (SMF) records and realtime system events to produce a comprehensive view of data set access activity for auditors.

IBM Guardium S-TAP for Data Sets enables you to collect many different types of information, including:

- Access to VSAM and non-VSAM data sets and security violations that are recorded by SMF.
- Data set operations that are performed against VSAM data sets, such as delete or rename events, recorded by SMF.
- Access to specific records within VSAM data sets, including key-sequenced data sets (KSDS) or relative record data sets (RRDS), captured as they occur.
- Transaction information that is associated with a VSAM KSDS or RRDS logical record operation, performed within a transaction that runs on the Customer Information Control System (CICS) Transaction Server.
- Access to read and update events for a particular VSAM cluster (consisting of one or more physical data sets) for actions performed on the data set as a whole, or actions performed at the individual level for records within the data set.

What's new in IBM Guardium S-TAP for Data Sets V10.0?

Speed and monitoring enhancements are now provided in V10.0.

Monitoring and reporting of accesses that reside on tape

In addition to the monitoring and reporting of accesses to data sets that reside on disk, you can now use IBM Guardium S-TAP for Data Sets to monitor and generate a report of accesses to data sets that reside on tape.

Multistream load balancing

Enabling multistream mode allows audit events to be collected by multiple Guardium appliances. You can stream data to up to 6 connected Guardium appliances to collect data.

Validating the z/OS MVS SMF environment at start-up

When you start IBM Guardium S-TAP for Data Sets V10.0, the product automatically checks to see if you have the correct components and selected SMF options that are required for data collection.

Reporting of partitioned data sets (PDS) and extended partitioned data set (PDSE) member names

If a PDS or PDSE member is allocated and opened, IBM Guardium S-TAP for Data Sets V10.0 reports the name of that member.

Reporting of non-VSAM exception (EXCP) counts

IBM Guardium S-TAP for Data Sets V10.0 automatically monitors, and generates a report of the EXCP count for non-VSAM data sets.

Reporting of Data Definition Names (DDNAMEs)

IBM Guardium S-TAP for Data Sets V10.0 enables you to filter by DDNAMEs.

IBM Guardium S-TAP for Data Sets components

IBM Guardium S-TAP for Data Sets consists of its data collection agent and the Security Guardium system. The IBM Guardium S-TAP for Data Sets agent collects data set access information that is obtained from the SMF record exit interface, as well as record access information that is obtained from individual I/O requests. The Guardium system is a server-based component that provides the product user interface.

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 types of data to collect. The policy specifies filter information, such as which jobs and data sets to monitor for data accesses.

Guardium system

Use the Guardium system to gather and generate reports on information from multiple agents that are running on multiple z/OS systems. The Guardium system:

- Provides the user interface, which processes your requests and displays the resulting information.
- Enables you to create collection policies, which specify the types of data that are 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 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.

Service updates and support information

Service updates and support information for this product, including software fix packs, PTFs, frequently asked questions (FAQs), technical notes, troubleshooting information, and downloads, are available from the web.

To find service updates and support information, see the following website:

http://www.ibm.com/support/entry/portal/support

Product documentation and updates

DB2® Tools information is available at multiple places on the web. You can receive updates to DB2 Tools information automatically by registering with the IBM My Notifications service.

Information on the web

The DB2 Tools Product Documentation web page provides current product documentation that you can view, print, and download. To locate publications with the most up-to-date information, refer to the following web page:

http://www.ibm.com/software/data/db2imstools/db2tools-library.html

You can also access documentation for many DB2 Tools from IBM Knowledge Center:

http://www.ibm.com/support/knowledgecenter

Search for a specific DB2 Tool product or browse the **Information Management** > **DB2 family**.

IBM Redbooks® publications that cover DB2 Tools are available from the following web page:

http://www.redbooks.ibm.com

The Data Management Tools Solutions website shows how IBM solutions can help IT organizations maximize their investment in DB2 databases while staying ahead of today's top data management challenges:

http://www.ibm.com/software/data/db2imstools/solutions/index.html

Receiving documentation updates automatically

To automatically receive emails that notify you when new technote documents are released, when existing product documentation is updated, and when new product documentation is available, you can register with the IBM My Notifications service. You can customize the service so that you receive information about only those IBM products that you specify.

To register with the My Notifications service:

1. Go to http://www.ibm.com/support/mysupport
2. Enter your IBM ID and password, or create one by clicking **register now**.
3. When the My Notifications page is displayed, click **Subscribe** to select those products that you want to receive information updates about. The DB2 Tools option is located under **Software** > **Information Management**.
4. Click **Continue** to specify the types of updates that you want to receive.
5. Click **Submit** to save your profile.

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 product documentation, use one of the following options:

- Use the online reader comment form, which is located at http://www.ibm.com/software/data/rcf/.
- Send your comments by email to comments@us.ibm.com. Include the name of the book, the part number of the book, the version of the product that you are

using, and, if applicable, the specific location of the text you are commenting on, for example, a page number or table number.

Accessibility features

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use a software product successfully.

The major accessibility features in this product enable users to perform the following activities:

- Use assistive technologies such as screen readers and screen magnifier software. Consult the assistive technology documentation for specific information when using it to access z/OS interfaces.
- Customize display attributes such as color, contrast, and font size.
- Operate specific or equivalent features by using only the keyboard. Refer to the following publications for information about accessing ISPF interfaces:
  - *z/OS ISPF User's Guide, Volume 1*
  - *z/OS TSO/E Primer*
  - *z/OS TSO/E User's Guide*

  These guides describe how to use the ISPF interface, including the use of keyboard shortcuts or function keys (PF keys), include the default settings for the PF keys, and explain how to modify their functions.

Chapter 2. Installation requirements for IBM Guardium S-TAP for Data Sets V10.0

Review the software and authorization prerequisites for installing IBM Guardium S-TAP for Data Sets V10.0.

Software prerequisites

IBM Guardium S-TAP for Data Sets requires z/OS Version 1 Release 13 or later, until end of service.

To access transaction information that is collected from the Customer Information Control System (CICS) transaction server, IBM Guardium S-TAP for Data Sets requires IBM CICS Transaction Server for z/OS V3 Release 1 or later, until end of service.

User ID authority requirements

To install the product, you must have the necessary z/OS user ID authorities.

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 you choose to enable CICS support, you must also have the authority to:

- Update CICS parameters.
- Add CICS program definitions.
- Update or create CICS system initialization and termination program list tables for startup and shutdown.

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

Chapter 3. Configuring the IBM Guardium S-TAP for Data Sets agent

You must configure the IBM Guardium S-TAP for Data Sets agent.

Configuration overview

To configure the product, complete the required steps.

- "Security": Review and establish the security requirements. 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.
- Review the required resource authorizations information, including:
  - "APF authorizing the load library" on page 8
  - "Authorizing the z/OS agent started task for the control data set" on page 8
  - "Defining an OMVS segment" on page 8
- "Planning your configuration" on page 8: Review the steps that are required to plan your configuration.
- "Job cards for the sample JCL in the sample library" on page 9: Provide valid job cards.
- "Allocating auxiliary storage" on page 9: Ensure that data will not be lost in the event of an overflow.
- "Configuring the SMFPRMxx parameter library member" on page 9: Ensure a complete audit by configuring the SMFPRMxx parameter library to collect the required SMF record types.
- "IAM and ACF2 collection considerations" on page 10: Review information about capturing IAM data set activity and ACF2 access failures.
- "Creating the control data set" on page 11: Generate the initial partitioned data set members.
- "Specifying subsystem options" on page 11: Review the subsystem changes that you can make to the options member in the control data set.
- "Configuring the started task JCL" on page 16: Determine the location of the started task control job language (JCL), and follow configuration steps and tips.
- "CICS Transaction Server support" on page 18: Review the requirements for enabling the CICS Transaction Server, and follow the instructions for "Configuring CICS Transaction Server support" on page 18.

Security

IBM Guardium S-TAP for Data Sets 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 IBM Guardium S-TAP for Data Sets 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, as described in the following sections.

Security products can include various software tools that are currently available, such as IBM Resource Access Control Facility (RACF®), Computer Associates International Top Secret, and Computer Associates International Access Control Facility (ACF2).

APF authorizing the load library

IBM Guardium S-TAP for Data Sets requires certain data sets to be accessible and APF authorized on the system on which the agent started task will run. SMF data will be collected by the agent.

The product data set SAUVLOAD, which contains the product load modules that are required for operation, must be APF authorized on the system on which IBM Guardium S-TAP for Data Sets will be run.

Refer to the z/OS MVS Programming Authorized Assembler Services Guide for guidelines and instructions for 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. IBM Guardium S-TAP for Data Sets uses a control data set that is defined in the agent started task.

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

Defining an OMVS segment

You must define an OMVS segment to your security product 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 about 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.

Before configuration, you must determine:

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

Job cards for the sample JCL in the sample library

Some JCL members that are included with the product sample library, SAUVSAMP, 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 that is allocated to the local page data sets. It is used as temporary backup storage for programs and data located in virtual and physical memory. IBM Guardium S-TAP for Data Sets can allocate auxiliary storage space if the **OUTAGE_SPILLAREA_SIZE** parameter is set in accordance with the following requirements.

- The **OUTAGE_SPILLAREA_SIZE** parameter option instructs the address space to allocate a data space equal in size to the value that you set for **OUTAGE_SPILLAREA_SIZE**.
- Verify that the current local page space can accommodate a new data space.

Example

Specifying **OUTAGE_SPILLAREA_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 about 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 IBM Guardium S-TAP for Data Sets.

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

The defaults used at the system level for those subsystems that are not explicitly defined should also specify collection of the required SMF record types. The required SMF record types are 14, 15, 17, 18, 30, 42, 60, 61, 62, 64, 65, 66, and 80. If any required SMF record types are not defined for collection, message AUV1450W alerts you to define them.

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 47
SMF records are correlated to IBM Guardium S-TAP for Data Sets contexts, as shown in the following table.

IAM and ACF2 collection considerations

IBM Guardium S-TAP for Data Sets can capture IAM data set activity and ACF2 access failures. Learn how to enable IBM Guardium S-TAP for Data Sets 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.

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. Because 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).

For IAM data sets, IBM Guardium S-TAP for Data Sets does not report the following items:

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

The CLOSE record counters will report IAM data sets differently from 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

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.

Enabling Innovations Data Processing IAM reporting

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

Procedure

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

Enabling Computer Associates International ACF2 reporting

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

Procedure

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

Creating the control data set

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

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 IBM Guardium S-TAP for Data Sets 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.V10R0 with the high-level qualifier of the installed IBM Guardium S-TAP for Data Sets 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 **`APPLIANCE_SERVER`** and **`AUDIT`** 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) is 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 IBM Guardium S-TAP for Data Sets, you must specify a four-character IBM Guardium S-TAP for Data Sets subsystem ID (SUBSYS) to associate with this particular instance of IBM Guardium S-TAP for Data Sets. The SUBSYS identifies the IBM Guardium S-TAP for Data Sets subsystem in messages that are generated by the product.

How to use subsystem options

Use either the *keyword=value* or *keyword(value)* format to specify values for these option members.

Option members and descriptions

The IBM Guardium S-TAP for Data Sets subsystem options are in the OPTIONS member of the IBM Guardium S-TAP for Data Sets 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 IBM Guardium S-TAP for Data Sets performs its functions.

To specify IBM Guardium S-TAP for Data Sets 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. ACF2 records access failures to a unique record ID. Determine the user-specified SMF record ID that is selected for ACF2 and specify that ID in the IBM Guardium S-TAP for Data Sets CONTROL data set **ACF_SMF_RECORD_ID** option if you want the product to report these failures.

ACF2 writes SMF access failure data to a user-defined SMF record ID. Specify a numeric 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.

APPLIANCE_CONNECT_RETRY_COUNT

Specify a numeric value that defines the number of times to retry communicating with the 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 has 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.

APPLIANCE_NETWORK_REQUEST_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.

APPLIANCE_PING_RATE

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

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

APPLIANCE_PORT

Specify a numeric value that defines the TCP/IP port number for communication with the Guardium system by IBM Guardium S-TAP for Data Sets. Use port 16022 for the V10.0 system protocol.

The default value is 16022.

If port 16023 is used, encryption support is required for the connection to the appliance.

Note: Specifying this keyword and parameter designates the port on which the Guardium appliance is listening to the S-TAP. The port is dedicated to the IP address of the appliance. Port 16022 or 16023 can also be in use on z/OS by another application.

Valid values are 16022 and 16023.

APPLIANCE_RETRY_INTERVAL

Specify a numeric value that defines the number of seconds between retries when an error is encountered during an initial attempt to connect to the Guardium system.

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

APPLIANCE_SERVER

Specify the TCP/IP address for the Guardium system with which IBM Guardium S-TAP for Data Sets is to communicate. In multistream processing scenarios, this address specifies the first Guardium appliance that is to be used.

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

Maximum length is 53 characters. There is no default.

APPLIANCE_SERVER_[1-5]

Specify alternative TCP/IP addresses to use for failover recovery processing and multistream Guardium appliance destinations. Up to five alternative TCP/IP addresses are supported.

To specify one or more entries, include this parameter with a numeric suffix from 1 - 5. Provide a unique TCP/IP address for each entry.

The option syntax is as follows:

- APPPLIANCE_SERVER_1=*addr*

or

- APPPLIANCE_SERVER_1(*addr*)

where 1 can be 1, 2, 3, 4, or 5.

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.

Both the **APPLIANCE_SERVER_[1-5]** and **APPLIANCE _SERVER_FAILOVER_[1-5]** parameters can be used to designate servers for multistreaming or failover. Use the **APPLIANCE_SERVER_LIST** parameter to designate how these parameters are used.

Maximum length is 51 characters.

APPLIANCE_SERVER_FAILOVER_[1-5]

Specify alternative TCP/IP addresses to use for failover and recovery processing. The product supports up to five alternative TCP/IP addresses. To specify one or more entries, include this parameter with a numeric suffix from 1 - 5, each time providing a unique TCP/IP address.

The option syntax is as follows:

```
APPPLIANCE_SERVER_FAILOVER_1=addr
```

or
`APPPLIANCE_SERVER_FAILOVER_`*1(addr)*
where *1* can be 1, 2, 3, 4, or 5.

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.

Both the **`APPLIANCE _SERVER_FAILOVER_[1-5]`** and **`APPLIANCE_SERVER_[1-5]`** parameters can be used to designate servers for multistreaming or failover. Use the **`APPLIANCE_SERVER_LIST`** parameter to designate how these parameters are used.

Maximum length is 42 characters.

APPLIANCE_SERVER_LIST(MULTI_STREAM|FAILOVER|HOT_FAILOVER)

Set **`APPLIANCE_SERVER_LIST`** to *MULTI_STREAM* for a Guardium appliance connection to be established for each server that is identified by the **`APPLIANCE_SERVER_n`** or **`APPLIANCE_SERVER_FAILOVER_n`** parameters.

- If a connection is lost, S-TAP audit events continue to transmit over the remaining appliance connection.
- Lost connections are retried at regular intervals that are determined by multiplying the **`APPLIANCE_CONNECT_RETRY_COUNT`** by the **`APPLIANCE_PING_RATE`**.

Set **`APPLIANCE_SERVER_LIST`** to *FAILOVER* for one Guardium appliance connection to be active at a time.

- If the connection to the primary appliance is lost, a failover action occurs, which results in an attempt to connect to the next available server. The next available server is identified by the **`APPLIANCE_SERVER_n`** or **`APPLIANCE_SERVER_FAILOVER_n`** parameter.
- After a failover action occurs, the connection to the primary server is retried at regular intervals that are determined by multiplying the **`APPLIANCE_CONNECT_RETRY_COUNT`** by the **`APPLIANCE_PING_RATE`**.

Set **`APPLIANCE_SERVER_LIST`** to *HOT_FAILOVER* to keep each connected Guardium appliance active via pings. If the primary Guardium appliance (which is set by the **`APPLIANCE_SERVER`** parameter) becomes unavailable and failover occurs, *HOT_FAILOVER* maintains the activity of the primary appliance policy.

With all settings of **`APPLIANCE_SERVER_LIST`**, if all connections fail, and a spill file is specified (parameter **`OUTAGE_SPILLAREA_SIZE`**), events are buffered to the spill file until a connection becomes available. If no spill file is specified, and all connections are lost, data loss occurs.

The default is *FAILOVER*.

AUDIT

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

There is no default.

CICS_SUPPORT

Enabling CICS® Transaction Server support activates additional reporting of CICS-specific information on record level events, including:

- VSAM_RLM_CICS_File_ID
- VSAM_RLM_CICS_Function_Code
- VSAM_RLM_CICS_Program_ID

- VSAM_RLM_CICS_Region_ID
- VSAM_RLM_CICS_Terminal_ID
- VSAM_RLM_CICS_Transaction_ID
- VSAM_RLM_CICS_User_ID

Enable or disable CICS support by specifying `ENABLE` or `DISABLE`.

The default is *DISABLE*.

If you enable CICS support, you must also configure CICS for record level monitoring events to be captured for CICS. For more information about CICS support, see "CICS Transaction Server support" on page 18.

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. IAM provides a unique user-specified record ID, which it writes during CLOSE processing. For IBM Guardium S-TAP for Data Sets to report this access, determine the user SMF record ID for IAM, and specify that value in the IBM Guardium S-TAP for Data Sets 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 that are due to timing out while trying to send a large amount of data. Specifying too small a value might 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.

MEGABUFFER_COUNT

Specify the number of IBM Guardium S-TAP for Data Sets audit events that are buffered, prior to the product attempting a TCP/IP send operation.

The megabuffer is flushed when either of two conditions is met:

- At regular intervals, based on the APPLIANCE_PING_RATE
- When the number of audit events that are held in the megabuffer reaches the count that is specified by this parameter

When MULTI_STREAM mode is enabled by parameter **APPLIANCE_SERVER_LIST**, and a megabuffer flush occurs, the audit event data stream is switched to the next available Guardium appliance. The event data stream will switch from appliance to appliance in a round-robin fashion as each megabuffer is sent.

Valid values are 1 - 8192. The default is 200.

OUTAGE_SPILLAREA_SIZE
Specify the size of the spill file to be used when a connection cannot be made.

If the product includes a spill file, and no secondary **APPLIANCE_SERVER_FAILOVER** address is specified, or none of the secondary **APPLIANCE_SERVER_FAILOVER** addresses respond, it writes to the spill file. The spill file is meant for short-term outages only, because when 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.

RLM Specify the initial status of RLM processing by setting the **RLM** parameter to either *ENABLE* or *DISABLE*. *ENABLE* enables record level monitoring. *DISABLE* disables record level monitoring.

The default value is *ENABLE*.

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.

SUBSYS
Choose any four-character alphanumerical subsystem ID to identify this particular instance of IBM Guardium S-TAP for Data Sets. For example, AUV1, AUV2, and so on.

Choose a unique SSID for each agent.

The default subsystem ID is *VTAP*.

Configuring the started task JCL

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

About this task

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

Note: Do not start the started task until you finish configuring IBM Guardium S-TAP for Data Sets. Attempting to start the started task before completing configuration can cause the started task to fail.

Procedure

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

   Tip: Name the IBM Guardium S-TAP for Data Sets started task member AUVSTAPV. This name is easily identifiable with the IBM Guardium S-TAP for Data Sets 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.V10R0 with the high-level qualifier of the installed IBM Guardium S-TAP for Data Sets 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 IBM Guardium S-TAP for Data Sets started task. This DD statement points to the subsystem OPTIONS member of the IBM Guardium S-TAP for Data Sets 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 IBM Guardium S-TAP for Data Sets.
     – By default, the OPTIONS DD statement uses the same data set as the RULEDEFS and RULEDEFB DD statements. If necessary, you can specify a different data set for the OPTIONS DD statement other than that which is used for the DD statements RULEDEFS and RULEDEFB. The OPTIONS member must be present in the data set that is specified for the OPTIONS DD statement.
   - A DD statement with a DDNAME of CONTROL must be in the IBM Guardium S-TAP for Data Sets started task. For example: //CONTROL DD DSN=AUV.V10R0.CONTROL,DISP=SHR. This DD statement points to the IBM Guardium S-TAP for Data Sets 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 CONTROL DD statement. 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 correctly 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.

   Note:

   IBM Guardium S-TAP for Data Sets accommodates the use of multistream and improves support for large policies by providing a default started task JCL region size of 96 megabytes. When multistream is enabled, a buffer is created for each appliance, based on the INTERNAL_BUFFER_SIZE value. (Valid values are 0 - 2047 megabytes. The default value is 8.) The default started task JCL region size of 96 megabytes can accommodate large policies by providing space for up to six connected appliances with a default INTERNAL_BUFFER_SIZE of 8 megabytes and approximately 150,000 values in a policy.

   You might need to increase the started task JCL region size if:
   - the value specified for INTERNAL_BUFFER_SIZE is greater than 8 megabytes
   - an installed policy contains more than 150,000 values

CICS Transaction Server support

IBM Guardium S-TAP for Data Sets CICS Transaction Server support enables you to filter and capture CICS transaction information.

Verify that the agent is running and correctly configured, and the appropriate work area storage is available.

- To capture data on files that are referenced within a transaction, the IBM Guardium S-TAP for Data Sets agent must be running and correctly configured to monitor each system image on which data sets reside.
- CICS support uses the XFCFROUT Global User Exit (GLUE).
- The GLUE acquires an above-the-line work area from the extended CICS dynamic storage area (ECDSA) of approximately 1412 bytes for each active or suspended transaction that performs at least one VSAM file operation. The work area is released at the end of the transaction.

Configuring CICS Transaction Server support

For CICS related information to be captured, you must configure CICS Transaction Server support.

About this task

If you configure CICS Transaction Server support, you can capture CICS transaction information that is associated with record level monitoring of logical record activities that occur within a CICS transaction for KSDS and RRDS data sets.

Procedure

1. Configure the CICS system options.
   a. Specify the **CICS_SUPPORT=ENABLE** option, by using the subsystem options that are located in the OPTIONS member of the control data set.

2. Configure the CICS system initialization and system termination program list tables (PLTs), as shown in the example at the end of this topic.
   a. Enter the program AUVPLTPI after the DFHDELIM PLT entry.
   b. Enter the program AUVPLTPS before the DFHDELIM PLT entry.
   c. After creating or modifying the CICS system initialization and system termination PLTs, you must assemble and link them. For more information about creating a PLT, see the CICS Transaction Server for z/OS Resource Definition Guide.
3. Specify autoinstall in the CICS system initialization parameters to automatically install the AUVPLTPI, AUVPLTPS, and AUVFROUT programs. If you do not specify autoinstall in the CICS system initialization parameters, you must define AUVPLTPI, AUVPLTPS, and AUVFROUT in the CICS system definition file (CSD). To install the program definitions in batch, sample JCL has been provided in member AUVCSDUP of the IBM Guardium S-TAP for Data Sets SAUVSAMP library that can be modified and used for the CICS program DFHCSDUP. Alternatively, the CICS CEDA Resource Definition Online transaction can also be used to perform the install of the program definitions. See the CICS Transaction Server for z/OS Resource Definition Guide for more information about installing resource definitions.
   a. Define the following attributes:
      - LANGUAGE (ASSEMBLER)
      - STATUS (ENABLED)
      - CEDF (NO)
      - DATALOCATION (BELOW)
      - EXECKEY (CICS)
      - EXECUTIONSET (FULLAPI)
      - RELOAD (NO)

      For the load modules to be located, the AUVPLTPI, AUVPLTPS, and AUVFROUT programs must be located in a load library located in the CICS DFHRPL concatenation within the CICS startup JCL.
4. Optional: The CICS facilities that implement RLM support, outside of normal CICS PLT initialization, can be enabled and disabled. To do so, define CICS transactions accordingly by using the batch CICS program **DFHCSDUP** or the CICS CEDA Resource Definition Online transaction.

   To enable the CICS facilities that are used to implement CICS RLM support, the following attributes must be assigned to the transaction:
   - TRANSACTION (*tran*, where *tran* is your chosen transaction ID)
   - PROGRAM (AUVPLTPI)
   - TASKDATAKEY (CICS)
   - TASKDATALOC (ANY)

   To disable the CICS facilities that are used to implement CICS RLM support, the following attributes must be assigned to the transaction:
   - TRANSACTION (*tran*, where *tran* is your chosen transaction ID)
   - PROGRAM (AUVPLTPS)
   - TASKDATAKEY (CICS)
   - TASKDATALOC (ANY)
5. Reference the program initialization and termination PLTs in parameters PLTPI and PLTPSD, as described in the topic, "Using CICS system initialization parameters" on page 20.

Results

If you have configured CICS support, message AUV3004I is displayed during CICS initialization to indicate that the Global User Exit AUVPLTPI XFCFROUT was installed and enabled.

Example

Enter the program AUVPLTPI after the DFHDELIM PLT entry in the CICS system initialization PLT:

```
*
*   CICS PROGRAM LIST TABLE FOR CICS SYSTEM INITIALIZATION
*
         DFHPLT TYPE=INITIAL,SUFFIX=I1
*
*  ENTRIES AHEAD OF DFHDELIM ARE EXECUTED IN FIRST PASS OF PLTPI
*  DURING THE SECOND PHASE OF CICS SYSTEM INITIALIZATION
*
         DFHPLT TYPE=ENTRY,PROGRAM=DFHDELIM
*
*  ENTRIES AFTERF DFHDELIM ARE EXECUTED IN SECOND PASS OF PLTPI
*  DURING THE THIRD PHASE OF CICS SYSTEM INITIALIZATION
*
         DFHPLT TYPE=ENTRY,PROGRAM=AUVPLTPI
*
         DFHPLT TYPE=FINAL
*
         END
```

Enter the program AUVPLTS before the DFHDELIM PLT entry in the CICS system termination PLT:

```
*
*   CICS PROGRAM LIST TABLE FOR CICS SYSTEM TERMINATION
*
         DFHPLT TYPE=INITIAL,SUFFIX=T1
*
*  ENTRIES AHEAD OF DFHDELIM ARE EXECUTED IN FIRST PASS OF PLTPSD
*  DURING THE FIRST PHASE OF CICS SYSTEM TERMINATION
*
        DFHPLT TYPE=ENTRY,PROGRAM=AUVPLTPS
*
        DFHPLT TYPE=ENTRY,PROGRAM=DFHDELIM
*
*  ENTRIES AFTERF DFHDELIM ARE EXECUTED IN SECOND PASS OF PLTSD
*  DURING THE SECOND PHASE OF CICS SYSTEM TERMINATION
*
*
         DFHPLT TYPE=FINAL
*
         END
```

Using CICS system initialization parameters

If you created program initialization and termination program list tables to use with IBM Guardium S-TAP for Data Sets, they must be referenced in the CICS system initialization parameters PLTPI and PLTSD.

- The suffix of the table that was created as the program initialization PLT must be referenced in the PLTPI parameter.
- The suffix of the table that was created as the program termination PLT must be referenced in the PLTSD parameter.

Here is a sample set of system initialization parameters that specifies the PLTPI and PLTSD suffixes:

```
AICONS=YES,
XRF=NO,
AUXTR=OFF,
AUXTRSW=NO,
APPLID=CICSSYSA,
FCT=NO,
    ...
PLTPI=I1,
PLTSD=T1,
    ...
SYSIDNT=SYSA
```

Configuring CICS signon reporting

IBM Guardium S-TAP for Data Sets can identify the CICS signon that was used for a specific file access event. Configure the product to enable the agent to send the CICS signon information to the Guardium system.

About this task

Remember: CICS signon records do not indicate a security failure. They are an indication that the identified user successfully accessed the named file or data set.

By default, IBM Guardium S-TAP for Data Sets reports only the CICS address SAF user ID for data set level events and failed security violations. However, for RACF environments, both CICS and RACF can be configured for the S-TAP agent to report all of the following:

- the CICS signon
- the file or data set name that was accessed
- the access context (ALTER, CONTROL, UPDATE, or READ)

Note:

- Implementation of this facility requires changes to both CICS and RACF. After implementation, the resulting change to SMF type 80 processing results in the SMF80USR field containing the CICS signon for specific file accesses. Consult your CICS and RACF security administrator when considering the implementation of this facility.
- This facility does not report the data set activity, only the security level for the requested access event.
- The following steps are also documented in the *RACF Security Guide*. For more information, see the CICS Transaction Server for z/OS RACF Security Guide.

To implement security for files managed by the CICS file control:

Procedure

1. Specify `RESSEC(YES)` in the CSD resource definition of the transactions that access the files.
2. Using the CICS file names for identification, define the profiles to RACF in the FCICSFCT or HCICSFCT resource classes, or their equivalent if you have a user-defined resource class names.
   a. For example, use the following commands to define files in the FCICSFCT class, and authorize users to read from or write to the files:

```
RDEFINE FCICSFCT (file1, file2, .., filen)
  UACC(NONE) NOTIFY(sys_admin_userid)
PERMIT file1 CLASS(FCICSFCT)
  ID(group1, group2) ACCESS(UPDATE)
PERMIT file2 CLASS(FCICSFCT)
  ID(group1, group2) ACCESS(READ)
```

3. To define files as members of a profile in the CICS file resource group class with an appropriate access list, use the following commands:

   ```
   RDEFINE HCICSFCT (file_groupname)
     UACC(NONE) ADDMEM(filea, fileb, .., filez)
     NOTIFY(sys_admin_userid)
   PERMIT file_groupname
     CLASS(HCICSFCT)
     ID(group_userid) ACCESS(UPDATE)
   ```

4. Specify `SEC=YES` as a CICS system initialization parameter, or `SECPRFX` if you define profiles with a prefix.
5. Specify `XFCT=YES` for the default resource class names of FCICSFCT and HCICSFCT, or XFCT=class_name for user-defined resource class names.

Results

RACF SMF type 80 records contain the CICS user signon in the **SMF80USR** field. The data is reported to the Guardium system records **User ID** field.

Starting the product

Start IBM Guardium S-TAP for Data Sets before 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 IBM Guardium S-TAP for Data Sets. Message AUV1196E will warn you of a product initialization order conflict.

If you receive this error at startup:

1. Shut down IBM Guardium S-TAP for Data Sets and any similar products, including the previous version of this product, IBM Guardium S-TAP for Data Sets.
2. Close any data sets that are open under IBM Guardium S-TAP for Data Sets.
3. Start IBM Guardium S-TAP for Data Sets before starting similar products.

Starting and stopping the agent started task

Follow these steps to start and stop the IBM Guardium S-TAP for Data Sets 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 IBM Guardium S-TAP for Data Sets. The following table lists them by type and description.

Table 1. Sample library members, types, and descriptions

Member	Type	Description
AUVCSDUP	JCL	Sample JCL to create CICS resource definition lists, groups, and program definitions with the CICS DFHCSDUP utility.
AUVJCNTL	JCL	Sample JCL to allocate and initially populate the control data set.
AUVJSTC	JCL	Sample PROC to start the IBM Guardium S-TAP for Data Sets agent address space.
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. IBM Guardium S-TAP for Data Sets administration

You must configure the Guardium system to communicate with the IBM Guardium S-TAP for Data Sets agent.

Communicating with the Guardium system

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

- The IBM Guardium S-TAP for Data Sets TCP/IP connection must be configured.
- At least one agent per z/OS image must be specified. When you are configuring an agent instance:
  - Specify the host name or IP address on which the Guardium system is running. This value is specified by the APPLIANCE_SERVER element 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 Guardium system.

Streaming audit data to multiple systems

Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 Guardium appliances (**APPLIANCE_SERVER** + **APPLIANCE_SERVER_***n*, where *n* can be 1 - 5).

IBM Guardium S-TAP for Data Sets sends events to a single appliance until a ping occurs, or the number of records that is specified by **MEGABUFFER_COUNT** is reached.

To enable multistreaming, you must specify *MULTI_STREAM* when you configure the **APPLIANCE_SERVER_LIST** parameter in the OPTIONS member of the CONTROL data set. Parameters **APPLIANCE_SERVER** and **APPLIANCE_SERVER_[1-5]** specify the appliances to which you intend to stream events. The appliance that is specified by **APPLIANCE_SERVER** provides the policy that is used for event matching.

For more information about OPTIONS member parameters, see “Specifying subsystem options” on page 11.

Keeping connections active when HOT_FAILOVER is enabled

When the *HOT_FAILOVER* feature is enabled by the **APPLIANCE_SERVER_LIST** parameter, each connected Guardium appliance is kept active via pings.

If the primary appliance becomes unavailable and failover occurs, the appliance policy that was originally pushed from the primary appliance continues to be active. When all Guardium appliances are connected, the status of each appliance connection, listed in the Guardium interface, is green.

Communicating with the IBM Guardium S-TAP for Data Sets started task

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

IBM Guardium S-TAP for Data Sets started task commands

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

Commands

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, for 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:

Table 2. Started task commands and descriptions.

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

Data collection

IBM Guardium S-TAP for Data Sets collects data from multiple sources. This section describes the data collection process, as well as filtering stages and their performance impacts.

Record level and SMF event monitoring

Event information is gathered at run time through record level and SMF event monitoring. For both record level and SMF event monitoring, the filtering options you specify can minimize overhead, and control the performance of the data collection and reporting phases of processing. IBM Guardium S-TAP for Data Sets 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 record level and SMF event 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.
- In the user interface, 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 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 record level and SMF event 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 IBM Guardium S-TAP for Data Sets 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 are not specified, data collection cannot be performed. See the *SMF record types collected by IBM Guardium S-TAP for Data Sets* 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 record level and SMF event 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
- Data set type
- DD name
- Job name
- Job type
- Program name
- Security system user ID
- Security system group ID
- SMF system ID
- Subsystem ID
- Sysplex name
- 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 record level monitoring: For record level monitoring, Stage 1 filtering occurs at OPEN time for KSDS and RRDS VSAM data sets.

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

Stage 2 filtering

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

- Data set open
- Data set close
- Data set create
- Data set alter
- Data set update
- Data set delete
- Data set rename
- Data set SAF alter
- Data set SAF control
- Data set SAF define
- Data set SAF read
- Data set SAF update

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

If CICS support is enabled, you can filter the record level monitoring event data that is captured within a CICS transaction. CICS transaction data can be filtered by:

- CICS user ID
- CICS transaction ID
- CICS program ID
- CICS file ID
- CICS system ID
- CICS terminal ID
- CICS function code

Stage 3 filtering

Stage 3 filtering is performed by IBM Guardium S-TAP for Data Sets based on Stage 2 filtering criteria that you define. During policy pushdown and activation, an analysis of the policy filtering criteria is performed. This analysis enables prefiltering processing determinations that can be performed across the product. Stage 3 prefiltering 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:

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

Exclusions

IBM Guardium S-TAP for Data Sets does not collect information on the following types of activities:

On IBM 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 IBM IMS™ subsystems

Accesses performed by the following program names:

- DFSMVRC0
- CQSINIT0
- HWSHWS00
- IRTRRC00
- DFSRRC00
- DFSUARC0
- DSPCINT0
- DSPURI00

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 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 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:

- Data set name
- Data set type
- Job name
- Job type
- Program name
- Security system user ID

- Security system group ID
- SMF system ID
- Subsystem ID
- Sysplex name
- VSAM record organization
- DD name

If CICS support is enabled you can also filter based on:

- CICS user ID
- CICS transaction ID
- CICS program ID
- CICS file ID
- CICS system ID
- CICS terminal ID
- CICS function code

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 by 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 Guardium system. Use the Guardium system interface to establish as restrictive a set of policy filters as possible. IBM Guardium S-TAP for Data Sets 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.
- Record level monitoring is only valid for use with VSAM data sets (KSDS and RRDS only).

SMF data set monitoring performance and filtering

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

Filter down to each specific VSAM data set event 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 SAF Alter
- Data Set SAF Update
- Data Set SAF Read
- Data Set SAF Define
- Data Set SAF Control

Filter down to each specific non-VSAM data set event with the following filters:

- Data Set Close
- Data Set Delete
- Data Set Rename
- Data Set Create
- Data Set SAF Alter
- Data Set SAF Update
- Data Set SAF Read
- Data Set SAF Define
- Data Set SAF Control

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.

Policy pushdown

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

Evaluating a match

When the product is searching for a match for the filtering criteria that 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
- Data set name
- Data set type
- DD name
- User ID
- Group ID
- SYSPLEX
- SSID
- SYS ID
- RECORG*
- Job type

*RECORG is valid only for the processing of VSAM record level monitoring.

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

- Key
- Key range
- Data set event
- RLM event
- CICS user ID
- CICS transaction ID
- CICS program ID
- CICS file ID
- CICS system ID
- CICS terminal ID
- CICS function code

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 that is 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 are matched.

Data set collection filtering parameters

Use the following filtering parameters to collect data set event data.

All the fields are optional and most have a default behavior as described. All fields apply to both VSAM and non-VSAM monitoring, unless otherwise specified.

Rule Type

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

Allowed values are: INCLUDE|EXCLUDE: Include collects events that satisfy the specified criteria; 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.

If nothing is specified, all types are collected. You can specify 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

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 that occur on SS01

SS01,EQ
Matches that occur on SS01

SS%,EQ
Matches that occur on systems with SS as the first 2 characters in the SMF system ID

RECORG
Indicates the record organization type to match.

Applies only to VSAM record level monitoring 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 record level monitoring 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 that are caused by user *PDUSER01*

PDUSER01,EQ
Matches events that are caused by user *PDUSER01*

PDUSER%,EQ
Matches events that are 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 that are accessed from IDCAMS

IDCAMS,EQ
Matches events that are accessed from IDCAMS

IDCAM%,EQ
Matches events that are accessed from programs 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 that are caused by someone within GROUP1

GROUP1,EQ
Matches events that are caused by someone within GROUP1

GROUP%,EQ
Matches events that are 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 that represents the data set name for which activity is 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, 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

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

1 - 8 character DD 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 for all DD names are considered a match.

Examples:

PAYFILE
Matches events that are accessed by DD name *PAYFILE*

PAYFILE,EQ
Matches events that are accessed by DD name *PAYFILE*

PAYFIL%,EQ
Matches events that are accessed by DD names beginning with *PAYFIL*

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

1 - 8 character name representing the job for which activity must be collected, 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 jobs are considered a match.

Examples:

AUVJOB01
Matches events that result from a job name AUVJOB01

AUVJOB01,EQ
Matches events that result from a job name AUVJOB01

AUVJOB%,EQ
Matches events that result from any job beginning with AUVJOB

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

Only applies to VSAM record level monitoring collection.

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

Multiple keys must 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 1 - 255 characters long.

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

An individual key must be surrounded in double quotation marks ("").

If the key is in hexadecimal format, it must be prefixed with x' and suffixed with a single quotation mark ('). It must 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 supplied with a hexadecimal key, the wildcard must 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 record level monitoring events with a key of KEY01

`"KEY01","KEY02"`
Matches record level monitoring events with a key of KEY01 or KEY02

`"x'F0F0'"`
Matches record level monitoring events with a key that contains the hexadecimal value F0F0

`"x'F0F0'","x'F0F1'"`
Matches record level monitoring events with a key that contains the hexadecimal value of F0F0 or F0F1

`"KEY01","x'F0F1'"`
Matches record level monitoring events with a key of KEY01 or a key with the hexadecimal value of F0F1

"KEY0%"
: Matches record level monitoring events with a key beginning with KEY0.

"x'F06C'"
: Matches record level monitoring events with a key with a hexadecimal value beginning with F0

"\x'F06C'"
: Matches record level monitoring events with a key of x'F06C'

Key Range

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

Only applies to VSAM record level monitoring collection.

A pair of keys in plain text, or a pair of keys in hexadecimal, representing the range to match for record level monitoring. This must 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 2 - 510 characters long and must have an even number of characters.

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

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

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

All key pairs must have the smaller key in the first value and the larger key in the second value; otherwise the key pairs 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 record level monitoring events where the key is between KEY01 and KEY09

"KEY01","KEY09","KEY11","KEY19"
: Matches record level monitoring events where the key is between KEY01 and KEY09 or between KEY11 and KEY19

"x'F0F0'","x'F0F9'"
: Matches record level monitoring events where the key has a hexadecimal value between F0F0 and F0F9

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

"\x'F0F0'","\x'F0F9'"

Matches record level monitoring 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.

Only applies to VSAM record level monitoring collection.

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 that is 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 record level monitoring events where the operation was a record insert

RINS,RDEL

Matches record level monitoring 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.

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

DSRDF
A security facility DEFINE 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 must 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.

Data Set Type
Indicates the type of data sets that should be considered for a match.

Must contain zero or one of the following values:

VSAM|NONVSAM|ALL, where:

VSAM
VSAM data sets

NONVSAM
Non-VSAM data sets

All Both VSAM and non-VSAM data sets

If nothing is specified, then only VSAM data set types are collected.

CICS collection filtering parameters

Use the following filtering parameters to collect transaction data from CICS.

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

1 - 8 character CICS logon user ID to match

The user ID can be followed by a comma (,) and a relational operator. If no relational operator is specified, then EQ is assumed.

Wildcards are supported.

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

Examples:

CICUSR01
Matches events that are caused by CICS logon user CICUSR01

CICUSR01,EQ
Matches events that are caused by CICS logon user CICUSR01

CICUSR%,EQ
Matches events that are caused by CICS logon users with the prefix CICUSR

CICS Transaction ID
Indicates the CICS transaction ID to use when searching for a match

1 - 4 character CICS transaction ID to match

The transaction ID can be 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 CICS transaction IDs are considered a match.

Examples:

VTAP Matches events that occur within CICS transaction ID VTAP

VTAP,EQ
Matches events that occur within CICS transaction ID VTAP

VT%,EQ
Matches events that occur within CICS transaction IDs starting with the prefix VT

CICS Terminal ID
Indicates the CICS terminal ID to use when searching for a match

1 - 4 character CICS terminal ID to match

The terminal ID 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 CICS terminal IDs are considered a match.

Examples

VTAP Matches events that occur within CICS transaction ID VTAP

VTAP,EQ
Matches events that occur within CICS transaction ID VTAP

VT%,EQ
Matches events that occur within CICS transaction IDs starting with the prefix VT

CICS Region ID
Indicates the CICS region ID to use when searching for a match. The Region ID is defined in the CICS Transaction Server System Initialization Table parameter SYSIDNT.

1 - 4 character CICS region ID to match

The region ID can be 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 CICS region IDs are considered a match.

Examples:

CICA Matches events that occur within the CICS region with an ID of CICA

CICA,EQ
Matches events that occur within the CICS region with an ID of CICA

CIC%,EQ
Matches events that occur within the CICS regions with a prefix of CIC

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

1 - 8 character CICS program name to match.

The program name can be 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 CICS program names are considered a match.

Examples:

PAYROLLA
Matches events that occur under control of the program that is named PAYROLLA

PAYROLLA,EQ
Matches events that occur under control of the program that is named PAYROLLA

PAYROLL%,EQ
Matches events that occur under control of program names that are prefixed with PAYROLL

CICS File ID
Indicates the CICS file ID to use when searching for a match.

1 - 8 character CICS file ID to match.

The file ID can be 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 CICS file IDs are considered a match.

Examples:

HRKSDS01
Matches events that occur for CICS file ID HRKSDS01

HRKSDS01,EQ
Matches events that occur for CICS file ID HRKSDS01

HRKSDS%,EQ
Matches events that occur for CICS file IDs prefixed with HRKSDS

CICS Function Code
Indicates the CICS function code to use when searching for a match. The function code is defined in the CICS Transaction Server Customization Guide. Search for “File control domain exits, XFCFRIN and XFCFROUT.” See the description for the XFCFROUT parameter UEP_FC_FUNCTION. The hex values for the UEP_FC_FUNCTION symbolic names are defined in the DFHUEXIT macro in the CICS SDFHMAC macro library.

Two hex characters represent the single character CICS function code.

The function code can be followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.

Wildcards are not supported.

If left blank, then all CICS function codes are considered a match.

Examples

01 Matches events that occur with the CICS function code defined by the hex character 01

01,EQ Matches events that occur with the CICS function code defined by the hex character 01

Chapter 5. Reference information

This section provides IBM Guardium S-TAP for Data Sets reference information.

VSAM and non-VSAM data set types and events

IBM Guardium S-TAP for Data Sets agent performs data set and record level monitoring for VSAM and non-VSAM data sets. The data set types, as well as the type of events that IBM Guardium S-TAP for Data Sets collects, are described here.

Data set level monitoring

The IBM Guardium S-TAP for Data Sets agent collects SMF data for the following data set organizations:

VSAM

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

Non-VSAM

PS Physical sequential

PO Partitioned organization

DA Direct access

PDSE Partitioned organization-extended

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.

VSAM

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

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

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

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

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

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

Security facility DEFINE violation
A security facility DEFINE violation of a supported data set type

Security facility READ violation
A security facility READ violation of a supported data set type

Security facility UPDATE violation
A security facility UPDATE violation of a supported data set type

Security facility ALTER violation
A security facility ALTER violation of a supported data set type

Security facility CONTROL violation
A security facility CONTROL violation of a supported data set type

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

Non-VSAM

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

For non-SMS data sets, a RENAME event also produces a DATA SET CREATE context record, in addition to a DATA SET RENAME context record.

DATA SET CLOSE
A CLOSE 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

Security facility DEFINE violation
A security facility DEFINE violation of a supported data set type

Security facility READ violation
A security facility READ violation of a supported data set type

Security facility UPDATE violation
A security facility UPDATE violation of a supported data set type

Security facility ALTER violation
A security facility ALTER violation of a supported data set type

Security facility CONTROL violation
A security facility CONTROL violation of a supported data set type

For partitioned organization data sets (PDS and PDSE), member additions, updates, and deletions are reported by z/OS as updates to the base data set. IBM Guardium S-TAP for Data Sets reports member additions, updates, and deletions as CLOSE events with an access of OUTPUT.

Record level monitoring

The IBM Guardium S-TAP for Data Sets 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 IBM Guardium S-TAP for Data Sets contexts, as shown in the following table.

Table 3. SMF record types, subtypes, and contexts

Record number	Record subtype	Purpose	SMF context
14		Collecting non-VSAM file activity	CLOSE (non-VSAM input)
15		Collecting non-VSAM file activity	CLOSE (non-VSAM output)
17		Collecting Delete activity	DELETE (non-VSAM)
18		Collecting Rename activity	RENAME (non-VSAM)
30	4, 5	Collecting Job/Step activity	Accounting
42	6	Collecting VSAM type information	Accounting (VSAM)
60		Collecting VVDS update activity	Data Set ALTER, Data Set CREATE
61		Collecting DEFINE/CATLG activity	Data Set CREATE
62		Collecting VSAM file activity	OPEN (VSAM)
64		Collecting VSAM I/O statistics	CLOSE (VSAM)
65		Collecting Delete activity	DELETE (VSAM)
66*		Collecting Rename activity	RENAME, ALTER (VSAM)
80		Collecting CICS sign-on security violations	Security Violation

*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 as they occur.
- Data Set CREATE context can appear for RENAME requests of non-SMS, non-VSAM data sets, because the RENAME process generates an SMF type 61 record.

Related reference:

"Configuring the SMFPRMxx parameter library member" on page 9
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 IBM Guardium S-TAP for Data Sets.

Time-to-reporting considerations

Learn about the benefits, considerations, and exceptions that apply to the time-to-reporting feature.

IBM Guardium S-TAP for Data Sets provides faster real-time reporting for data set level events. When possible, the S-TAP agent immediately delivers data set level information to the Guardium system. The agent presents the data as it occurs, giving you up-to-the-minute results without waiting for jobs to end or SMF type 30 records to be generated.

Benefits

Immediate reporting
No need to wait for a CICS address space to terminate, or a TSO user logs off.

Reduced storage usage
The agent immediately reports data set events to the Guardium system, which substantially reduces the agent storage requirement. The data set event record is complete and ready for transmission to the Guardium system as soon as z/OS MVS creates the source SMF record.

Considerations

Additional event records
A notable difference as a result of this enhancement is the appearance of data set event records that were not identified in previous versions of this product. Collecting the data set event records in preparation for the SMF type 30 record caused seemingly similar records to merge. For example, a Close event could be reported for a KSDS event, although z/OS DFSMSdfp actually records this as two separate events (one for the Cluster Data component, and one for the Cluster Index component). Improved time-to-reporting now more accurately reflects data set events.

Events Span Data Set Types
With this feature, and the V10.0 addition of non-VSAM reporting, data set event records might span data set types. For example, when you delete a VSAM KSDS event, z/OS DFSMSdfp deletes a VSAM and a non-VSAM collection of components. Use the DS_TYPE policy filter to adjust this reporting.

Exceptions

To avoid waiting for the SMF type 30 record, the agent scans various z/OS system control blocks in the address space when z/OS is writing the data set SMF record. There are instances when these control blocks are unavailable because of the state of the address space. Before this scan is run, the agent assesses the state of the address space for compatibility. If the address space is not in a compatible state, the agent waits for the SMF type 30 record, which delays reporting of the event until the address space has terminated.

Chapter 6. Troubleshooting

Use these topics to diagnose and correct problems that you might experience with IBM Guardium S-TAP for Data Sets.

Messages and codes

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

Error message code descriptions

Security Guardium S-TAP for Data Sets error messages adhere to the following format: AUV*nnnx*

Where:

AUV Indicates that the message was issued by Security Guardium S-TAP for Data Sets.

nnn Indicates the message identification number.

x Indicates the severity of the message:

Table 4. 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.

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 Software 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 Software 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 Software 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 Software 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 Software 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 Software 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 required.

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 required.

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.

AUV1022E INVALID KEYWORD/DELIMITER - ***pppppppp***

Explanation: During product installation, while processing the subsystem options in the OPTIONS member, an invalid keyword or delimiter was encountered. The value *pppppppp* indicates the associated keyword.

User response: Correct the specified option keyword or delimiter 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 - SUBSYS=*ssss*

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

User response: No action is required.

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

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the SUBSYS 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 – APPLIANCE_PING_RATE=*nnnnn*

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

User response: No action is required.

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

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the APPLIANCE_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 – APPLIANCE_RETRY_INTERVAL=*nnnnn*

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

User response: No action is required.

AUV1033E VALUE SPECIFIED FOR OPTION – APPLIANCE_RETRY_INTERVAL=*nnnnn*

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the APPLIANCE_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: Contact IBM Software 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: Contact IBM Software 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 Software 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 Software 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 Software 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 Software 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 Software 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 Software Support.

AUV1048I PROCESSING OPTION SET: APPLIANCE_CONNECT_RETRY_COUNT

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

User response: No action is required.

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

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the APPLIANCE_CONNECT_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 *NNNNNNNNNNNNNNNN* **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 *NNNNNNNNNNNNNNNN*. 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 Software Support.

AUV1052E UNABLE TO DELETE *NNNNNNNNNNNNNNNN* **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 *NNNNNNNNNNNNNNNN*. The return code encountered is specified by *RRRRRRRR* and the reason code is specified by *SSSSSSSS*.

User response: Contact IBM Software Support.

AUV1054E GSSB IS NOT PRESENT

Explanation: During activation of a policy RULEDEFS member, a necessary Security Guardium S-TAP for Data Sets control block could not be located.

User response: Ensure that the Security Guardium S-TAP for Data Sets started task has been successfully started. If no error was encountered during the initialization of the started task, contact IBM Software Support.

AUV1055E GSSB CONTROL BLOCK ID IS INVALID

Explanation: During activation of a policy RULEDEFS member, a necessary Security Guardium S-TAP for Data Sets control block was located but it is not valid.

User response: Ensure that the Security Guardium S-TAP for Data Sets started task has been successfully started. If no error was encountered during the initialization of the started task, contact IBM Software Support.

AUV1056I PROCESSING OPTION SET – APPLIANCE_NETWORK_REQUEST_TIMEOUT=*nnnnn*

Explanation: This message is issued during product initialization to display the value (*nnnnn*) that is specified for the

APPLIANCE_NETWORK_REQUEST_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 Software Support.

AUV1058I PROCESSING OPTION SET – APPLIANCE_SERVER=*a**

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

User response: No action is required.

AUV1059E INVALID VALUE SPECIFIED FOR OPTION - APPLIANCE_SERVER=*a**

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

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

AUV1060I PROCESSING OPTION SET – AUDIT=*a**

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

User response: No action is required.

AUV1061E VALUE SPECIFIED FOR OPTION – AUDIT=*a**

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

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

AUV1062I PROCESSING OPTION SET – CICS_SUPPORT=*nnnnnnn*

Explanation: This message is issued during product initialization to display the value *nnnnnnn* that was specified for the CICS_SUPPORT keyword in the OPTIONS member.

User response: No action is required.

AUV1063E INVALID VALUE SPECIFIED FOR OPTION – CICS_SUPPORT=*nnnnnnn*

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

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

AUV1064W Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.

Explanation: The `APPLIANCE_PORT` parameter currently supports a setting of 16022 or 16023. If `APPLIANCE_PORT` is specified with a value other than 16022 or 16023, message AUV1064W is issued and port 16022 is used instead.

User response: Change the `APPLIANCE_PORT` parameter setting to one of the supported values, or remove the parameter.

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 Software 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 Software 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 Software 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 Software 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 Software 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 Software 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 Software 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 Software Support.

AUV1100E ACRONYM CHECK FAILED FOR GSSB

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

User response: Contact IBM Software 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 Software Support.

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

Explanation: During initialization of the Security Guardium S-TAP for Data Sets 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 Security Guardium S-TAP for Data Sets. If the STEPLIB appears to correctly contain all of the product load modules, contact IBM Software Support.

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

Explanation: During initialization of the Security Guardium S-TAP for Data Sets 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 Security Guardium S-TAP for Data Sets. If the STEPLIB appears to correctly contain all of the product load modules, contact IBM Software 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 Software Support if the 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 Software 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 Software 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 Software 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 Security Guardium S-TAP for Data Sets 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 action 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 action 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 Software 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 Software 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 Software 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 Software 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: No action is required.

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: No action is required.

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 Software 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 memory dump is taken. Depending upon the particular intercept, product initialization might continue or terminate.

User response: Contact IBM Software 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 Software 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 Software 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 Security Guardium S-TAP for Data Sets started task and restart. If the problem persists, contact IBM Software 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 Security Guardium S-TAP for Data Sets started task. If the problem persists, contact IBM Software Support.

AUV1213E ERROR RETRIEVING SSRE

Explanation: An internal error was encountered.

User response: Contact IBM Software Support.

AUV1214E UNEXPECTED SSRE QUEUE ERROR

Explanation: An internal error was encountered.

User response: Contact IBM Software Support.

AUV1215E UNEXPECTED SSRE QUEUE ERROR

Explanation: An internal error was encountered.

User response: Contact IBM Software Support.

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

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

User response: No action is required.

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

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

User response: No action is required.

AUV1402I CURRENT POLICY *EEE* -*SSSS*

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

User response: No action is required.

AUV1405I RECORD LEVEL MONITORING SUCCESSFULLY ENABLED -*SSSS*

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

User response: No action 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 Security Guardium S-TAP for Data Sets operator command **ENABLE RLM** for subsystem *SSSS*. The enable action was successful, but no filters specifying record level monitoring processing exist in the currently activated policy.

System action: Record level monitoring will not be performed.

User response: To perform record level monitoring, add record level monitoring 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 Security Guardium S-TAP for Data Sets operator command **ENABLE RLM** for subsystem SSSS. The policy activation containing record level monitoring filters was successful, but record level monitoring 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 is 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 - OUTAGE_SPILLAREA_SIZE=*nnnnnnn*

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

User response: No action is required.

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

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the OUTAGE_SPILLAREA_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 is 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 - APPLIANCE_SERVER_FAILOVER=a*

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

User response: No action is required.

AUV1417E INVALID VALUE SPECIFIED FOR OPTION - *keyword*=a*

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the keyword. The *keyword* value indicates APPLIANCE_SERVER_FAILOVER_*n*, or its alternate specification, APPLIANCE_SERVER_*n*, where *n* is 1, 2, 3, 4, or 5. The value *a** indicates the invalid value.

User response: Correct the specified option keyword and restart.

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 Security Guardium S-TAP for Data Sets to report IAM access, specify the value *nnn* in the control data set IAM_SMF_RECORD_ID option.

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 Security Guardium S-TAP for Data Sets to report access failures to a unique record ID, specify the value *nnn* in the 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.

AUV1422I PROCESSING OPTION SET - APPLIANCE_SERVER_LIST(*nnn*)

Explanation: This message is issued during product initialization to display the value specified for the APPLIANCE_SERVER_LIST keyword in the OPTIONS member. This value *nnn* identifies one of the following selected options:

FAILOVER
One appliance connection is active at a time. If the connection to the primary appliance is lost, a failover action occurs, which results in an attempt to connect to the next available server. The appliance attempts to reconnect to the primary server at intervals of 12 times the `PING_RATE`.

MULTI_STREAM
An appliance connection is established for each server that is listed by the `APPLIANCE_SERVER_n` or `APPLIANCE_SERVER_FAILOVER_`n parameter.

When a connection is lost, Security Guardium S-TAP for Data Sets audit events continue to be spread over the remaining appliance connections. Any lost connections are retried at regular intervals of 12 times the `PING_RATE`.

HOT_FAILOVER
Keeps each connected Guardium appliance active via pings. If the primary Guardium appliance becomes unavailable and failover occurs, *HOT_FAILOVER* maintains the activity of the primary appliance policy.

User response: No action is required.

AUV1423E INVALID VALUE SPECIFIED FOR OPTION - APPLIANCE_SERVER_LIST(*nnn*)

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

User response: Correct the specified option keyword and restart.

AUV1424I PROCESSING OPTION SET - MEGABUFFER_COUNT =*nnnnnnn*

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

User response: No action is required.

AUV1425E INVALID VALUE SPECIFIED FOR OPTION MEGABUFFER_COUNT =*nnnnnnn*

Explanation: During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the `MEGABUFFER_COUNT` option. The value *nnnnnnn* indicates the incorrect 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 Security Guardium S-TAP for Data Sets operator command `DISPLAY SMFEXIT1` for subsystem *SSSS*. The value *EEEEEEEE* indicates *ENABLED* or *DISABLED*.

User response: No action is required.

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

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

User response: No action is required.

AUV1450W SMF RECORDING TEST FAILED, RC=*cc*, TYPE=*nnn*, SUBSYSTEM=*ssss*

Explanation: The Security Guardium S-TAP for Data Sets address space issues this message if it detects an inadequacy in the SMF environment. During initialization,Security Guardium S-TAP for Data Sets tests z/OS MVS SMF to determine if SMF is collecting the record types that are necessary for data set level auditing. The S-TAP address space issues this message for each SMF record type *nnnn*, and z/OS MVS subsystem *ssss*, for which the test fails. RC *cc* identifies one of the following return codes:

16 SMF is not active or has ended abnormally.

36 Information for the specified record type is not being recorded.

User response: To audit data set level events, configure z/OS MVS SMF to collect the required SMF records. Refer to the *Configuring the SMFPRMxx parameter library member* topic for more information.

AUV1747E SUBSYSTEM IS NOT ACTIVE OR ENABLED

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

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

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

Explanation: This message is issued in response to the Security Guardium S-TAP for Data Sets policy pushdown operation for subsystem *SSSS*. The policy pushdown containing record level monitoring filters was successful, but record level monitoring 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*.

AUV2000E INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING

Explanation: During an attempt to intercept an OPEN/CLOSE event, Security Guardium S-TAP for Data Sets 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 Software Support.

AUV2030E UNRECOGNIZED INTERCEPT ID ENCOUNTERED (*XX*)

Explanation: Security Guardium S-TAP for Data Sets 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 Software 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 Software 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 Software 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 Software Support.

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

Explanation: During interception of an OPEN or CLOSE event, Security Guardium S-TAP for Data Sets was unable to locate a product control block for the address space with the ASID *xxxx*.

System action: Processing is bypassed for the current job.

User response: Contact IBM Software Support.

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

Explanation: During interception of an OPEN or CLOSE event, Security Guardium S-TAP for Data Sets 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 Software Support.

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

Explanation: During termination processing of the Security Guardium S-TAP for Data Sets 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 Software 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 Guardium system.

User response: No action is required.

AUV2172E *function* **CALL TO GUARDIUM APPLIANCE FAILED**

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

INIT Guardium system initialization, which occurs when the started task starts.

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

SEND-SMF
Agent transmission of the audit records to the Guardium system.

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 Software Support for further assistance.

AUV2173E *function* **CALL TO GUARDIUM 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 system failed. Before reporting the failure, the agent retried the request the number of times specified on the APPLIANCE_RETRY_INTERVAL parameter for the number of iterations specified on the APPLIANCE_CONNECT_RETRY_COUNT parameter. The function will be one of the following:

INIT Guardium system initialization, which occurs at started task initialization.

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

SEND-SMF
Agent transmission of the audit records to the Guardium system. 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 Software 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 Software Support for further assistance.

AUV2174E SPILL FILE FULL, DATA LOSS MIGHT OCCUR

Explanation: Connection to the Guardium system 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 system 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 system has unexpectedly terminated. SPILL_BUFFER was not specified in the configuration member.

User response: Determine the cause of the network interruption and correct the problem so that the connection can be re-established. 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.

AUV2178I SPILL FILE IS *xx*% **FULL**

Explanation: This message is issued while the spill file is in use. It indicates that the spill file has been filled to the percentage indicated.

User response: No action is required.

AUV2179E UNABLE TO OBTAIN REQUESTED STORAGE FOR INTERNAL_BUFFER_SIZE: dddd. PROCESSING CONTINUES.

Explanation: An attempt to allocate storage for the internal buffer has failed. The started task remains up, but data processing does not run as efficiently.

User response: Ensure that a sufficient region size is provided in the started task JCL, or decrease the amount specified for INTERNAL_BUFFER_SIZE in the OPTIONS member. If the problem persists, contact IBM Software Support.

AUV2180W WRITING TO SPILL FILE

Explanation: The connection to the Guardium system has been lost. All data is now being written to a spill file. The data in the spill file will be written to the Guardium system when the connection is restored.

User response: Determine the cause of the network interruption and correct the problem so that the connection can be re-established.

AUV2181I NO LONGER WRITING TO SPILL FILE

Explanation: The connection to the Guardium system has been restored, and the agent is no longer writing to the spill file.

User response: No action is required.

AUV2182I CONNECTION ESTABLISHED TO *x*

Explanation: An attempt to connect to the Guardium system was successful, where *x* is the system with which a connection has been made.

User response: No action is required.

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 Software 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 Software 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 Software 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 Software Support.

AUV3000E ERROR ENABLING AUVFROUT: EIBRCODE=*NNNNNNNNNNNN*

Explanation: While running the Program List Table Program Initialization module AUVPLTPI, an error was encountered attempting to enable the XFCFROUT Global User Exit program AUVFROUT. The value *NNNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response: Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, "Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.

AUV3001E ERROR OBTAINING GWA ADDR: EIBRCODE=*NNNNNNNNNNNN*

Explanation: While running the Program List Table Program Initialization module AUVPLTPI, an error was encountered regarding an attempt to obtain the address of the Global Work area. The value *NNNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response: Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, "Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.

AUV3003E ERROR STARTING AUVFROUT: EIBRCODE=*NNNNNNNNNNNN*

Explanation: While running the Program List Table Program Initialization module AUVPLTPI, an error was encountered regarding an attempt to start the XFCFROUT Global User Exit AUVFROUT. The value *NNNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response: Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, "Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.

AUV3004I AUVPLTPI XFCFROUT GLOBAL USER EXIT SUCCESSFULLY ENABLED AND STARTED

Explanation: While running the Program List Table Program Initialization module AUVPLTPI, the XFCFROUT Global User Exit AUVFROUT was successfully enabled and started.

User response: No action is required.

AUV3005E ERROR STOPPING AUVFROUT: EIBRCODE=*NNNNNNNNNNNN*

Explanation: While running the Program List Table Program Termination module AUVPLTPS, an error was encountered regarding an attempt to stop the XFCFROUT Global User Exit AUVFROUT. The value *NNNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response: Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, "Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.

AUV3006E ERROR OBTAINING GWA ADDR: EIBRCODE=*NNNNNNNNNNNN*

Explanation: While running the Program List Table Program Termination module AUVPLTPS, an error was encountered regarding an attempt to obtain the address of the Global Work area. The value *NNNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response: Interpret the error codes using the documentation that is provided in the CICS Transaction Server System Programming Reference manual, Appendix B. EXEC interface block (EIB) response and function codes. Contact IBM Software Support if you are unable to determine the cause of the problem.

AUV3008E ERROR DISABLING AUVFROUT: EIBRCODE=*NNNNNNNNNNNN*

Explanation: While running the Program List Table Program Termination module AUVPLTPS, an error was encountered regarding an attempt to disable the XFCFROUT Global User Exit AUVFROUT. The value *NNNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response: Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, "Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.

AUV3009I AUVPLTPS XFCFROUT GLOBAL USER EXIT SUCCESSFULLY STOPPED AND DISABLED

Explanation: While running the Program List Table Program Termination module AUVPLTPS, the XFCFROUT Global User Exit AUVFROUT was successfully stopped and disabled.

User response: No action is required.

AUV3010W CICS PLTPI INSTALLED BUT CICS_SUPPORT NOT SPECIFIED IN OPTIONS

Explanation: The CICS Support Program List Table Program Initialization program AUVPLTPI was defined to CICS, but the CICS_SUPPORT parameter was not enabled in the OPTIONS start-up parameters for the Security Guardium S-TAP for Data Sets started task.

User response: To use full CICS support within the product, you must specify CICS_SUPPORT=ENABLE in the OPTIONS parameters defined to the started task. Make the necessary changes to the OPTIONS parameters and restart the product.

Notices

This information was developed for products and services offered in the U.S.A.

This material may be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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.

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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US.

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.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered marks 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.

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

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions:

Applicability: These terms and conditions are in addition to any terms of use for the IBM website.

Personal use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights: Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM

Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Index

Product Number: 5655-STZ

Printed in USA

SC27-8021-00