Version 10 Release 1.3

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

SC27-8022

Note:

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

March 2020 Edition

This edition applies to Version 10 Release 1.3 of IBM® Security Guardium® S-TAP® for IMS on z/OS® (product number 5655-ST9) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this information..... vii

Chapter 1. What does IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 do?..... 1
What's new in IBM Security Guardium S-TAP for IMS on z/OS V10.1.3?..... 1
IBM Guardium S-TAP for IMS components..... 2
IBM Guardium system..... 2
IBM Guardium S-TAP for IMS agent..... 2
Service updates and support information..... 3
Product documentation and updates..... 3
Accessibility features..... 4

Chapter 2. Installing IBM Security Guardium S-TAP for IMS on z/OS..... 5
Hardware and software prerequisites..... 5
User ID authorities that are required for installation..... 5

Chapter 3. IBM Security Guardium S-TAP for IMS on z/OS security..... 7
APF authorization..... 7
OMVS segment..... 7
TCP/IP connections..... 7
z/OS log streams..... 8
IMS RESLIB data sets..... 8
SMF and IMS archive log data sets..... 8
DBRC RECON data sets..... 8
Operator commands..... 9
Quarantining Database DLI calls..... 9

Chapter 4. Configuration overview..... 11
Upgrading from Guardium S-TAP for IMS V9.0..... 11
Upgrading from Guardium S-TAP for IMS V9.1 or V10.0..... 12
Planning your configuration and customizing your environment..... 12
Customizing the ISPF edit macro..... 13
Job cards for the sample JCL in the SAMPLIB..... 13
Setting up z/OS log streams..... 14

Chapter 5. Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent... 19
Customizing the agent configuration files..... 19
Agent configuration..... 33
Customizing the agent JCL..... 33
Starting and stopping the agent..... 34
Agent security considerations..... 34
Modifying the frequency of AUIJ012I messages..... 34

Chapter 6. Setting up an IMS environment for auditing..... 35
Security consideration for IMS processing..... 35
Customizing IMS environments to capture DLI calls..... 35
Customizing IMS cataloged procedures..... 35
Coexisting with other DFSFLGX0 and DFSISVI0 Exit routines..... 35
Defining LOGWRT exits..... 37

Customizing IMS to use a System z Integrated Information Processor (ZzIIP)....37
Copying common load modules from SAUILOAD to SAUIIMOD....37
Configuring APP_EVENT support....38
APP_EVENT examples....38

Chapter 7. Using agent configuration keywords....41
Simulation mode....42
Specifying multiple SMF data set masks....43
Disabling SMF auditing at the agent level....43
Controlling the frequency of SMF z/OS catalog queries....43
Changing the retention period of incomplete SMF events....43
Changing the name of the SMF address space JCL....44
Auditing IMS data set access....44
Changing the types of events that are audited using SMF records....44
Using alternate RECON data sets for SMF and SLDS processing....45
Overriding the range of ports used for communication between address space....45
Overriding the TCP/IP DNS resolver table....46
Specifying agent messages to issue to the operator console....47
Creating a spill area for short-term outages....47
Disabling IMS SLDS auditing at the agent level....48
Controlling the frequency with which IMS System Log Data Sets are allocated and read....48
Changing the name of the IMSL address space JCL....48
Changing the types of events audited using IMS SLDS records....48
Changing the name of the Common Memory Management address space JCL....49
Excluding DLI calls on specific LPARS from being audited....49
Running more than one agent in a SYSPLEX....49
Restricting auditing to specific IMS systems when multiple IMS systems share RECON data sets....50
Using the System z Integrated Information Processor (zIIP)....50
Using multiple Guardium systems....51
Providing Guardium system failover....51
Streaming to multiple Guardium systems....52
Keeping connections active when HOT_FAILOVER is enabled....53

Chapter 8. IBM Security Guardium S-TAP for IMS on z/OS agent reference information....55
Sample library members....55
Agent environment....56
APF authorization....56
Agent job output....56
Stopping the agent....56
Starting and stopping the secondary address spaces....57

Chapter 9. Data collection....59
IMS database DLI calls....59
SMF records....59
Records from IMS system log data sets (SLDS)....60
Filtering stages....61
Stage 0 filtering....61
Stage 1 filtering....61
Stage 2 filtering....62
Policy pushdown....62

Chapter 10. Creating and modifying IMS definitions....63
Navigating to the IMS Definitions panel....63
IMS Definition fields....63
IMSPLEX data sharing and XRF considerations....64
Adding an IMS definition....65

Modifying an IMS definition....65
Deleting an IMS definition....65

Chapter 11. Reference information....67
Data collection monitors....67
IMS Logtypes and SMF record types that are collected by InfoSphere Guardium S-TAP for IMS....69
Fields that are used for IMS policy pushdown....70
Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS....72
Calculating the Optimal Log Stream Size....72
Considerations....73
Using IBM Documentation....73
Pertinent Report Fields....74
Additional Resources....74
XML statement definitions....74
Sample XML file....78
AUIA060W....79

Chapter 12. Troubleshooting....81
Messages and codes for 81
Error messages and codes: AUIAxxxx....81
Error messages and codes: AUIBxxxx....85
Error messages and codes: AUIFxxxx....86
Error messages and codes: AUIGxxxx....87
Error messages and codes: AUIIxxxx....90
Error messages and codes: AUIJxxxx....95
Error messages and codes: AUILxxxx....105
Error messages and codes: AUIPxxxx....106
Error messages and codes: AUIRxxxx....108
Error messages and codes: AUITxxxx....108
Error messages and codes: AUIUxxxx....110
Error messages and codes: AUIXxxxx....111
Error messages and codes: AUIYxxxx....120
Error messages and codes: AUIZxxxx....121

Notices....129
Trademarks....130
Terms and conditions for product documentation....130
Privacy policy considerations....131

Index....133

About this information

IBM Security Guardium S-TAP for IMS on z/OS (also referred to as IBM Guardium S-TAP for IMS) collects and correlates data access information from a variety of IMS 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 IMS to help database administrators, system programmers, and application programmers perform these tasks:

- Plan for the installation of IBM Guardium S-TAP for IMS
- Install and operate IBM Guardium S-TAP for IMS
- Customize your IBM Guardium S-TAP for IMS environment
- Diagnose and recover from IBM Guardium S-TAP for IMS problems
- Design and write applications for IBM Guardium S-TAP for IMS
- Use IBM Guardium S-TAP for IMS with other Db2® or IMS products

Tip: To find the most current version of this information, always use the Security Guardium Knowledge Center: https://www.ibm.com/support/knowledgecenter/SSMPHH_10.1.0/com.ibm.guardium.doc.zos/z_plugin-gentopic1.html

Chapter 1. What does IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 do?

IBM Security Guardium S-TAP for IMS on z/OS (also referred to as IBM Guardium S-TAP for IMS) is an auditing tool that collects and correlates data access information from IMS Online regions, IMS batch jobs, IMS archived log data sets, and SMF records to produce a comprehensive view of business activity that occurs within one or more IMS environments.

IBM Guardium S-TAP for IMS assists auditors in determining who read or updated a particular IMS database and its associated data sets, what mechanism was used to perform that action, and when the access took place.

IBM Guardium S-TAP for IMS can collect and correlate many different types of information, including:

- Accesses to databases and segments from IMS Online regions.
- Accesses to databases and segments from IMS DLI/DBB batch jobs.
- Accesses to databases, image copies, IMS logs, and RECON data sets and security violations to these data sets as recorded by SMF.
- IMS Online region START and STOP, database, and PSB change of state activity and user signon and signoff as recorded in the IMS Archived Log data sets.

Restriction: IBM Guardium S-TAP for IMS supports auditing of Data Entry Databases (DEDBs) and IMS Full Function databases. Auditing of Main Storage Databases (MSDBs) is not supported.

What's new in IBM Security Guardium S-TAP for IMS on z/OS V10.1.3?

Here's what's new in version 10.1.3 of IBM Guardium S-TAP for IMS.

Enhancements to this version include:

- Echoing of active policy XML as described in “Echoed XML statement definitions” on page 74.
- Increased security of online and batch log streams as described in “z/OS log streams” on page 8.
- Filtering of DLI called based on IMS LTERM names
- Collection of the accessed HALDB PARTITION name during DLI call processing
- Check agent status without accessing z/OS by using a Guardium interface command
- Ability to enable simulation mode to simulate mainframe activity levels, test deployment, and gauge appliance requirements without sending data to the Guardium appliance
- New parameters to simplify audit record validation, debugging, and agent configuration
- Simplified agent configuration:
  - Complete SMF configuration is no longer required if the **`SMF_CYCLE_INTERVAL(0)`** parameter is specified in the AUICONFG file and SMF processing is disabled.
  - Complete IMSL configuration is no longer required if the **`IMSL_CYCLE_INTERVAL(0)`** parameter is specified in the AUICONFG file and IMSL processing is disabled.
- Messages AUII050I and AUIJ250I now include the IMSID to help identify which IMS system issued the message.
- Reduced CPU consumption and greater reliability during processing of IMS DLI calls in IMS online environments.
- RECON data sets that are read by the SMF (AUIF*STC* and IMS SLDS (AUIL*STC*) can optionally be copies of the live IMS RECON data sets.
- Option to disable DLI call auditing of IMS online DLI calls that originate from the following IMS region types: AER, BMP, CICS®, DBCTL, IFP, MPP, and ODBA.

- Support for Internet Protocol version 6 (IPV6) introduced with PH16991

IBM Guardium S-TAP for IMS components

IBM Guardium S-TAP for IMS consists of an agent, a Common Storage Management Utility, and the IBM Guardium system.

IBM Guardium system

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

Note: In environments where multiple agents connect to a common IBM Guardium system or appliance, the z/OS agent started task names (AUIA*STC*, AUIL*STC*, AUIF*STC*) must be unique. Unique started task names enable the IBM Guardium S-TAP for IMS policies that are pushed from the IBM Guardium system to be attributed to, and monitored by, the correct z/OS agent.

IBM Guardium system components

The IBM Guardium system:

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

IBM Guardium system and S-TAP agent communication

The IBM Guardium system and the IBM Guardium S-TAP for IMS agent communicate using a TCP/IP connection. The policies you create, using the user interface, tell the agent what data to collect. The policy specifies filter information, such as which data sets are to be monitored for data accesses.

IBM Guardium S-TAP for IMS agent

The IBM Guardium S-TAP for IMS agent coordinates the collection of audited data, and the transmission of audited DLI call data to the IBM Guardium system.

The IBM Guardium S-TAP for IMS agent can collect data from one or more of the following sources within a SYSPLEX:

- A single IMS system
- Multiple IMS systems that share a common set of RECON data sets
- Multiple IMS systems using diverse RECON data sets

The agent maintains the communication links that are needed to exchange information with:

- The IBM Guardium system
- IMS Online and Batch data collectors and activity monitors
- The IMS Archive Log data set and SMF activity monitors

The agent also provides data collection schemas, called policies, to the activity monitors on which detail the IMS artifacts are to be audited, and to what level.

The agent runs as a started task on the z/OS host. An example of the JCL to be used is in member AUIASTC of the SAUISAMP installation data set.

The agent collects data from the following sources:

- IMS online activities
- IMS batch activities
- SMF data

- IMS archived log data
- IMS RECON data sets

For more information about how data is collected from these sources, see "Data collection monitors" on page 67.

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/Overview/Software/Information_Management/IMS_Tools

Product documentation and updates

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

Information on the web

The IMS 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/imstools-library.html

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

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

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

IBM Redbooks® publications that cover IMS 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 IMS 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 IMS 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 helps IBM to provide quality information. Send any comments that you have about this book or other IMS Tools documentation to comments@us.ibm.com. Include the name and version number of the product and the title and number of the book. If you are commenting on specific text, provide the location of the text (for example, a chapter, topic, or section title).

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. Installing IBM Security Guardium S-TAP for IMS on z/OS

The following sections describe hardware, software, and user ID authority prerequisites for product installation.

Review the IBM Guardium S-TAP for IMS V10.1.3 Program Directory for a list of product materials and SMP/E installation instructions.

Hardware and software prerequisites

The following hardware and software are required to operate IBM Guardium S-TAP for IMS V10.1.3.

- z/OS Version 2 Release 2 or later, until end of service.
- IMS V13 -- V15, until end of service.
- Any hardware capable of running z/OS Version 2 Release 1 or later, until end of service.

IBM Guardium S-TAP for IMS requires use of the following:

- 64-bit memory
- TCP/IP connectivity
- z/OS System logger log streams
- UNIX System Services
- OMVS segment

User ID authorities that are required for installation

The following z/OS USERID authorities are needed to install IBM Guardium S-TAP for IMS.

If you are installing this product, your z/OS user ID must have the authority to:

- Define z/OS system log streams
- Update the IMS cataloged procedure data set members DLIBATCH and DBBBATCH to include product load libraries

Chapter 3. IBM Security Guardium S-TAP for IMS on z/OS security

IBM Guardium S-TAP for IMS requires access to various IMS data sets and IBM Guardium system components.

APF authorization

IBM Guardium S-TAP for IMS requires certain data sets to be accessible and APF-authorized on all LPARS of the SYSPLEX where IMS batch jobs or monitored IMS online regions might run.

About this task

Refer to the *z/OS Knowledge Center* for more information about how to APF authorize libraries.

Procedure

1. APF-authorize product data set SAUILOAD on all LPARS of the SYSPLEX.
   SAUILOAD contains the IMS Online and Batch Activity Monitor executable code.
2. APF-authorize product data set SAUIIMOD on all LPARS of the SYSPLEX where IMS batch jobs or IMS online regions to be monitored might run.
   SAUIIMOD contains IMS specific executable load modules.

OMVS segment

TCP/IP connectivity and other UNIX System services on z/OS require that the address space that is using these services use a z/OS user ID or group name that is defined with an OMVS segment.

Defining your z/OS user ID or group name with an OMVS segment might require the use of the IBM RACF command **`ADDUSER/ALTUSER xxxxxx OMVS(UID(zzz))`** or a security product equivalent command. Review your z/OS Security Server documentation for more information.

TCP/IP connections

IBM Guardium S-TAP for IMS uses Transmission Control Protocol/Internet Protocol (TCP/IP) to connect to the Guardium appliance. To enable this communication, make sure you have the correct permissions assigned.

If you are working from a secure communications port, enable the user ID that is associated with the agent started task to have READ/WRITE permissions on the ports that are assigned to the agent.

See Chapter 7, “Using agent configuration keywords to customize auditing,” on page 41 for more information about the **`ADS_LISTENER_PORT`**, **`APPLIANCE_PORT`**, and **`LOG_PRT_SCAN_START`** configuration keywords.

z/OS log streams

IBM Guardium S-TAP for IMS monitors the IMS batch jobs and online regions and writes audit data to z/OS log streams.

The IBM Guardium S-TAP for IMS Online and DLI/DBB batch data collectors audit DLI events that occur in the IMS Online and DLI/DBB Batch regions. Audited DLI events are written to z/OS System Logger log streams, which are then read by the IBM Guardium S-TAP for IMS agent. The IMS agent sends the audit data to the IBM Guardium appliance by using TCP/IP connections.

To permit the IMS Online and DLI/DBB batch collectors to write to the log streams, systems authorization facility (SAF) security access of UPDATE to the z/OS log stream is required for all user IDs associated with the audited IMS Control region and DLI/DBB batch jobs that might cause IMS DLI calls to be audited.

You can now use an additional SAF resource to further secure the online and batch log streams. For example, you can now prevent the log streams from being read by a user program or utility that is initiated by a user who is authorized to update to the log stream. Apply z/OS V2R3 and V2R4 APAR OA56050 to optionally add an additional authority check for a SAF profile that covers resource (WRITE_ONLY_log-stream-name) in class LOGSTRM. This new profile option enables you to limit users to only connecting to (IXGCONN REQUEST=CONNECT), writing to (IXGWRITE), and disconnecting from (IXGCONN REQUEST=DISCONNECT) the log stream. Other IXG calls, such as IXGBRWSE (read), are rejected with return code 8 and reason code '081C'x. For more information, refer to the documentation provided in the HOLD data for APAR OA56050.

Note: User IDs that are associated with the IBM Guardium S-TAP for IMS agent must have authority to read and delete data from the log stream and should not be limited by using resource (WRITE_ONLY_log-stream-name). Log stream UPDATE authority is recommended for the IBM Guardium S-TAP for IMS agents.

IMS RESLIB data sets

READ access to the IMS RESLIB/SDFSRESL data sets is required for each IMS system that requires the IMS SLDS to be processed by IBM Guardium S-TAP for IMS. READ access is required to allow a LOAD/READ of module DFSVC000 to determine the version release level of the audited IMS.

SMF and IMS archive log data sets

READ access to the SMF data sets and the IMS archived logs data sets (SLDS) is required for the user under whose authority the agent runs. If these data sets are protected by RACF® or another security product, a policy must be defined to grant this access. The z/OS catalogs containing the names of these data sets, as well as the physical data sets themselves, must be accessible from the LPAR on which the IBM Guardium S-TAP for IMS agent runs.

Consult your security administrator to determine what is currently protected and how to grant the required access.

DBRC RECON data sets

IBM Guardium S-TAP for IMS uses the native VSAM services to read data from the RECON data sets. These RECON data sets must be accessible from all the LPARS where the IBM Guardium S-TAP for IMS agents might run.

VSAM access to the RECON data sets is READ-ONLY, allowing the IBM Guardium S-TAP for IMS jobs and started tasks with a security access of READ to process the RECON data sets.

Consult your security administrator to determine how your RECON data sets are protected, and how to grant the required access.

Operator commands

You can use z/OS Operator commands, to start IBM Guardium S-TAP for IMS tasks.

The user ID that is assigned to the IBM Guardium S-TAP for IMS agent started task must be permitted to issue **START** commands to initiate the AUIF*stc*, AUIL*stc*, and AUIU*stc* tasks. During installation, administrators can configure the z/OS security product to restrict users and programs from issuing z/OS Operator commands.

Quarantining Database DLI calls

IBM Guardium S-TAP for IMS enables you to quarantine the DB DLI calls of specific users for specific periods of time.

Quarantining a user of a specific IMS subsystem means that for the specified time period, the quarantined user is not able to run DB DLI calls either by using the targeted IMS subsystem, or while running DLI/DBB batch jobs.

If a quarantined user attempts access during a restricted time, the DLI call is not performed, and a status code of AI is returned in the DBPCB status code field.

To create quarantine rules, access the **Policy Builder** from the **Tools and Views** section of the Guardium appliance interface **Setup** menu.

Note:

- DLI calls that are made to IMS Fast Path databases by using IMS Fast Path exclusive transactions or BMPs cannot be quarantined.
- Quarantine does not take effect immediately. The audited DLI call that produces the event to trigger the quarantine is completed before the quarantine takes effect. It is possible for DLI calls to be run by the quarantined user before the quarantine takes effect.

Chapter 4. Configuration overview

These actions are required to configure IBM Guardium S-TAP for IMS.

Review the following steps, which are described in greater detail in the following sections:

- Verify that you have the resource authorizations that are required to configure the product.
- Review the steps to plan your configuration and customize your environment.
- Set up the z/OS log streams. Review the CFRM and log stream size requirements, and the related security considerations, limitations, and restrictions. Define the log streams for batch and online jobs.
- Determine a naming convention for the agent (AUIA*STC*, AUIF*STC*, AUIL*STC*, and AUIU*STC*) started tasks, where *STC* can be changed to any 1 - 4 character length string.

  Tip: Retain the AUI prefix to simplify task identification.
- Configure the agent by customizing the configuration file, customizing the agent JCL, and starting the agent.
- Set up the IMS environment for auditing by customizing the IMS cataloged procedure, configuring IMS exits, customizing IMS to use an IBM System z® Integrated Information Processor (zIIP), and review the related security considerations.

Note: No WLM (Workload Manager) considerations are necessary. All agent started tasks use the STC WLM class.

Upgrading from Guardium S-TAP for IMS V9.0

Complete the following steps to upgrade from InfoSphere® Guardium S-TAP for IMS V9.0 to IBM Guardium S-TAP for IMS V10.1.3. These steps enable V9.0 product assets, such as JCLs and configuration and repository contents, to be upgraded to V10.1.3, while allowing the full use and functionality of the V10.1.3 product.

Before you begin

New versions or releases of IBM Guardium S-TAP for IMS should be installed as a new installation base. However, if circumstances prevent you from doing so, follow these instructions to upgrade from the previous version's installation base.

Procedure

1. Deactivate or uninstall all policies that apply to the agent that you are upgrading.
2. Shut down the agent that you are upgrading.
3. Customize the AUIMIG10 SAMPLIB member to convert the configuration file and repository to V10.1.3 format, and submit.

   The comments that are contained in the AUIMIG10 SAMPLIB member describe how to customize the JCL. A V10.1.3 format configuration file, and an IMS definition report will be produced.
4. Use the IMS definition report, which is produced by the AUIMIG10 utility, to add the IMS definitions to your IBM Guardium system.
5. Update the new configuration file, which is produced by the AUIMIG10 utility, with any changes.
6. Update the AGENT (AUIA*STC*) and Memory Management Utility (AUIU*STC*) JCLs as follows:
   a) Remove the //AUICFG DD JCL statement.
   b) Add a //AUICONFG DD JCL statement, and set it to reference the new configuration member produced by the AUIMIG10 utility.
   c) Change the //STEPLIB DD JCL statement to reference the V10.1.3 product load library (SAUILOAD).

d) Remove the //AUIREPOS DD JCL statement from the AUIU*STC* JCL.

7. Update the SMF (AUIF*STC*) and IMS Archive Log (AUIL*STC*) JCLs as follows:
   a) Remove the //AUICFG DD JCL statement, and any procedure parameters that reference it.
   b) Change the //STEPLIB DD JCL statement to reference the V10.1.3 product load library (SAUILOAD).
8. Update the IMS Control region JCLs that are audited by the agent to use the V10.1.3 product IMS load library (SAUIIMOD).
9. Update the IMS DBBBATCH and DLIBATCH cataloged procedures, and any equivalent JCL members, to use the V10.1.3 product IMS load library (SAUIIMOD).
10. Start the agent.
11. Install or activate the policies that you want to apply.
12. Stop and restart your IMS systems.

What to do next
Now, you can:

- Install additional policies on the z/OS host by using the IBM Guardium system user interface.
- Manage agent and IMS definitions by using the IBM Guardium system user interface.

Note: The format of the data that is written to the z/OS logstreams has changed from V9.0 to V10.1.3. IBM Guardium S-TAP for IMS V10.1.3 converts any existing V9.0 data from existing logstreams to a usable format. If you migrate from a V10.1.3 system back to a V9.0 system, you must reinitialize the z/OS log streams before restarting InfoSphere Guardium S-TAP for IMS V9.0.

Upgrading from Guardium S-TAP for IMS V9.1 or V10.0

The agent JCL and configuration file that are used by IBM Guardium S-TAP for IMS V9.1 and V10.0 are compatible with IBM Guardium S-TAP for IMS V10.1.3. No configuration changes are required to upgrade from IBM Guardium S-TAP for IMS V9.1 to IBM Guardium S-TAP for IMS V10.1.3.

Before you begin
Do not attempt to run AUIMIG10 to upgrade from Guardium S-TAP for IMS V9.1 or V10.0 to IBM Guardium S-TAP for IMS V10.1.3.

About this task
The format of the data that is written to the z/OS logstreams has changed in V10.1.3. IBM Guardium S-TAP for IMS V10.1.3 converts any existing Guardium S-TAP for IMS V9.1 and V10.0 data from existing logstreams to a usable format. If you migrate from a V10.1.3 system back to a V9.1 or V10.0 system, you must reinitialize the z/OS log streams before restarting the previous product version.

Planning your configuration and customizing your environment

Collect user ID and environment information before you configure IBM Guardium S-TAP for IMS V10.1.3.

Tip: To upgrade to IBM Guardium S-TAP for IMS from a previous version, refer to the appropriate topic:

- “Upgrading from Guardium S-TAP for IMS V9.0” on page 11
- “Upgrading from Guardium S-TAP for IMS V9.1 or V10.0” on page 12

If you are upgrading from a previous version to V10.1.3, no further configuration steps are required. Upgrading to V10.1.3 requires the use of, and modifications to, the same agent name and JCLs that were used with previous versions. For your reference, see the “Sample library members” on page 55 table.

Before you configure a new installation of IBM Guardium S-TAP for IMS V10.1.3, determine the following:

- The user IDs that will be used to run the agent started tasks

- Where the agent started tasks will run

Then, customize the ISPF edit macro, review the job card requirement, and set up the z/OS log streams, as described in the following sections.

Customizing the ISPF edit macro

The SAUISAMP data set shipped with IBM Guardium S-TAP for IMS includes an ISPF edit macro to help with the editing of the rest of the SAMPLIB members to be used in the subsequent steps.

About this task

The edit macro is named AUIEMAC1 and provides a straightforward way to customize the variable values for the variables that appear in the JCL that will run. Use this edit macro as part of a command list (CLIST) to edit the other SAMPLIB members.

Procedure

1. To set up the edit macro, copy AUIEMAC1 from the #HLQ.SAUISAMP to a CLIST library.
2. Edit the macro by providing the appropriate values for each of the variables.
3. To run the macro, type the name of the edit macro in the command line in ISPF.

Results

After you modify the edit macro, you can use it as a command to customize other SAMPLIB members in the following steps, unless otherwise specified.

Example

The contents of the edit macro AUIEMAC1 included in the SAMPLIB are as follows:

```
ISREDIT MACRO (NP)
ISPEXEC VGET (ZUSER)
ISREDIT CHANGE ALL '#AUILOAD'        AUI.IBMTAPE.SAUILOAD
ISREDIT CHANGE ALL '#AUIIMOD'        AUI.IBMTAPE.SAUIIMOD
ISREDIT CHANGE ALL '#AUISAMP'        AUI.IBMTAPE.SAUISAMP
ISREDIT CHANGE ALL '#AUICONFG'        AUICONFG
```

This table describes each variable in the edit macro AUIEMAC1 included in the SAMPLIB:

Table 1. AUIEMAC1 Edit macro variables

Variable	Default	Instructions
#AUILOAD	AUI.IBMTAPE. SAUILOAD	Change the default value to point to the location of the SAUILOAD for IBM Guardium S-TAP for IMS.
#AUIIMOD	AUI.IBMTAPE. SAUIIMOD	Change the default value to point to the location of the SAUIIMOD for IBM Guardium S-TAP for IMS.
#AUISAMP	AUI.IBMTAPE. SAUISAMP	Change the default value to point to the location of the SAUISAMP data set, or copy of that data set where you will be performing the configuration and customization edits.
#AUICONFG	AUICONFG	Change the default value to point to the member name in the configuration file that you want to use.

Job cards for the sample JCL in the SAMPLIB

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

A valid job card conforming to your site's JCL standards must be provided before submitting any of the JCL.

Setting up z/OS log streams

IBM Guardium S-TAP for IMS uses the z/OS System Logger to funnel events from IMS online regions and DLI/DBB batch jobs to the DLI event processor (AUIA*STC* task). Both XCF based and DASD based log streams are supported.

Each agent requires two unique log streams:

- one log stream for DLI events generated by IMS Control regions
- one log stream for DLI events generated by DLI/DBB batch jobs

Log streams cannot be shared between agents. Each log stream name must be unique.

It is recommended that XCF based log streams be used whenever possible, because this type of log stream is accessible from any LPAR within a sysplex, and has performance benefits. For more information about log streams, refer to the IBM publication: *System Programmer's Guide to: z/OS System Logger*.

Log stream security

Verify the following conditions have been met to insure log stream security.

Important:

- The USERID your IMS online control region runs under must have WRITE access to the log stream.
- If DLI/DBB batch jobs runs under a common USERID, that USERID must have WRITE permission to the log stream.
- The USERID under which the DLI Event Collector (AUIA*STC* task) executes must have READ/WRITE access to the log streams.
- If individual users are permitted to run DLI/DBB batch jobs under their own USERID, a universal access of WRITE is recommended for the log stream.

XCF-based log streams

The advantages of using XCF-based log streams, as opposed to DASD-based log streams, include accessibility from any LPAR within the sysplex, and improved performance.

AUILSTR1

Two JCL members in the SAUISAMP product data set are included to assist in the definition of XCF-based log streams.

This JCL is used to define the XCF structures to a CFRM policy needed by the log streams used by the DLI/DBB batch and IMS online control regions. Detailed instructions are in the comments of the JCL.

Note: The addition of structures to a CFRM policy are cumulative, and the execution of this JCL without consideration to previously defined structures within the CFRM policy result in the loss of existing CFRM structure definitions. It is highly recommended that a systems programmer customize and submit this JCL.

There are two DEFINE STRUCTURE sections for this JCL: one for the batch structure, and one for the online structure. The following values must be customized for the batch structure:

The name of the batch structure
(NAME(batch_struc_name))

The coupling facility used to contain the structure
(PREFLIST(cfname))

The following values must be customized for the online structure:

The name of the online structure
(NAME(online_struc_name))

The coupling facility used to contain the structure
(PREFLIST(cfname))

Do not change any other values, such as SIZE, INITSIZE, and ALLOWAUTOALT without carefully considering the impact that your changes will have on performance and data integrity.

Note:

- AUILSTR1 must run successfully before proceeding.
- When auditing in a large test or production environment, the **INITSIZE** and **SIZE** parameters can be increased to a higher value (example: 49200) for improved throughput.

AUILSTR2

This JCL is used to add the XCF based log streams to a LOGR policy used by the IMS Control region and DLI/DBB batch jobs. Detailed instructions are in the comments of the JCL.

Note: The addition of structures to a CFRM policy are cumulative, and the execution of this JCL without consideration to previously defined structures within the CFRM policy result in the loss of existing CFRM structure definitions. It is highly recommended that a systems programmer customize and submit this JCL.

There are two DEFINE STRUCTURE sections for this JCL: one for the batch structure and log stream, and one for the online structure.

Values that must be customized for IMS Batch processing include:

DEFINE STRUCTURE values:

The name of the batch structure (from AUILSTR1)
(NAME(batch_struc_name))

The name of this log stream is used as input to the **Batch DLI Log Stream Name** field when defining log streams to the agent. Use the LOG_STREAM_DLIB keyword of the configuration member that is specified by the AUICONFG DD statement of the agent (AUIA*STC*) JCL. The LOGSNUM, MAXBUFSIZE and AVGBUFSIZE should not be changed from the default values.

The name of the batch structure (from AUILSTR1)
(STRUCTNAME(batch_struc_name))

The selection of the Staging data set classes
(STG_DATACLAS, STG_MGMTCLAS, and STG_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging data set for the log stream. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters.

The selection of offload data set classes
(LS_DATACLAS, LS_MGMTCLAS, and LS_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates an offload data set for the log stream. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters.

The size of the Batch Log stream DASD data sets
(STG_SIZE)

Note: This can be removed if the STG_DATACLAS value is specified.

The allocation/size of the offload data sets
(LS_SIZE(13500))

The default value is 13500 (the number of 4K blocks). The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of this size. When auditing in a large test or production environment, a value of 40500 might improve throughput.

The High level qualifier of the offload and staging data sets
(HLQ or EHLQ)

The HLQ and EHLQ are mutually exclusive and only one can be used. Other parameters found in the batch structure and online log stream definition might have a **do not change** comment. These parameters

contain the recommended values and should not be altered without careful consideration of the impact of changes to log stream performance and data integrity. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.

You must customize the following values for online structure and log stream processing:

DEFINE STRUCTURE values:

The name of the online structure (from AUILSTR1)
(NAME(online_struc_name))

The LOGSNUM, MAXBUFSIZE and AVGBUFSIZE should not be changed from the default values.

DEFINE LOGSTREAM values:

The name of the log-stream
(NAME(online_logstream_name))

The name of this log stream is used as input to the **Online DLI Log Stream Name** field when defining log streams to the agent. Use the LOG_STREAM_DLIO keyword of the configuration member specified by AUICONFG DD statement of the agent (AUIA*STC*) JCL.

The name of the online structure (from AUILSTR1)
(STRUCTNAME(online_struc_name))

The selection of the Staging data set classes
(STG_DATACLAS, STG_MGMTCLAS, and STG_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging data set for the log stream. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.

The size of the ONLINE Log stream DASD data sets
(STG_SIZE)

Note: This can be removed if the STG_DATACLAS value is specified.

The selection of offload data set classes
(LS_DATACLAS, LS_MGMTCLAS, and LS_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates an offload data set for the log stream. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.

The allocation/size of the offload data sets
(LS_SIZE(13500))

The default value is 13500 (the number of 4K blocks). The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of this size. When auditing in a large test or production environment, a value of 40500 might improve throughput.

The High level qualifier of the offload and staging data sets
(HLQ or EHLQ)

The HLQ and EHLQ are mutually exclusive and only one can be used. Other parameters found in the batch structure and online log stream definition might have a **do not change** comment. These parameters contain the recommended values and should not be altered without careful consideration of the impact of changes to log stream performance and data integrity. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.

DASD-based log streams
This section provides rules and information about DASD-based log streams. Using DASD-based log streams limits auditing by the agent to the LPAR within which the agent is started. IMS Control regions and IMS DLI/DBB batch jobs that run on other LPARS will not be audited.

DASD-based logs streams can only be accessed from one LPAR at a time. Any IMS Online Control regions and DLI/DBB batch jobs to be audited must run on the same LPAR as the agent runs on.

One JCL member in the SAUISAMP product data is included to assist in the definition of DASD-based log streams.

AUILSTR3

This JCL is used to add the DASD based log streams to a LOGR policy used by the IMS Control region and DLI/DBB batch jobs. Detailed instructions can be found within the comments of the JCL.

Note: It is highly recommended that a systems programmer customize and submit this JCL.

There are two DEFINE STRUCTURES sections to this JCL: one for the batch structure, and one for the online structure. Values which must be customized for IMS batch log stream processing are as follows:

DEFINE LOGSTREAM values:

The name of the log-stream
(NAME(batch_logstream_name))

The name of this log stream is used as input to the Batch DLI Log Stream Name field when defining log streams to the agent. Use the LOG_STREAM_DLIO keyword of the configuration member specified by AUICONFG DD statement of the agent (AUIA*STC*) JCL.

The selection of the Staging data set classes
(STG_DATACLAS, STG_MGMTCLAS and STG_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging data set for the log stream. Other parameters found in the batch structure and online log stream definition might have a **do not change** comment. These parameters contain the recommended values and should not be altered without careful consideration of the impact of changes to log stream performance and data integrity. For more information, the IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters, and can be found on the IBM Information Center.

The selection of offload data set classes
(LS_DATACLAS, LS_MGMTCLAS and LS_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates an offload data set for the log stream. For more information, the IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters, and can be found on the IBM Information Center.

The size of the Batch Log stream DASD data sets
(STG_SIZE)

Note: This can be removed if the STG_DATACLAS value is specified.

The allocation/size of the offload data sets
(LS_SIZE(13500))

A value of 13500 (the number of 4K blocks) is the default/supplied value. For more information, the publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of this size, and can be found on the IBM Information Center.

The High level qualifier of the offload and staging data sets
(HLQ or EHLQ)

The HLQ and EHLQ are mutually exclusive and only one can be used. For more information, the IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter, and can be found on the IBM Information Center.

Values which must be customized for IMS ONLINE processing include the following:

DEFINE LOGSTREAM values:

The name of the log-stream
(NAME(online_logstream_name))

The name of this log stream is used as input to the Online DLI Log Stream Name field when defining log streams to the agent using the Guardium user interface.

The selection of the Staging data set classes
(STG_DATACLAS, STG_MGMTCLAS, and STG_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging data set for the log stream. For more information, the IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters, and can be found on the IBM Information Center.

The size of the ONLINE Log stream DASD data sets
(STG_SIZE)

Note: This can be removed if the STG_DATACLAS value is specified.

The selection of offload data set classes
(LS_DATACLAS, LS_MGMTCLAS, and LS_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates an offload data set for the log stream. For more information, the publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters, and can be found on the IBM Information Center.

The allocation/size of the offload data sets
(LS_SIZE(13500))

A value of 13500 (the number of 4K blocks) is the default/supplied value. For more information, the publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of this size, and can be found on the IBM Information Center.

The High level qualifier of the offload and staging data sets
(HLQ or EHLQ)

The HLQ and EHLQ are mutually exclusive and only one can be used. Other parameters found in the batch structure and online log stream definition might have a **do not change** comment. These parameters contain the recommended values and should not be altered without careful consideration of the impact of changes to log stream performance and data integrity. For more information, the publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter, and can be found on the IBM Knowledge Center

Chapter 5. Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

This section describes the information necessary for configuring the agent.

The agent has a primary agent address space that runs as a started task (AUIA*STC*) and multiple secondary address spaces (AUIF*STC*, the SMF collector, AUIL*STC*, the IMS log collector, AUIU*STC*, the common storage utility) that are automatically started and stopped by the primary address space.

The agent primary address space reads the configuration file specified by the AUICONFG DD statement in the AUIA*STC* JCL, and passes the appropriate configuration information to the associated AUIF*STC* and AUIL*STC* tasks. The AUIU*STC* JCL requires the same configuration file to be specified as was specified for the AUIA*STC* task. Use the AUICONFG DD statement to specify the configuration file.

The SAUISAMP member AUICONFG provides a sample configuration that can be used by the agent primary address space started task.

Refer to the following instructions about the AUICONFG data set or the instructions in the data sets to complete the next steps.

Note:

- The data set must be edited using the EBCDIC encoding (1047 CCSID).
- It is recommended that you make a copy of the AUICONFG from SAUISAMP and customize it for use by a given agent.

Customizing the agent by using agent parameter keywords

Use agent parameter keywords to customize the agent. The agent configuration file provides the parameters that can be customized. The parameters that do not have a default value must be specified before you start the agent started task.

How to use the agent parameters

- Use the AUICONFG DD statement to reference these parameters with the agent JCL (AUIA*STC*) and Memory Management secondary address space JCL (AUIU*STC*).
- The AUICONFG DD can be used in other agent secondary address space JCLs (AUIF*STC* and AUIL*STC*).
- Define the data set (DSORG=PS) or data set member (DSORG=PDS|PDS/E) that contains these parameters as RECFM=FB LREL=80.
- Specify only one keyword and parameter per line.
- An asterisk (*) or hyphen (-) in column one indicates that the line is a comment.
- Characters in column 72 and beyond are ignored.

Required parameters
The following parameters must be manually configured:

- **APPLIANCE_SERVER**
- **LOG_STREAM_DLIB**
- **LOG_STREAM_DLIO**
- **SMF_DSN_MASK**
- **SMF_SPILL_FILE**

All available agent parameters

ADS_SHM_ID
Required: No

Default: None

Description: This keyword is optional when only one agent exists in a sysplex environment. If more than one agent exists, the configuration file for each agent should have this keyword specified with a unique integer with a value of 100000 - 999999 specified as its parameter. This keyword identifies a shared memory segment that is specific to each agent.

Note:

- This keyword must be used in combination with **ADS_LISTENER_PORT**.
- If you specify this keyword, you must add an //AUICONFG DD statement to the AUIF*STC* and AUIL*STC* address space JCLs. This DD statement should point to the same data set and member as the agent AUIA*STC* and AUIU*STC* JCLs to enable communication between all participating address spaces.

Syntax: ADS_SHM_ID*(Shared_Memory_label)*

Example: ADS_SHM_ID(100010)

ADS_LISTENER_PORT
Required: No

Default: 39987

Description: This keyword is optional when only one agent exists in a sysplex environment. If more than one agent exists, the configuration file for each agent should have this keyword specified with a unique port number specified. This keyword identifies an agent-specific communications port between the agent (AUIA*STC*) and the agent secondary address spaces (AUIF*STC*, AUIL*STC*). Valid port numbers are 1 - 65535. Check with your network administrator for a list of ports available for this use.

Note:

- This keyword must be used in combination with **ADS_SHM_ID**.
- If you specify this keyword, you must add an //AUICONFG DD statement to the AUIF*STC* and AUIL*STC* address space JCLs. This DD statement should point to the same data set and member as the agent AUIA*STC* and AUIU*STC* JCLs to enable communication between all participating address spaces.

Syntax: ADS_LISTENER_PORT*(port_number)*

Example: ADS_LISTENER_PORT(16055)

APPLIANCE_SERVER
Required: Yes

Default: None

Description: The host name or IP address (in dotted decimal notation, for example: 1.2.3.4) of the IBM Guardium system to which the agent (AUIA*STC*) should connect.

Note: This parameter must be correctly configured to enable a connection to the IBM Guardium system. This value can contain up to 128 characters.

Syntax: APPLIANCE_SERVER*(hostname|IP_address)*

Example:

```
APPLIANCE_SERVER(wal-vm-guardium20)
APPLIANCE_SERVER(192.168.2.205)
```

APPLIANCE_SERVER_[1-5]
Required: No

Default: None

Description: Enables alternative host names or TCP/IP addresses to be used for multistream Guardium appliance destinations or failover recovery processing. Up to five alternative host names or TCP/IP addresses are supported.

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

Valid values are any valid host name or TCP/IP address.

Note:

- The use of this keyword does not eliminate the need for the **APPLIANCE_SERVER** keyword.
- The **APPLIANCE_SERVER_LIST** parameter designates how this parameter is used.
- If used in combination, this parameter overrides the **APPLIANCE _SERVER_[MULTI_STREAM|FAILOVER|HOT_FAILOVER]_[1-5]** parameter.

Syntax:

```
APPLIANCE_SERVER_n(hostname|IP_addr)
```

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

Example:

```
APPLIANCE_SERVER_1(nwt-vm-guardium3)
APPLIANCE_SERVER_1(192.168.2.205)
```

APPLIANCE_SERVER_[MULTI_STREAM|FAILOVER|HOT_FAILOVER]_[1-5]

Required: No

Default: None

Description: The host name or IP address (in dotted decimal notation, for example: 1.2.3.4) of the IBM Guardium system for the IBM Guardium S-TAP for IMS agent to use to stream to multiple Guardium appliance destinations or for failover processing. This value can contain up to 128 characters.

Note:

- The use of this keyword does not eliminate the need for the APPLIANCE_SERVER keyword.
- If this parameter, or the **APPLIANCE_SERVER_[1-5]** parameter, is not detected at startup, then neither failover nor hot failover processing is activated.
- The **APPLIANCE_SERVER_LIST** parameter designates how this parameter is used.
- If used in combination, this parameter is overridden by the **APPLIANCE_SERVER_[1-5]** parameter.

Syntax:

```
APPLIANCE_SERVER_[MULTI_STREAM|FAILOVER|HOT_FAILOVER]_n(hostname|IP_address)
```

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

Example:

```
APPLIANCE_SERVER_MULTI_STREAM_1(wal-vm-guardium20)
APPLIANCE_SERVER_FAILOVER_1(nwt-vm-guardium8)
APPLIANCE_SERVER_HOT_FAILOVER_1(wal-vm-guardium16)
APPLIANCE_SERVER_MULTI_STREAM_1(192.168.2.201)
APPLIANCE_SERVER_FAILOVER_1(192.168.2.202)
APPLIANCE_SERVER_HOT_FAILOVER_1(192.168.2.203)
```

APPLIANCE_SERVER_LIST(MULTI_STREAM|FAILOVER|HOT_FAILOVER)

Required: No

Default: FAILOVER

Description: 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_MULTI_STREAM_n** parameter.

- 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_FAILOVER_n** parameter. The agent attempts to connect to subsequent Guardium systems, beginning with **APPLIANCE_SERVER_FAILOVER_1** and ending with **APPLIANCE_SERVER_FAILOVER_5**.
- 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 cause connection types for each connected Guardium appliance identified by the **APPLIANCE_SERVER_HOT_FAILOVER_n** parameter to be kept active by pings.

- You must specify the primary Guardium appliance by using the **APPLIANCE_SERVER** parameter.
- If the primary Guardium appliance becomes unavailable and failover occurs, *HOT_FAILOVER* maintains the activity of the primary appliance policy.

With any setting 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*.

APPLIANCE_PORT

Required: No

Default: 16022

Valid ports: 16022 or 16023

Description: The IP port number of the IBM Guardium system to which the IBM Guardium S-TAP for IMS agent should connect. This parameter must be correctly configured to enable a connection to the IBM Guardium system. 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 IBM Guardium system 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.

Syntax: APPLIANCE_PORT*(port_number)*

Example: APPLIANCE_PORT(16022)

APPLIANCE_PING_RATE

Required: No

Default: 5

Description: Specifies the interval time between accesses to the IBM Guardium system to prevent timeout disconnections during idle periods. The value is in number of seconds.

Syntax: APPLIANCE_PING_RATE*(ping_interval)*

Example: APPLIANCE_PING_RATE(5)

APPLIANCE_NETWORK_REQUEST_TIMEOUT

Required: No

Default: 500

Description: Specifies a value in milliseconds of time to wait for the completion of a network communication request to send or receive. A value of 0 results in no timeout period. Range: 0 or 500 - 12000.

Syntax: APPLIANCE_NETWORK_REQUEST_TIMEOUT*(milliseconds)*

Example: APPLIANCE_NETWORK_REQUEST_TIMEOUT(500)

AUIU_EXCLUDE_LPAR

Required: No

Default: None

Description: Specifies a list of LPAR names (one to eight characters) in a SYSPLEX environment where the Common Storage Management Utility (AUIU*STC*) should not be scheduled. Multiple **AUIU_EXCLUDE_LPAR** statements can be specified to allow for LPAR name strings that are longer than 53 bytes.

Note: Use this keyword with caution. DLI calls run on the excluded LPARS are not audited.

With the exception of the LPAR where the agent resides, all LPARS can be excluded by using the option *ALL in place of an LPAR name.

Syntax: AUIU_EXCLUDE_LPAR(*list_of_lpars*)

Example: AUIU_EXCLUDE_LPAR(RS21,MYLPAR,YOURLPAR) or AUIU_EXCLUDE_LPAR(*ALL)

AUIU_PROC_NAME

Required: No

Default: AUIU*STC*

Description: Specifies the PROCLIB member name that contains the Common Storage Management Utility JCL. This JCL is supplied as member name AUIU*STC* in the sample library (AUISAMP). If multiple agents are used within a sysplex, each agent requires a separate JCL for each AUIU*STC* address space.

Syntax: AUIU_PROC_NAME*(auiu_mbr_name)*

Example: AUIU_PROC_NAME(AUIUV1013)

DISPLAY_IMSMSG_DLIB(Y|N)

Required: No

Default: N

Description: Controls the output of informational messages AUIJ255I, AUIJ256I, AUIJ257I, and AUIJ258I in the AUILOG output DD of the AUIA*STC* agent address space. These messages are generated from data that is produced by the IMS DLI/DB batch jobs, and is passed to the agent from the DLIB z/OS log stream.

The default setting, *N*, prevents these messages from being written to the AUILOG DD.

Specify *Y* for these messages to be written to the AUILOG DD.

Syntax: DISPLAY_IMSMSG_DLIB*(Y|N)*

Example: DISPLAY_IMSMSG_DLIB(Y)

DISPLAY_IMSMSG_DLIO(Y|N)

Required: No

Default: N

Description: Controls the output of informational messages AUIJ255I, AUIJ256I, AUIJ257I, and AUIJ258I in the AUILOG output DD of the AUIA*STC* agent address space. These messages are generated from data that is produced by the IMS Control Region and passed to the agent from the DLIO z/OS log stream.

The default setting, *N*, prevents these messages from being written to the AUILOG DD.

Specify *Y* for these messages to be written to the AUILOG DD.

Syntax: DISPLAY_IMSMSG_DLIO*(Y|N)*

Example: DISPLAY_IMSMSG_DLIO(Y)

DLIFREQ

Required: No

Default: 100K

Description: Enables you to customize the number of DLI calls that are sent to the Guardium appliance before message AUIJ012I (providing a count of the number of events sent to appliance) is issued.

The count can be represented in thousands (K) or millions (M). Valid values are 10K – 999K and 1 – 10M.

Syntax: DLIFREQ*(100K)*

Example: DLIFREQ(100K)

FORCE_LOG_LIMITED

Required: No

Default: N

Description: Enables you to force limited audit logging by removing sensitive information (such as IMS segment data and concatenated key values) from data that is sent to the Guardium appliance by the S-TAP.

Specify *Y* to restrict sensitive data from being sent to the Guardium appliance.

Syntax: FORCE_LOG_LIMITED*(Y|N)*

Example: FORCE_LOG_LIMITED(N)

IMSL_AUDIT_LEVELS

Required: No

Default: ALL

Description: Specifies the events to be audited from those that are found using the IMS Archive Log task (AUIL*STC*) for each IMS instance under control of this agent. A specification other than ALL limits auditing to the events you specify.

For example, if you specify USERS, then all audited IMS instances under the agent report user signons and signoffs. If you specify ALL, you can use the Guardium interface to specify further limitations on what is audited for each audited IMS subsystem.

Table 2. IMSL_AUDIT_LEVELS audit parameters and events.

Parameter	**Audited event**
ALL	All events are audited (default)
CTL_STRT	IMS control region stops and starts
USERS	User signon and signoff
DBOPN	Database opens and closes
DB_PSB	DBDDUMP, DB/PSB START/STOP/LOCK/UNLOCK

Syntax: IMSL_AUDIT_LEVELS*(ALL|CTL_STRT|USERS|DBOPN|DB_PSB)*

Example: IMSL_AUDIT_LEVELS(ALL)

IMSL_CYCLE_INTERVAL

Required: No

Default: 15

Description: Specifies the frequency (in minutes) that the IMS Archive Log task (AUIL*STC*) checks the RECON data sets for new IMS SLDS (System Log Data Sets) to process. This value should correspond to the frequency at which IMS generates SLDS data sets during a normal workload. For example, if IMS SLDS are produced every 20 minutes, the **IMSL_CYCLE_INTERVAL** should be set to 20. A value of 0 (zero) can be specified to instruct the agent not start the AUIL*STC* task for any IMS subsystem that the agent controls. Valid parameters are 0 – 1440.

Syntax: IMSL_CYCLE_INTERVAL*(time_in_minutes)*

Example: IMSL_CYCLE_INTERVAL(45)

IMSL_ID_PREFIX

Required: No

Default: None

Description: Allows the partial customization of the 8-byte ID that is used when starting the AUILSTC task.

When this keyword is not used, the string *AAAAAAAA* is used for the first AUILSTC task to be started. Subsequent started AUILSTC tasks cause the ALPHA string to be incrementally increased by one character until the value of *ZZZZZZZZ* is reached. When *ZZZZZZZZ* is reached, the string is reset to *AAAAAAAA* when the agent (AUIASTC) is stopped and restarted.

When this keyword is used, the specified prefix (up to 6 bytes) is used, while the remaining two to seven characters are incrementally increased in the manner previously described. This enables a constant value (the specified prefix) to be used, alongside a wildcard character, when you are defining the ID to the TCP/IP security package to permit access to TCP/IP ports.

Note: The first character of the keyword must be an alphabetic character.

Syntax: IMSL_ID_PREFIX*(your_prefix)*

Example: IMSL_ID_PREFIX(MYPFX)

The example **IMSL_ID_PREFIX(MYPFX)** results in a generated AUILSTC ID of *MYPFXAAA* -- *MYPFXZZZ*.

IMSL_PROC_NAME

Required: No

Default: AUIL*STC*

Description: Specifies the PROCLIB member name that contains the IMS Archive Log JCL. This JCL is supplied as member name AUIL*STC* in the sample library (AUISAMP). If multiple agents are used within a sysplex, each agent requires a separate JCL for each AUIL*STC* address space.

Syntax: IMSL_PROC_NAME*(auil_mbr_name)*

Example: IMSL_PROC_NAME(AUILV1013)

IMSL_SLDS_SRCH

Required: No

Default: 30

Description: This keyword can be used to limit the number of days within which the IMS log reader (AUILxxxx) will search for IMS system log data sets (SLDS) to process.

- If an IMS checkpoint does not exist for the SLDS reader, AUILxxxx will search for IMS SLDS that were created on the current day and for *x* days prior to the current day (where *x* is the value that you set for this parameter).
- If an IMS checkpoint that is set for the SLDS reader exceeds the number of days between the current day and the value that you set for this parameter, then the IMS checkpoint will be used as the starting point for IMS SLDS to be read and processed.
- If you set a value of *0* (zero) for this parameter, then only the current day's IMS SLDS will be processed. Also, IMS SLDS that were migrated from a hierarchical storage manager product will not be recalled for processing.

Note: If you set a value of *0* (zero) for this parameter, AUILxxxx processing will omit any IMS SLDS that were created on the previous day. This can cause data to be missed if, for example, the AUILxxxx task is run at 12:05 AM. IMS SLDS that were created prior to midnight will not be recognized as being within the current day, and thus will not be processed.

Syntax: IMSL_SLDS_SRCH*(number_of_days)*

Example: IMSL_SLDS_SRCH(15)

LOG_FILTER(I/E)

Required: No

Default: I (include)

Description: Specifies whether to include or exclude messages that have been specified by the **LOG_FILTER_MSG_ID** parameter.

- The default value, I, allows only the specified message IDs to be included in the AUILOG output stream. Message IDs that are not specified by the **LOG_FILTER_MSG_ID(messages)** parameter will be suppressed. The default value should be used unless there is a specific business need to suppress messages.
- The optional value, E, suppresses the specified message IDs from the AUILOG output stream.

  Tip: The E value should only be used if the **LOG_FILTER_MSG_ID** keyword has been customized to suppress specific messages. Do not use the optional value (E) in conjunction with **LOG_FILTER_MSG_ID(*)** unless you want to prevent all messages from being written to the AUILOG output stream. Suppressing all messages is not recommended.

Syntax: LOG_FILTER*(include/exclude)*

Example: LOG_FILTER(E)

LOG_FILTER_MSG_ID(messages)

Required: No

Default: * (all messages)

Description: Can be used in conjunction with the **LOG_FILTER(I/E)** parameter to suppress specific messages from being written to the AUILOG output stream.

Tip: The **LOG_FILTER_MSG_ID(*)** default value should only be used with the **LOG_FILTER(I)** default value. Do not specify **LOG_FILTER(E)** in conjunction with **LOG_FILTER_MSG_ID(*)** unless you want to prevent all messages from being written to the AUILOG output stream. Suppressing all messages is not recommended.

Syntax: LOG_FILTER_MSG_ID*(id1,id2,id3...)*

Example: LOG_FILTER_MSG_ID(AUIZ014W)

LOG_PORT_SCAN_START

Required: No

Default: 41500

Description: Specifies the first communications port number to be checked for availability to be used for internal message logging communications. Use this keyword if environmental conditions dictate that a sequential scan and test of ports from port numbers 41500 - 65535 should not be performed. You can override the starting port with a port of your choice. This keyword and parameter can be used with the **LOG_PORT_SCAN_COUNT** keyword to limit the ports that are scanned to a specific range.

Syntax: LOG_PORT_SCAN_START*(port_number)*

Example: LOG_PORT_SCAN_START(41500)

LOG_PORT_SCAN_COUNT

Required: No

Default: 10

Description: This keyword can be used in conjunction with the **LOG_PORT_SCAN_START** keyword to limit number of the ports that are scanned and tested for availability. The integer specified (1 - 65535) represents the number of ports that should be scanned. If the port number specified by the

LOG_PORT_SCAN_START value plus the **LOG_PORT_SCAN_COUNT** value exceeds 65535, the scan terminates at port 65535.

Syntax: LOG_PORT_SCAN_COUNT*(number_of_ports)*

Example: LOG_PORT_SCAN_COUNT(1000)

LOG_STREAM_DLIB

Required: Yes

Default: None

Description: This required keyword is used to specify the z/OS System Logger log stream to stream audited events from DLI DBB batch jobs. The value should be the **BATCH_LOGSTREAM_NAME** value specified as the DEFINE LOGSTREAM NAME parameter of the AUILSTR2 or AUILSTR3 JCLs.

Syntax: LOG_STREAM_DLIB*(log_stream_name)*

Example: LOG_STREAM_DLIB(AUI_BATCH_LOG_STREAM)

LOG_STREAM_DLIO

Required: Yes

Default: None

Description: This required keyword is used to specify the z/OS System Logger log stream to be used to stream audited events from IMS Control Regions. The value should be the **ONLINE_LOGSTREAM_NAME** value specified as the **DEFINE_LOGSTREAM_NAME** parameter of the AUILSTR2 or AUILSTR3 JCLs.

Syntax: LOG_STREAM_DLIO*(log_stream_name)*

Example: LOG_STREAM_DLIO(AUI_ONLINE_LOG_STREAM)

LOOPBACK_ADDRESS

Required: No

Default: LOCALHOST

Description: Specifies the loopback host or IP address that is used for communications between the agent and the agent secondary address spaces. For most network configurations, the default value of LOCALHOST can be used. If LOCALHOST cannot be resolved on your system, consult your network specialist for the correct loopback mnemonic or IP address to be used.

Syntax: LOOPBACK_ADDRESS*(hostname|IP_address)*

Example: LOOPBACK_ADDRESS(LOCALHOST)

LPAR_MONITOR_INTERVAL

Required: No

Default: 5

Description: Specifies the frequency (in minutes) for the agent to request a list of LPARs that are active within the SYSPLEX. Schedule the Common Storage Management Utility (AUIU*STC*) tasks on any LPAR coming online to the SYSPLEX. Valid parameters are integers between 1 and 60.

Syntax: LPAR_MONITOR_INTERVAL*(minutes)*

Example: LPAR_MONITOR_INTERVAL(5)

MESSAGE_LOG_LEVEL

Required: No

Default: I

Description: Controls the amount of output log information that is generated by the agent.

Table 3. Message severity codes and descriptions.

Message severity code	Description
I	Includes all log messages

Table 3. Message severity codes and descriptions. (continued)	
Message severity code	**Description**
W	Includes all log messages with a warning severity or higher
E	Includes all log messages with an error severity or higher
O	Instructs the agent not to log error messages
S	Includes all log messages with a severe error code

Syntax: MESSAGE_LOG_LEVEL*(I|W|E|O|S)*

Example: MESSAGE_LOG_LEVEL(I)

OUTAGE_SPILL_AREA_SIZE

Required: No

Default: 0

Description: Determines the maximum amount of memory in megabytes to be allocated for the retention of audit data in the event of a IBM Guardium system connection outage. A value of 0, or the absence of this keyword, disables spill area support. The maximum value permitted as a parameter is 1024.

Syntax: OUTAGE_SPILL_AREA_SIZE*(memory_size)*

Example: OUTAGE_SPILL_AREA_SIZE(15)

POLICY_READ_INTERVAL

Required: No

Default: 5

Description: Determines the frequency in seconds that the connection to the IBM Guardium system checks for changes to the installed policies that are used to determine audited event collection.

Syntax: POLICY_READ_INTERVAL*(time_in_seconds)*

Example: POLICY_READ_INTERVAL(5)

STAP_STREAM_EVENTS

Required: No

Default: Y

Description: Specifies whether events will be streamed to the IBM Guardium system. The default value, *Y*, enables streaming. Specify *N* to disable streaming and enable Simulation mode.

Syntax: STAP_STREAM_EVENTS*(Y|N)*

Example: STAP_STREAM_EVENTS(Y)

PREFER_IPV4_STACK

Required: No

Default: N

Description: If set to Y, this parameter causes a request to be issued to the Domain Name Server (DNS) for an IPV4 address for the hostname that is specified in the **APPLIANCE_SERVER** parameter:

- The DNS lookup request for an IPV4 address is attempted. If an IPV4 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
- If only an IPV6 address is defined at the DNS, then the DNS will respond with the IPV6 address that will be used to connect to the Guardium appliance.
- If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.

If this parameter is set to N or omitted from configuration, a request for an IPV6 address is issued to the DNS for the hostname that is specified by the **APPLIANCE_SERVER** parameter:

- The DNS lookup request for an IPV6 address is attempted. If an IPV6 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
- If only an IPV4 address is defined at the DNS, then the DNS will respond with the IPV4 address that will be used to connect to the Guardium appliance.
- If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.

Note: Whether or not this parameter is used, if the address returned from the DNS is not valid for the hostname, it will result in failure to connect to the appliance, and the IBM Guardium S-TAP for IMS started task will terminate.

Syntax:

```
PREFER_IPV4_STACK(Y|N)
```

Example:

```
PREFER_IVP4_STACK(Y)
```

SMF_AUDIT_LEVELS

Required: No

Default: ALL

Description: Specifies which events to audit of those found using the SMF task (AUIF*STC*). A specification other than ALL limits the events to be audited to the events you specify. For example, if DELETE is specified, then all audited IMS instances under the agent would only be capable of reporting data set DELETE events. If ALL is specified, you can further limits what is audited for each audited IMS subsystem, using the user interface.

Table 4. SMF_AUDIT_LEVELS audit parameters and events

Parameter	**Audited event**
ALL	All events are audited (default)
UPDATE	Data sets opened with UPDATE access
DELETE	Data sets deleted
READ	Data sets opened with READ access
CREATE	Data sets created
ALTER	Data sets opened with ALTER access
RACF	RACF violations on data sets

Syntax: SMF_AUDIT_LEVELS*(ALL|UPDATE|DELETE|READ|CREATE|ALTER|RACF)*

Example: SMF_AUDIT_LEVELS(ALL)

SMF_CYCLE_INTERVAL

Required: No

Default: 300

Description: Specifies the frequency (in minutes) that the SMF task (AUIFSTC) checks the z/OS catalog for new data sets, which meet the specified data set masks, using the **SMF_DSN_MASK** keyword. This value should correspond to the frequency at which your z/OS system swaps SMF logging VSAM files (sometimes known as SMF MANX|MANY) during a normal workday. For example, if the SMF logging files are swapped every 8 hours, the **SMF_CYCLE_INTERVAL** should be set to 480 (8

hours * 60 minutes). A value of zero can be specified to indicate that the agent should not start the AUIF*STC* task and SMF auditing should not be performed. Valid parameters are 0 – 1440.

Syntax: SMF_CYCLE_INTERVAL*(time_in_minutes)*

Example: SMF_CYCLE_INTERVAL(45)

SMF_DSN_MASK_[1-10]

Required: Yes

Default: None

Description: At least one instance of this keyword is required (**SMF_DSN_MASK_1**). This keyword provides a data set mask used to query the z/OS catalog for sequential format data sets containing SMF data offloaded from the SMF log-files (MANX|MANY) using the IFASMFDP program. These sequential files can be the original files created when offloading the MANX|MANY files, or a copy of these sequential files created by customizing and running AUISMFDF and AUISMFDP jobs located in the product sample data set. In most environments, only one **SMF_DSN_MASK** would be specified, but up to 10 are allowed.

Table 5. Masking character rules

Character	Rule
%	Indicates that only one alphanumeric or national character can occupy that position
%%%	Indicates that more than one character can be substituted, with the number of substitution characters being equal to the number of percent signs specified.

Example 1: specifying a GDG data set in the mask: If the AUISMFDP job has been customized to produce a GDG data set as the SORTOUT DD output data sets, you can choose to specify the fully qualified GDG base name in the mask for system name field. For example, A.B.C. IBM Guardium S-TAP for IMS uses catalog services to determine the names of all cataloged GDG entries under this name, for example:

- A.B.C.G0001V00
- A.B.C.G0002V00
- A.B.C.G0003V00

Example 2: specifying a data set name explicitly: Provide the generation and version values as a mask. For example, A.B.C.G%%%%V%%. IBM Guardium S-TAP for IMS uses catalog services to determine the names of all cataloged data sets that match this mask, for example:

- A.B.C.G0021V00
- A.B.C.G0022V00
- A.B.C.G0023V00

Example 3: specifying a DSN using a DATE/TIME naming convention: If you have customized the AUISMFDP job to produce a data set name that contains date and time values as qualifiers within the data set name as the SORTOUT DD output data sets, you can specify the data set name using a string of percent signs within the date and time qualifier names. For example: HLQ.D%%%%%%.T%%%%%%.SMFDATA. IBM Guardium S-TAP for IMS uses catalog services to determine the names of all cataloged data sets matching the mask, for example:

- HLQ.D091122.T131000.SMFDATA
- HLQ.D091123.T131100.SMFDATA
- HLQ.D091124.T131200.SMFDATA

Note: The percent (%) wildcard character should only be specified for the numeric characters of the generation and version node of GDG data sets, or as the numeric characters of date or time nodes of the SMF dataset.

Syntax: SMF_DSN_MASK_1*(SMF.DUMP.DSN)*

Example:

```
SMF_DSN_MASK_1(AUI.SMF.DUMP.COPY)
SMF_DSN_MASK_2(AUI.SMF.DUMP.GDG.G%%%%V%%)
SMF_DSN_MASK_3(AUI.SMF.D%%%%%%.T%%%%%%.COPY)
```

SMF_EVENT_EXPIRY

Required: No

Default: 5

Description: Specifies the number of days that incomplete SMF events should be retained in the SMF spill file. Incomplete SMF events are audited events that have not yet received the associated SMF Type 30 record, which indicates that the step/job is complete, and contains information that is needed to complete the reporting of the event. When an event exceeds the expiration date, it is flagged as incomplete, sent to the IBM Guardium system, and removed from the SMF spill file. The valid range is 1 to 180 days.

Syntax: SMF_EVENT_EXPIRY*(days)*

Example: SMF_EVENT_EXPIRY(5)

SMF_PROC_NAME

Required: No

Default: AUIFSTC

Description: Specifies the PROCLIB member name that contains the SMF secondary address space JCL. This JCL is supplied as member name AUIF*STC* in the sample library (AUISAMP). If multiple agents are used within a sysplex, each agent requires a separate JCL for each AUIF*STC* address space.

Syntax: SMF_PROC_NAME*(auif_mbr_name)*\

Example: SMF_PROC_NAME(AUIFV91)

SMF_SELF_AUDIT

Required: No

Default: N

Description: Indicates whether to audit the accesses of IMS data sets that are used by the product to determine the names of IMS artifacts to be audited. Examples of IMS data sets that can be accessed include RECON data sets and IMS archived logs (SLDS). A value of N indicates that these accesses should not be audited. A value of Y indicates that these data sets should be considered for auditing.

Syntax: SMF_SELF_AUDIT*(N|Y)*

Example: SMF_SELF_AUDIT(N)

SMF_SPILL_FILE

Required: Yes

Default: None

Description: Specifies the DSN of a sequential format fixed block data set with a LRECL of 300. This data set is used to store incomplete audited SMF events. Incomplete audited SMF events are events triggered by SMF records that have yet to encounter an SMF Type 30 record, indicating the step or job has completed. The AUIFUSPL member of the SAUISAMP data set provides an example of the allocation specifications for this data set.

Syntax: S**MF_SPILL_FILE***(dsn)*

Example: SMF_SPILL_FILE(AUI.V1013.SPILL)

TCPIP_BUFFER_SIZE

Required: No

Default: 32768

Description: Specifies the size of an internal buffer that is used to hold audited events in preparation of the TCP/IP send to the IBM Guardium system, and specifies the size of the TCP/IP buffer. In most environments, the size of this buffer should not be changed

Syntax: TCPIP_BUFFER_SIZE*(buffer_size)*

Example: TCPIP_BUFFER_SIZE(32768)

TRACE_CONFIG

Required: No

Default: ON

Description: TRACE_CONFIG(ON) enables IBM Guardium S-TAP for IMS configuration values to display by default at agent startup. You can optionally use this keyword to disable the IBM Guardium S-TAP for IMS configuration value display. To prevent the displayed report of agent configuration parameters during agent startup, specify TRACE_CONFIG(OFF).

Syntax: TRACE_CONFIG*(ON|OFF)*

Example: TRACE_CONFIG(OFF)

WTO_MSG

Required: No

Default: None

Description: Allows a user to request that specific informational, warning, or error messages written to the AUILOG DD statement of the agent (AUIA*STC*) or agent secondary address spaces (AUIF*STC*, AUIL*STC* or AUIU*STC*) also be written to the Operator Console (WTO). This enables these messages to be recognized by an automated operations tool, or provides higher operator visibility for these messages and allows appropriate action to be taken. Each message requires a separate keyword, and each keyword must be specified on a separate line.

Syntax: WTO_MSG*(msgnumber)*

Example:

```
WTO_MSG(AUIJ011I)
WTO_MSG(AUIL607W)
WTO_MSG(AUIY006E)
```

XML_ECHO_AUILOG(Y|N)

Required: No

Default: N

Description: Indicates that when an audit policy is installed on a IBM Guardium system appliance, its corresponding XML is to be echoed to the AUILOG DD. If there is more than one policy installed on the agent, the XML of each policy is echoed. If all installed policies are subsequently uninstalled, then the echoed XML reflects that there are no installed policies. For more information about echoed XML statements, see XML statement definitions.

Syntax: XML_ECHO_AUILOG(Y|N)

Example: XML_ECHO_AUILOG(Y)

XML_ECHO_DATASET(Data_Set_Name[,Cylinders])

Required: No

Default: None

Description:

Indicates that when the IBM Guardium system installs an audit policy, its corresponding XML is echoed to a data set (specified by the data set name value in this parameter). If there is more than one policy installed on the agent, the XML of each is echoed. If all installed policies are subsequently uninstalled, then the echoed XML reflects that there are no installed policies. The XML will not be echoed when the installed policy is already active, is being reinstalled, and there have been no changes to the policy.

If *Data_Set_Name* is intended to be a Generation Data Group (GDG), then it must be set as the GDG base name. The agent checks the system catalog to determine whether *Data_Set_Name* exists and whether or not it is a GDG base name.

Data_Set_Name can contain z/OS system symbols such as &SYSNAME. To determine the names of the system symbols that are currently defined to the system, issue the **DISPLAY SYMBOLS** command to the system console.

If *Data_Set_Name* does not exist, and there is no GDG base defined in this name, the agent allocates the data set as non-GDG. If *Data_Set_Name* is a regular physical sequential data set (non-GDG based) and does exist, the agent allocates space for the *Cylinders* keyword when the agent is restarted.

Cylinders defaults to 1 and can range from 1 – 10.

Syntax: XML_ECHO_DATASET*(&Data_Set_Name[,Cylinders])*

Example: XML_ECHO_DATASET(AUIAGENT.ECHO.XML.GDG.BASE,2)

ZIIP_AGENT_DLI

Required: No

Default: N

Description: Indicates that the following agent processes should be zIIP capable: agent reads of audited events from the z/OS System Logger log streams, formatting of these events into protobuf style messages, and sending of these messages to the IBM Guardium system using TCP/IP.

Note: Use of the zIIP depends on the presence of a zIIP on the LPAR where the agent is running, as well as use of the Workload Management Service Policies. For more information about zIIP, see the topic on Customizing IMS to use a System z Integrated Information Processor (zIIP).

Syntax: ZIIP_AGENT_DLI*(Y|N)*

Example: ZIIP_AGENT_DLI(Y)

Related reference

Customizing IMS to use a System z Integrated Information Processor (zIIP)

IBM Guardium S-TAP for IMS allows you to configure an IMS control region to prepare specific auditing functions for execution on a System z Integrated Information Processor (zIIP). Execution on a zIIP is governed by the Workload Management software on your appliance, as well as the workload already assigned to the zIIP.

Agent configuration

The IP addresses of the IBM Guardium system appliances are specified using the SAUISAMP data set AUICONFG member using the APPLIANCE_SERVER and APPLIANCE_SERVER_FAILOVER_[1-5] keywords.

See “Providing Guardium system failover” on page 51 for more information.

Customizing the agent JCL

The SAUISAMP member AUIA*STC* provides a sample JCL that can be used for the agent started task. This topic describes how to customize the JCL.

Before you begin

In environments where multiple agents connect to a common IBM Guardium system or appliance, the z/OS agent started task names (AUIA*STC*, AUIL*STC*, AUIF*STC*) must be unique. Unique started task names enable the IBM Guardium S-TAP for IMS policies that are pushed from the IBM Guardium system to be attributed to, and monitored by, the correct z/OS agent.

Procedure

1. Edit SAUISAMP members AUIA*STC*, AUIF*STC*, AUIL*STC* and AUIU*STC* by running the ISPF edit macro.
   See “Planning your configuration and customizing your environment” on page 12 for more details.

2. Modify the CFG=AUI.V100.AGTCFG(AUICONFG) in AUIA*STC* to specify the location of the customized configuration data set for the agent created in the previous section.
3. You can rename the AUIA*STC* member to any character name that is valid for started tasks in your environment.
4. You can rename the AUIF*STC*, AUIL*STC*, and AUIU*STC*. AUIF*STC*, AUIL*STC*, and AUIU*STC* names should match the values of the IMSL_PROC_NAME, SMF_PROC_NAME, and AUIU_PROC_NAME keywords that you supply in the configuration file.
5. Copy the AUIA*STC*, AUIF*STC*, AUIL*STC* and AUIU*STC* members to the PROCLIB for the site.

   Contact the z/OS systems programmer to determine the location of the PROCLIB.

   Note: APF authorization of the AUILOAD file is required for each of these members before they are started.

Starting and stopping the agent

Start the agent by issuing the command **/S AUIASTC** from the SDSF command line. The primary agent address space starts the AUIF*STC* address spaces. One or more instances of AUIL*STC* might also be started, depending on the list of active collections.

Stop the agent by issuing the command **/STOP AUIASTC**, or **/MODIFY AUIASTC,STOP**, from the SDSF command line. The primary agent address space then stops all the secondary address spaces that are online, and shuts down. Depending on the load, and the activity in the other secondary address spaces, the shut down process can take time. Monitor the AUILOG DD of the primary address space AUIA*STC* for informational messages on the status of the secondary address spaces.

Agent security considerations

The user ID of the agent started tasks (the primary and the secondary started tasks) should have the necessary RACF profiles for reading the configuration member contents.

Important: Contact your system administrator to ensure that **localhost** is resolving to 127.0.0.1 (loopback address). The TCP/IP communication between the agent and the secondary address spaces relies on this resolution. If this is not possible at your site, use the *loop-back-address* element in the AUICONFG sample library member to avoid localhost resolution by specifying the loopback IP address directly, or by specifying an appropriate host name that resolves to the loopback address.

Modifying the frequency of AUIJ012I messages

You can modify how frequently the agent provides a count of DLI calls (from the default of every 10K DLI calls to a value of your choice, 10K – 999K, 1M – 10M.)

Use the agent parameter keyword **DLIFREQ** to modify the frequency of AUIJ012I messages, or issue the command **/MODIFY AGENT,SET CONFIG DLIFREQ** *aaaK* | *bbM*, from the SDSF command line.

Chapter 6. Setting up an IMS environment for auditing

This section describes how to customize IMS environments to capture DLI calls, including customizing IMS catalogued procedures, coexisting with other DFSFLGX0 and DFSISVI0 exit routines, customizing IMS to use a zIIP, copying common load modules from SAUILOAD to SAUIIMOD, and the security considerations related to IMS processing.

Security considerations for IMS processing

IBM Guardium S-TAP for IMS does not impose any additional RACF or other security restrictions on IMS assets during IMS processing. However, the IMS control region and any DLI/DBB batch jobs being executed, must have UPDATE authority to the z/OS system log streams you have defined for use by IBM Guardium S-TAP for IMS.

Customizing IMS environments to capture DLI calls

For IBM Guardium S-TAP for IMS to report on IMS database accesses, it needs to be sensitive to IMS DL/I calls. Use the following sections to establish proper set-up of the relationship between your IMS online and batch environments and IBM Guardium S-TAP for IMS.

Note: The IBM Guardium S-TAP for IMS programs that are used to communicate with your IMS environments are found in the SAUIIMOD data set, and are created during product installation.

Customizing IMS cataloged procedures

For IBM Guardium S-TAP for IMS to monitor DL/I calls from IMS online Transactions, BMPs and DLI/DBB batch jobs, the IMS Control region and DLI/DBB batch jobs require access to these IBM Guardium S-TAP for IMS programs.

The IBM Guardium S-TAP for IMS programs that must be accessed reside in the SAUIIMOD installation data set. The preferred method of installing IBM Guardium S-TAP for IMS into your IMS environment is to copy the entire contents of the SAUIIMOD data set into your IMS RESLIB (IMS.SDFSRESL) data set.

If copying IBM Guardium S-TAP for IMS programs into your IMS RESLIB is not possible, then the SAUIIMOD data set must be included in your IMS control region JCL as the first data set of the STEPLIB DD concatenation. The SAUIIMOD data set must also be included as the first data set of the STEPLIB DD concatenation of the DLI batch cataloged procedure (DLIBATCH member of the IMS PROCLIB data set) and the DBB batch cataloged procedure (DBBBATCH member of the IMS PROCLIB data set).

Note:

- If the SAUIIMOD data set is included in any JCL, you must ensure that it is APF-authorized.
- IBM Guardium S-TAP for IMS provides and uses the DFSFLGX0 and DFSISIV0 IMS exits to establish communication with IMS services, however no customization of these exits is required.

Coexisting with other DFSFLGX0 and DFSISVI0 exit routines

IBM Guardium S-TAP for IMS provides product-specific DFSFLGX0 (IMS Logger) and DFSISVI0 (IMS Batch) exits to enable the product to report on IMS DL/I call activity. In some IMS environments, user requirements or third-party vendor products also require the use of these exits. IBM Guardium S-TAP for IMS can accommodate the use of multiple DFSFLGX0 and DFSISVI0 exit routines.

Using IMS Tools Generic Exits

IMS Tools Generic Exits are a collection of components that provide common command and exit routine interfaces to support the operation of IMS tools in an IMS environment.

IBM Guardium S-TAP for IMS supports the protocols used by the IMS Tools Generic Exit product. You can define the IBM Guardium S-TAP for IMS copy of the DFSFLGX0 exit by either supplying IMS with a PROCLIB member using a BPE-style control statement, or by building a load module that contains the required information.

An example of the PROCLIB control statement follows:

```
EXITDEF(TYPE(LOGR) EXITNAME(AUIFLGX0) LOADLIB(AUI.SAUIIMOD))
```

See the IBM IMS Tools Generic Exit Reference Manual for Generic Logger Exit setup and usage.

Important: The IBM IMS Tools Generic Exit product does not support exit DFSISVI0.

Using IBM Guardium S-TAP for IMS exit cascading

For situations where the IBM IMS Tools Generic Exit is not available for use, IBM Guardium S-TAP for IMS provides a method of supporting two instances of the DFSFLGX0 and DFSISVI0 exits.

When loaded and run, the IBM Guardium S-TAP for IMS supplied program AUIFLGX0 (DFSFLGX0) and AUIISVI0 (DFSISIV0) determines from which DSN within the JOBLIB/STEPLIB concatenation it was loaded from. It then searches all subsequent DSNs within the JOBLIB/STEPLIB DD concatenation, looking for the next occurrence of the exit with the same name.

- If none are found, or it is determined that the IMS Tools Generic Exit product is involved in executing the exit, no cascading is done.
- If an exit is found, and it is determined that the exit found is in fact another instance of the IBM Guardium S-TAP for IMS exit (as could happen if the SAUIIMOD data set was specified multiple times in the JOBLIB/STEPLIB concatenation), the search will continue with the remainder of the DSNs in the concatenation.
- If a non-IBM Guardium S-TAP for IMS Exit is found, this new exit is loaded, and called with R13 pointing to the save area supplied by IMS. A new 512 byte user work area, obtained specifically for this exit instance, is then pointed to by the SXPLAWRK field of the IMS Standard User Exit Parameter List (DFSSXPL). This 512 byte work area is obtained when the first (or INIT) call is done; the work area address (in the SXLPAWRK field) and work area content are maintained for all subsequent calls.

Exit cascading restrictions

Note: These restrictions only apply when using the exit cascading feature, and not when using the IBM IMS Tools Generic Exit product.

The IBM Guardium S-TAP for IMS Exit (AUIFLGX0 or AUIISVI0) must be first in the JOBLIB/STEPLIB concatenation, unless the exit that exists in a prior DSN also has a method of cascading calls to other exits, and is capable of providing an IMS formatted area in R13 and the address of a unique, persistent 512 byte work area in the SXPLAWRK parameter list field to the AUIFLGX0 or AUIISVI0 program.

In a non-APF-authorized environment, such as when executing program DFSULTR0 or an IMS DLI/DBB batch program, the exit load module to be cascaded to must have an ALIAS, and the ALIAS must be appropriately either DFSFLGX0 or DFSISVI0, if the target exit module has the RENT or REUS attribute on.

Defining LOGWRT exits

Use the **EXITDEF** parameter in the USER_EXITS section of the DFSDFxxx IMS PROCLIB member to define LOGWRT exits to be used by your IMS subsystem.

You must specify the exit name AUIFLGX0 in the list of LOGWRT exits to be used. This disables the cascading feature, which prevents other LOGWRT exits in the STEPLIB from being unintentionally invoked. You must include the SAUIIMOD load library in the IMS Control Region STEPLIB concatenation.

Example:

```
<SECTION=USER_EXITS>
EXITDEF=(TYPE=LOGWRT,EXITS=(AUIFLGX0))
```

Customizing IMS to use a System z Integrated Information Processor (zIIP)

IBM Guardium S-TAP for IMS allows you to configure an IMS control region to prepare specific auditing functions for execution on a System z Integrated Information Processor (zIIP). Execution on a zIIP is governed by the Workload Management software on your appliance, as well as the workload already assigned to the zIIP.

To use this feature, the LPAR on which the IMS Control region executes must have a zIIP installed. The IMS Control Region should also make use of the z/OS Workload Manager product. For more information on using z/OS Workload Manager with the IMS Control Region, see the *Workload Manager and IMS* section of the *IBM IMS System Administration* manual.

The following processes can be scheduled on a zIIP:

- Calling of the compiled filter to determine if the DLI event is to be audited, and if the segment concatenated key or segment data should be sent to the Guardium appliance.
- Movement of the audited DLI calls to a storage buffer used to hold audited data until a write to the z/OS System Logger log-stream can be executed
- Calling of the z/OS System Logger IXGWRITE, which moves the audited data from the buffer to the log-stream when the buffer fills, or a flush of the buffer is scheduled

To indicate that the IMS Control region should attempt to schedule these processes on the zIIP, a **// AUIZIIP DD DUMMY** DD statement should be added to the IMS Control Region JCL. When detected, the audit code produces the informational message AUII055I, indicating that zIIP processing will be attempted.

Warning messages AUII042W and AUII043W are issued if zIIP processing is requested when a zIIP is not available, and when IMS is not using Workload Manager. Error message AUII044E indicates that the request was rejected. In all instances where the attempt to use the zIIP has failed, audit processing continues without attempting to execute the audit code on the zIIP.

Related reference

Customizing the agent by using agent parameter keywords
Use agent parameter keywords to customize the agent. The agent configuration file provides the parameters that can be customized. The parameters that do not have a default value must be specified before you start the agent started task.

Copying common load modules from SAUILOAD to SAUIIMOD

After the initial SMP/E installation of IBM Guardium S-TAP for IMS, copy common load modules from the SAUILOAD to SAUIIMOD data set using the modules described in this topic.

AUI$NAP
Module used to trace data

Provided in the SAUILOAD data set

Also needed in the SAUIIMOD data set

AUICPMOD

An SAUISMAP member

Performs a copy of the AUI$NAP module from the SAUILOAD to the SAUIIMOD data set

Should be customized and submitted after the initial SMP/E installation

Configuring APP_EVENT support

IBM Guardium S-TAP for IMS allows IMS DLI application programs to store user information on the IBM Guardium system. This enables your user data to be linked with DLI DB calls that are made from within the same application checkpoint, unit-of-work, or commit. APP_EVENT calls are linked to audited DLI calls by subsystem ID, application sequence number, and number of commits within a schedule. Follow these steps to install and configure a new IMS database, named AUIAPPEV, to be used for this purpose.

Procedure

1. Perform a Database Descriptor Generator (DBD gen) for the AUIAPPEV database.
   An example of the DBD source to use is in member AUIAPPEV of the SAUISAMP data set.
2. Create a database data set for the AUIAPPEV database.
3. If appropriate for your site, register the DB and DDN to DBRC, specifying NOREOV if possible.
4. If appropriate for your site, create a dynamic allocation (MDA) member for the database data set.
5. Modify application program PSBs to include a PCB for the AUIAPPEV database.
   Use a PROCOPT of *G* and a KEYLENGTH of *0*.
6. If the APP_EVENT feature is to be used by an IMS Online system, perform an ACBGEN for DBD member AUIAPPEV and the modified PSBs.
7. Modify application programs to send APP_EVENT information using the AUIAPPEV PCB:
   a) In the 2000 byte I/O area, modify the application programs to include the information that you want to be sent to the appliance.
   b) Perform a DLI GET call by using the AUIAPPEV PCB.
      A DLI status code of blanks will be returned.

APP_EVENT examples

Examples of the AUIAPPEV database, a PSB with DBPCB for the AUIAPPEV database included, the Assembler language of an IMS DLI call, and a C program are provided here. These code samples are for example purposes only. There is no guarantee of the reliability, serviceability, or function of these programming examples.

AUIAPPEV database

The AUIAPPEV database is used to support the transmittal of environmental information from an application program to the Guardium appliance. The following is an example:

```
DBD             NAME=AUIAPPEV,ACCESS=(HDAM,OSAM),RMNAME=(DFSHDC40,10,20)
DATASET         DD1=AUIAPPEV,SIZE=2048
SEGM          NAME=ROOT,PARENT=0,BYTES=2000
DBDGEN
FINISH
END
```

PSB with DBPCB for the AUIAPPEV database included

The following is an example of a PSB with DBPCB for the AUIAPPEV database included:

```
PCB            TYPE=DB,PROCOPT=A,KEYLEN=4,DBDNAME=AUEVOL01, PCBNAME=ODBPCB1
SENSEG         NAME=ROOT,PARENT=0
```

```
PCB             TYPE=DB,PROCOPT=G,KEYLEN=0,DBDNAME=AUIAPPEV, PCBNAME=APPEV01
SENSEG          NAME=ROOT,PARENT=0
PSBGEN          LANG=ASSEM,CMPAT=YES,PSBNAME=AUIPSBAV
END
```

Assembler language of an IMS DLI call

The following is an example in the Assembler language of an IMS DLI call that will send a string to the Guardium appliance:

```
MVC       IOAREA(20),=CL20'THIS IS AN APP_EVENT'    /Set APP_EVENT message
XC        PARM@(12*4),PARM@               /Clear parameter area
LA        R1,GN                      /Addr of GN literal
ST          R1,PARM@+0                        /Save in parmlist
L         R2,APPCB@                        /Addr of AUIAPPEV PCB
ST       R2,PARM@+4                       /Save in parmlist
LA       R1,IOAREA                          /Addr of IOAREA
ST        R1,PARM@+8                 /Save in parmlist
OI       PARM@+8,X'80'           /Terminate parmlist
LA       R1,PARM@                 /Addr of parmlist
L        R15,DLI@                /Addr of ASMTDLI program
BASR     R14,R15                            /Call ASMTDLI
```

C program

The following is an example of a C program:

```
#define    iopcb     (IO_PCB_TYPE *)(__pcblist)        /* I/O PCB */
#define    dbpcb     (PCB_STRUCT_8_TYPE *)(__pcblist)  /* DB PCB  */
#define    aepcb     (PCB_STRUCT_8_TYPE *)(__pcblist)  /* AUIAPPEV DB PCB  */

int  rc = 0;
const static char GU = "GU  ";

struct {
  char output 2000¨;
} iodata ;


....
....

/* create a APP_EVENT */
sprintf(iodata.output, "THIS IS AN APP_EVENT");
rc = ctdli(GU, aepcb, &iodata);
```

Chapter 7. Using agent configuration keywords to customize auditing

Some agent configuration keywords must be used for the product to function. You can also use agent configuration keywords for optional auditing specifications.

Required keywords
The following keywords must be set for the product to function:

APPLIANCE_SERVER
This is the host name, or IP address, of the IBM Guardium system to which the agent should connect.

LOG_STREAM_DLIO
This is the log stream name for online DLI calls.

LOG_STREAM_DLIB
This is the log stream name for batch DLI calls.

You can also audit accesses to database-related data sets using SMF records. To audit accesses to IMS data sets that occur outside of IMS services, use the following keywords:

SMF_SPILL_FILE
This is the data set name.

SMF_DSN_MASK_1
This is the data set mask value.

Optional keywords
To set the following optional specifications, use the keyword that is listed. More information about each specification is provided, following this list.

Enabling Simulation mode
STAP_STREAM_EVENTS(N)

Restricting IMS segment and concatenated key data from being sent to the Guardium appliance
FORCE_LOG_LIMITED(Y)

Using multiple SMF data set masks
SMF_DSN_MASK_2 through **SMF_DSN_MASK_10**

Disabling SMF auditing at the agent level
SMF_CYCLE_INTERVAL(0)

Note: If **SMF_CYCLE_INTERVAL(0)** is specified, no additional SMF configuration parameters are required.

Controlling the frequency of SMF z/OS catalog queries
SMF_CYCLE_INTERVAL(time in minutes)

Changing the retention period of incomplete SMF events
SMF_EVENT_EXPIRY(number of days)

Changing the name of the SMF address space JCL
SMF_PROC_NAME(new name)

Auditing IMS data set access
SMF_SELF_AUDIT(Y)

Changing the type of events audited using SMF records
SMF_AUDIT_LEVELS(ALL|UPDATE|DELETE|READ|CREATE|ALTER|RACF)

Overriding the range of ports used for address space communications
LOG_PORT_SCAN_START(41501), LOG_PORT_SCAN_COUNT(24003)

Requesting specific agent messages to be issued to the operator console
`WTO_MSG(AUIF507E), WTO_MSG(AUIT013I)`

Determining the context of APPLIANCE_SERVER_[1-5] or APPLIANCE_SERVER_[FAILOVER|MULTI_STREAM|HOT_FAILOVER]_[1-5]
`APPLIANCE_SERVER_LIST(FAILOVER|MULTI_STREAM|HOT_FAILOVER)`

Providing Guardium system failover support
`APPLIANCE_SERVER_FAILOVER_[1-5](IP address or host name)`

Providing Guardium system multistream support
`APPLIANCE_SERVER_MULTI_STREAM_[1-5](IP address or host name)`

Providing Guardium system hot failover support
`APPLIANCE_SERVER_HOT_FAILOVER_[1-5](IP address or host name)`

Providing a spill area for short term outages
`OUTAGE_SPILL_AREA_SIZE(megabytes)`

Disabling IMS SLDS auditing at the agent level
`IMSL_CYCLE_INTERVAL(0)`

Note: If `IMSL_CYCLE_INTERVAL(0)` is specified, no additional IMSL configuration parameters are required.

Controlling the frequency IMS System Log Data Sets are allocated and read
`IMSL_CYCLE_INTERVAL(time in minutes)`

Changing the name of the IMSL address space JCL
`IMSL_PROC_NAME(new name)`

Changing the type of events audited using IMS SLDS records
`IMSL_AUDIT_LEVELS(ALL|CTL_STRT|USERS|DBOPN|DB_PSB)`

Changing the name of the Common Memory Management address space JCL
`AUIU_PROC_NAME(new name)`

Excluding DLI calls occurring on specific LPARS from being audited
`AUIU_EXCLUDE_LPAR(lpar1, lpar2…lpar9)`

Running more than one agent in a SYSPLEX
`ADS_SHM_ID(100010), ADS_LISTENER_PORT(16055)`

Removing Segment data and Concatenated Key values from audited data at the agent level
`FORCE_LOG_LIMITED(Y)`

Using the System z Integrated Information Processor (zIIP)
`ZIIP_AGENT_DLI`

Viewing AUI messages that are produced by the IMS Control regions in the AUI agent log
`DISPLAY_IMSMSG_DLIO(N|Y)`

Viewing AUI messages produced by the IMS DLI/DBB batch jobs in the AUI agent log
`DISPLAY_IMSMSG_DLIB(N|Y)`

Restricting auditing to specific IMS systems when multiple IMSs share RECON data sets
`IMSNAME_EQ_IMSSSID(N|Y)`

Enabling/Disabling the IBM Guardium S-TAP for IMS configuration value display at agent startup
`TRACE_CONFIG(ON|OFF)`

Setting the number of days within which AUILxxxx will process IMS system log data sets (SLDS)
`IMSL_SLDS_SRCH(number of days)`

Simulation mode

Simulation mode enables you to simulate agent processing. IBM Guardium S-TAP for IMS uses various z/OS MVS system services to gather audit data and move it to the agent address space. The agent address space evaluates this data according to the specified policy, and transmits the audit record to the

Guardium appliance by using TCP/IP. To assess the impact on MVS processing, use the **STAP_STREAM_EVENTS** parameter to simulate data collection.

When **STAP_STREAM_EVENTS** is set to *N*, the parameter stops the agent TCP/IP data transmission process. The agent performs all data collection processes but does not send the audit record to the Guardium appliance.

Specifying multiple SMF data set masks

You can use the SMF_DSN_MASK keyword to specify up to nine additional SMF data set masks.

Specifying multiple SMF data set masks
The naming conventions of some environments prohibit the use of a SMF_DSN_MASK_1 value, which allows all required data sets to be read. To audit accesses to database-related data sets from multiple LPARS of your SYSPLEX, you can specify up to nine additional data set mask values: SMF_DSN_MASK_2 through SMF_DSN_MASK_10.

Disabling SMF auditing at the agent level

You can use the SMF_CYCLE_INTERVAL keyword to disable SMF auditing at the agent level.

For any IMS systems that are audited by this agent, you can disable audit access to IMS data sets that occur outside the use of IMS services. To do so, specify the following keyword with the value of zero: SMF_CYCLE_INTERVAL(0)

Specifying SMF_CYCLE_INTERVAL(0) turns off auditing process that uses SMF records. The agent address space (AUIA*STC*) will not start the SMF auditing address space (AUIF*STC*).

Controlling the frequency of SMF z/OS catalog queries

You can change the frequency of SMF z/OS catalog queries by using the SMF_CYCLE_INTERVAL keyword to specify a value in minutes:

To determine if any new, unread data sets match the specified SMF_DSN_MASK_x values, the SMF processing address space (AUIF*STC*) periodically performs a query against the z/OS catalog, looking for data sets to process. By default, this query is performed when the AUIF*STC* task is started, and repeated every 300 minutes (5 hours). To change the default time value, use the keyword SMF_CYCLE_INTERVAL*(time in minutes)*. If you specify a time value of zero, the SMF auditing feature will be disabled.

Changing the retention period of incomplete SMF events

By default, incomplete SMF events will be retained in your SMF spill data set for 5 days. You can change this time range by specifying the SMF_EVENT_EXPIRY keyword:

In some situations, such as a canceled job or end-of-memory events, a type 30 record is not produced for a step or job. To keep these types of records from filling your SMF spill data set, you can set a time limit in days to determine how long incomplete SMF records are retained. The default value is 5 days and can be changed by specifying the SMF_EVENT_EXPIRY keyword to indicate the number of days of your choice: SMF_EVENT_EXPIRY*(number of days).*

Changing the name of the SMF address space JCL

To change the name of the AUIF*STC* JCL member name, use the SMF_PROC_NAME keyword to change AUIFSTC to a name of your choice:

AUIF*STC* is the name of the JCL that provides auditing of data set accesses using SMF records. AUIF*STC* is provided in the product installation sample data set (SAUISAMP). If the name AUIF*STC* conflicts with your site's naming convention standards, or if more than one agent is being used, you can change the name of this JCL. Use the SMF_PROC_NAME keyword to change the member name from AUIF*STC* to a name of your choice: SMF_PROC_NAME*(new name)*.

Ensure that this JCL resides in a procedure data set (PROCLIB) that allows the z/OS START command **S taskname** to be used.

Auditing IMS data set access

To obtain a report of IMS artifact access, use the SMF_SELF_AUDIT keyword.

IBM Guardium S-TAP for IMS reads the IMS RECON data sets and system log data sets produced by IMS (SLDS) to obtain IMS environment information, such as IMS artifact names. IMS artifact names determine the databases and data sets that are used to create audit information.

By default, IBM Guardium S-TAP for IMS does not report accesses of IMS artifacts. To obtain a report of these accesses, specify a value of Y using the SMF_SELF_AUDIT keyword: SMF_SELF_AUDIT*(Y)*.

Changing the types of events that are audited using SMF records

Use the SMF_AUDIT_LEVELS keyword to indicate a list of events to be audited, instead of collecting all event types.

When auditing using SMF records is enabled, the default action is to provide auditing for all of the following accesses to data sets:

- Open events with READ access
- Open events with UPDATE/WRITE access
- Open events with ALTER access
- Data set DELETE events
- Data set CREATE events
- Access denied (RACF violation)

To specify some and not all of these events for auditing, you can specify each type of event to be audited by using the SMF_AUDIT_LEVELS keyword: SMF_AUDIT_LEVELS (*ALL*|*READ*|*UPDATE*|*DELETE*|*CREATE*|*ALTER*|*RACF*).

Remember: This keyword affects the SMF auditing level for all IMS subsystems controlled by this agent. If you do not include READ accesses in the SMF_AUDIT_LEVELS parameter, then no READ accesses will be reported for any of the IMS environments that are audited by using the agent.

Note: You can separate parameters for the collection of different event types. For example, to audit UPDATE and READ events, include the UPDATE and READ records as follows:

```
SMF_AUDIT_LEVELS(UPDATE)
SMF_AUDIT_LEVELS(READ)
```

instead of:

```
SMF_AUDIT_LEVELS(UPDATE|READ)
```

Using alternate RECON data sets for SMF and SLDS processing

You can optionally use copies of the IMS RECON data sets when processing SMF (AUIF*STC*) and IMS SLDS (AUIL*STC*) data instead of using the live RECON data sets.

To use alternate RECON data sets for SMF and SLDS processing:

1. Add a //AUIARCN DD statement to the AUIF*STC* and AUIL*STC* JCLs that contain the name of the IMS system (as defined in the **IMS Definition** panel of the Guardium interface).
2. Add the alternate RECON data set names to be used when processing these two types of data sources.

   Note: Specifying alternate RECON data set names only affects AUIF*STC* and AUIL*STC* task processing. It has no effect on processing of any other tasks.

Use IDCAMS, or another VSAM-compatible method, to create cataloged, VSAM copies of your live RECON data sets.

The data set that is specified by the AUIARCN DD statement must be defined as Fixed Block (FB) with a record length of 80 bytes (LRECL=80), and it can be a PDS, PDS/E, or sequential file. The following guidelines apply:

- An asterisk (*) in column 1 indicates that the line is a comment.
- Keywords must start in column 1.
- No spaces are allowed within keywords and parameters.
- Multiple IMSNAME keywords can be specified in one AUIARCN file.
- At least one RECON data set must be included under each IMSNAME identifier.
- Alternate RECON data sets must be cataloged and in IMS format.

Table 6. IMSNAME and RECON data set values, defined:

Value	Purpose
IMSNAME=	Specifies the IMS to which the subsequent RECON1, 2, and 3 keywords pertain.
RECON1=	Specifies the alternate data set name to be used for RECON1.
RECON2=	Specifies the alternate data set name to be used for RECON2.
RECON3=	Specifies the alternate data set name to be used for RECON3.

Example:

```
IMSNAME=IMSV14
RECON1=IMSEA1.ALT.RECON1
RECON2=IMSEA1.ALT.RECON2
RECON3=IMSEA1.ALT.RECON3
*
IMSNAME=IMSV13
RECON1=IMSDA1.ALT.RECON1
RECON2=IMSDA1.ALT.RECON2
```

Overriding the range of ports used for communication between address spaces

You can set the available port scan starting point and limit the number of ports to check for availability.

IBM Guardium S-TAP for IMS uses a communications port to pass messages between threads within each address space. The default port is 41500. If the address space determines that port 41500 is not available for use, all subsequent ports up to 65535 are examined, and the first available port is used.

Some installations have restrictions on which ports should be examined and used. Use the LOG_PORT_SCAN _START and LOG_PORT_SCAN_COUNT keywords to set the available port scan starting point and limit the number of ports to be checked for availability:

- LOG_PORT_SCAN_START(41501)
- LOG_PORT_SCAN_COUNT(24003)

The sum of the value of the SCAN_START port number plus the SCAN_COUNT should not exceed 65535.

Overriding the TCP/IP DNS resolver table

IBM Guardium S-TAP for IMS uses TCP/IP as a host path for intra- and inter-address space communication of information such as collection policy details and address space status updates. To receive information from an AUIU*STC*_(Common Storage Management Utility) address space running on a different LPAR in the sysplex, the AUIA*STC*_(agent) address space must determine its own physical IP address and make it known to AUIU*STC*.

To determine its physical IP address, the IBM Guardium S-TAP for IMS agent uses the z/OS getaddrinfo function and passes it to the LPAR name specified in the CVTSNAME field of the z/OS CVT control block. The getaddrinfo function uses the DNS resolver table to map the agent's LPAR name to its physical IP address. The DNS resolver table should contain entries that associate each LPAR within the sysplex to its physical IP address. If there is no association found, the agent (AUIA*STC*) uses the z/OS gethostname and getaddrinfo services to obtain the physical IP address of its own LPAR; but the IP addresses of other LPARs in the sysplex cannot be determined. In that case, inter-address space communication is not possible and events that occur on other LPARs are not reported to the Guardium appliance. Similarly, inter-address space communications can fail if users of Dynamic Virtual IP Addressing (VIPA) attempt to associate multiple IP addresses to a single VIPA token.

To determine if the LPAR name, in the CVTSNAME field, is included in the DNS table:

1. Run the Rexx executable that is located in the SAUISAMP data set of member AUIPING.
2. If the ping is successful, the LPAR name is defined in the DNS table and no further action is required.
3. If the ping fails due to an unknown host error, the LPAR name was not found in the DNS table. Contact your network administrator to request the addition of the LPAR name and the associated IP address to the DNS table.

Network administrators can manually associate the LPAR name that is found in the z/OS CVTSNAME field with the name that is used in the DNS revolver table by including the AUIHOST DD statement file in all IMS S-TAP agent task address space JCLs.

***cvts_lpar_name*(*dns_name*)**
Required if AUIHOST DD is specified.

Default: None.

Description: Translates the CVTSNAME to the name in the DNS table.

lpar_name
Found in the z/OS CVTSNAME field.

Use the AUIPING REXX exec found in the SAUISAMP data set to obtain that name.

The *lpar_name* value can be from 1 -- 8 bytes in length.

dns_name
Found in the DNS table that associates the LPAR with an IP address.

The DNS_NAME value must conform to the following z/OS TCP/IP HOSTNAME rules:

- Must contain 1 or more tokens separated by a period.
- Each token must be at least 1 character and less than 64 characters.
- Each token must start with a letter or number.
- Remaining characters in each token must be a letter, number, or hyphen.

Example: PRODA(SYSTEM_1)

wherein:

- *PRODA* is the LPAR name found in the CVTSNAME field of your z/OS system
- *SYSTEM_1* is the mnemonic used in your DNS table to relate this LPAR to a TCP/IP address.

The AUIHOST DD statement file must meet the following standards:

- It must be a sequential file, or a member of a Partitioned Data Set (PDS) or Extended Partitioned Data Set (PDSE).
- It must be defined with a Fixed Blocked (FB) Record Format (RECFM).
- It must have a Logical Record Length (LRECL) of 80 bytes.
- Commented lines can be indicated by an asterisk (*) in column one or by a slash-asterisk (/*) in columns one and two.
- It must contain all host definitions on one line.
- Up to 16 DNS names can be specified.

The following is an example of an AUIHOST DD statement file:

```
MYLPAR20(MYLPAR20.mycompany.com)
MYLPAR21(MYLPAR21.mycompany.com)
MYLPAR22(MYLPAR22.mycompany.com)
MYLPAR23(MYLPAR23.mycompany.com)
MYLPAR24(MYLPAR24.mycompany.com)
MYLPAR25(MYLPAR25.mycompany.com)
MYLPAR26(MYLPAR26.mycompany.com)
```

Specifying agent messages to issue to the operator console

You can use the WTO_MSG keyword to specify the messages to issue to the operator console.

IBM Guardium S-TAP for IMS allows you to specify informational, warning, or error messages to be written to the operator console. This allows an automated operations product to take some predefined action or provide a higher level of operator visibility to these messages. You can use the WTO_MSG to specify which messages should be write-to-operated.

- WTO_MSG(AUIF507E)
- WTO_MSG(AUIT013I)

You can specify one message ID per WTO_MSG instance. Messages originating from the AUIA*STC*, AUIF*STC*, AUIL*STC*, and AUIU*STC* address spaces are supported.

Creating a spill area for short-term outages

Use the OUTAGE_SPILL_AREA_SIZE keyword and parameter to indicate the size in megabytes to allocate for the spill area.

Short-term communication outages between the agent address spaces and the IBM Guardium system can be handled by using a z/OS data space spill area. Use of the spill area can prevent the loss of audited data by allowing the z/OS agent to save audited data until the connection to the IBM Guardium system is restored. The restoration of the communications link results in the flushing of the data space contents to the IBM Guardium system.

Use the OUTAGE_SPILL_AREA_SIZE keyword and parameter to indicate the size in megabytes to allocate for the spill area: OUTAGE_SPILL_AREA_SIZE*(megabytes).* If you specify zero or omit this keyword, the spill area will not be allocated or used. The maximum value you can specify is 1024 MB.

Disabling IMS SLDS auditing at the agent level

You can turn off the auditing process that uses IMS SLDS records by specifying the IMSL_CYCLE_INTERVAL keyword with a value of zero.

For any IMS systems to be audited by this agent, you can disable audit events that are determined by reading IMS System Log Data Sets (SLDS). To disable the auditing process that uses IMS SLDS records, specify the following keyword with the value of zero: IMSL_CYCLE_INTERVAL*(0)*. The agent address space (AUIA*STC*) will not start the IMS SLDS auditing address space (AUIL*STC*).

Controlling the frequency with which IMS System Log Data Sets are allocated and read

You can specify the frequency of IMS RECON data set queries by specifying the IMSL_CYCLE_INTERVAL keyword.

For the product to determine if any new, unread IMS System Log Data Sets LDS data sets have been created by the IMS Online system, the IMSL processing address space (AUIL*STC*) periodically performs a query against the IMS RECON data sets, looking for new SLDS. This query is performed when the AUIL*STC* task is started, and then by default, every 15 minutes. The frequency can be changed by providing a value in minutes by using the IMSL_CYCLE_INTERVAL keyword: IMSL_CYCLE_INTERVAL*(time in minutes)*

A value of zero will cause the IMS SLDS auditing feature to be disabled.

Changing the name of the IMSL address space JCL

To change the JCL member name AUIL*STC*, use the IMSL_PROC_NAME keyword.

AUIL*STC* is the name of the JCL that is used to audit data sets using IMS SLDS records. AUIL*STC* is provided in the product installation sample data set (SAUISAMP). If this name conflicts with your site's naming convention standards, or if more than one agent is being used, you can change the name of this JCL.

Use the IMSL_PROC_NAME keyword to change the member name from AUIL*STC* to a name of your choice: IMSL_PROC_NAME*(new name)*

Ensure that this new JCL is in a procedure data set (PROCLIB) that allows the z/OS START command **S taskname** to be used.

Changing the types of events audited using IMS SLDS records

To audit some, instead of all event types, you can specify each event type to be audited by using the IMSL_AUDIT_LEVELS keyword.

When you enable auditing by using IMS SLDS records, the default is to provide auditing for all of the following event types:

- IMS Online region starts and stops
- Users sign on/sign off
- Database Opens and Closes
- PSB|DBD start, stop, lock, unlock, and DBDDUMP

To audit only some of these events, you can specify each event type to be audited using the IMSL_AUDIT_LEVELS keyword: IMSL_AUDIT_LEVELS (*ALL*|*CTL_STRT*|*USERS*|*DBOPN*|*DB_PSB*).

This keyword governs the IMS SLDS auditing level for all IMS subsystems that are controlled by this agent. For example, if user signon/signoff is not included in the IMSL_AUDIT_LEVELS parameter, then no

signon or signoff events will be reported from any of the IMS environments that are audited using the agent.

Note: You can separate parameters for the collection of different event types. For example, to audit CTL_STRT and DBOPN events, include the CTL_STRT and DBOPN records as follows:

```
IMSL_AUDIT_LEVELS(CTL_STRT)
IMSL_AUDIT_LEVELS(DBOPN)
```

instead of:

```
IMSL_AUDIT_LEVELS(CTL_STRT|DBOPN)
```

Changing the name of the Common Memory Management address space JCL

Use the AUIU_PROC_NAME keyword to change the member name from AUIU*STC* to a name of your choice.

AUIU*STC* is the name of the JCL that is used to build filtering criteria in E/CSA on all LPARS of the SYSPLEX. AUIU*STC* is provided in the product installation sample data set (SAUISAMP). If this name conflicts with your site's naming convention standards, or if more than one agent is being used, you can change the name of this JCL.

Use the AUIU_PROC_NAME keyword to change the member name from AUIU*STC* to a name of your choice: AUIU_PROC_NAME*(new name)*.

Ensure that this JCL resides in a procedure data set (PROCLIB) that allows the z/OS START command **S taskname** to be used.

Excluding DLI calls on specific LPARS from being audited

To stop the transmission of the AUIU*STC* address spaces to all LPARs, the AUIU_EXCLUDE_LPAR keyword can be used to exclude specific LPARS from the target list of eligible LPARS.

By default, the IBM Guardium S-TAP for IMS agent creates Common Memory Management address spaces (AUIU*STC*) on all LPAR members of a SYSPLEX. This allocates E/CSA memory, and inserts DLI call filtering criteria across all LPARS. A single agent monitors IMS control regions and DLI/DBB batch jobs running on any LPAR of the SYSPLEX.

If you do not want to transmit the AUIU*STC* address spaces to all LPARs, the AUIU_EXCLUDE_LPAR keyword can be used to exclude specific LPARS from the target list of eligible LPARS: AUIU_EXCLUDE_LPAR*(lpar1, lpar2...lpar9)*

The LPAR where the agent is running cannot be excluded. All other LPARS can be excluded by using the *ALL option in place of the LPAR name.

For example, AUIU_EXCLUDE_LPAR(*ALL).

Running more than one agent in a SYSPLEX

If two or more IMS agents are running on one SYSPLEX, use the ADS_SHM_ID and ADS_LISTENER_PORT keywords to differentiate the shared memory segment and port for each agent environment.

The agent address space (AUIA*STC*) and subordinate address spaces (AUIF*STC* and AUIL*STC*) communicate by using a shared memory segment and communications port. Multiple agents require multiple unique shared memory segments and port values to ensure correct inter-address space communications. If you need to have two or more IBM Guardium S-TAP for IMS agents available on one SYSPLEX, the following keywords provide a method of uniquely identifying the shared memory segment and port for each agent environment:

- ADS_SHM_ID(100010)
- ADS_LISTENER_PORT(16055)

Specification of the ADS_SHM_ID and ADS_LISTENER_PORT requires the addition of a //AUICONFG DD statement to the AUIF*STC* and AUIL*STC* address space JCLs. This DD statement should point to the same data set and member as the AUIA*STC* and AUIU*STC* JCLs for the agent, to ensure that communications between all participant address spaces use the correct memory object and ports.

See "Customizing the agent by using agent parameter keywords" on page 19 for complete descriptions of all valid parameters, including the ADS_SHM_ID and ADS_LISTENER_PORT keywords.

Restricting auditing to specific IMS systems when multiple IMS systems share RECON data sets

If multiple unrelated IMS systems share RECON data sets, and you want to audit only on one or more specific IMS systems, use the keyword **IMSNAME_EQ_IMSSSID(Y)** to isolate auditing to the desired IMS system.

The default option, **IMSNAME_EQ_IMSSSID(N)**, causes only the IMS RECON data sets to be used when IBM Guardium S-TAP for IMS attempts to find and match IMS systems to active audit policies.

Specifying **IMSNAME_EQ_IMSSSID(Y)** causes both the IMS RECON data sets, and the 8-byte IMS subsystem/DBCTL RSENAME to be used when IBM Guardium S-TAP for IMS attempts to find and match IMS systems to active audit policies.

Consider the following example:

RECON data sets A.B.C1/C2/C3 contain information for IMSA and IMSB. Auditing is only desired for IMSB. Policy **AUDIT_ALL** is installed by using IMS appliance definition *MY_IMS*, which references RECON data sets A.B.C1/C2/C3.

If subsystems IMSA and IMSB both use RECON data sets that are referenced by the policy, **AUDIT_ALL**, and associated with the IMS definition, *MY_IMS*, then both IMSA and IMSB are audited when the default, **IMSNAME_EQ_IMSSSID(N)**, is specified.

To restrict auditing to IMSB:

1. Specify **IMSNAME_EQ_IMSSSID(Y)** in the AUICONFG file.
2. Name the IMS definition in the appliance IMSB.
3. Relate policy **AUDIT_ALL** to IMSB.
4. Install the policy.

As a result, IMSB is audited with the criteria that is set in policy **AUDIT_ALL**, and IMSA is not audited.

Note: DLI batch jobs (DLI/DBB) might not be tightly associated with an IMSID, therefore IBM Guardium S-TAP for IMS will report on all DLI batch jobs that use the audited RECON data set. The **IMSNAME_EQ_IMSSID** parameter does not affect DLI/DBB batch job auditing.

Using the System z Integrated Information Processor (zIIP)

You can use the System z Integrated Information Processor (zIIP) when running IBM Guardium S-TAP for IMS Control region address space, and in the agent address space (AUIA*STC*). Use the ZIIP_AGENT_DLI keyword with the **Y** parameter to cause the agent to make a zIIP-enabled enclave SRB initialization attempt.

IMS control region

The following processes are moved to the zIIP in the IMS Online Control Region, pending redirection by the operating system:

- DLI call filtering
- IXGWRITE of audited DLI call data to the z/OS System Logger log stream

To use a zIIP in the IMS Online Control region, add a **//AUIZIIP DD DUMMY** to the IMS control region JCL.

Agent address space

The following processes are moved to the zIIP in the agent address space (AUIA*STC*), pending redirection by the operating system:

- IXGBROWSE read of audited data from the z/OS System Logger log streams for both Online and Batch DLI calls
- TCP/IP send of the data to the Guardium system

To use a zIIP in the agent address space, use the ZIIP_AGENT_DLI keyword with the **Y** parameter to the configuration file that is pointed to by the AUICONFG DD statement in the agent JCL (AUIA*STC*).

Using multiple Guardium systems

You can configure multiple Security Guardium systems for automatic failover. By configuring one or more backup systems, you ensure continuous auditing capability. This process is known as failover. You can also enable the streaming of audited data from one or more IBM Guardium S-TAP for IMS agents to up to 6 connected Security Guardium systems. This process is known as multistreaming.

Providing Guardium system failover

You can specify up to five additional Guardium systems to be connected to the agent by using the APPLIANCE_SERVER_FAILOVER_x keyword, where x = a digit between one and five.

The failover process

IBM Guardium S-TAP for IMS uses the concept of a single primary IBM Guardium system and multiple secondary backup systems.

- When a primary IBM Guardium system goes offline, the IBM Guardium S-TAP for IMS agent automatically establishes a connection to a secondary IBM Guardium system, and the audited data is sent to the secondary system.
- When a primary IBM Guardium system comes back online, the IBM Guardium S-TAP for IMS agent detects it, and reestablishes the connection to the primary IBM Guardium system and restarts, sending data to the primary system.

This allows the use of any IBM Guardium system as a short-term backup, while always attempting to use the primary system as the main data storage medium.

In the following example failover scenario, where none of the systems are online, the IBM Guardium S-TAP for IMS agent attempts to connect to the primary IBM Guardium system at a regular interval and follows the usual failover logic if the primary IBM Guardium system is offline. A connection is reestablished to any of the configured appliances as soon as one becomes available.

Enabling multiple system failover support

IBM Guardium S-TAP for IMS allows the specification of up to five additional IBM Guardium system to be connected to the agent. This feature provides failover protection, which allows the agent to continue to send audited data to one of a number of backup IBM Guardium system in the event of a communication failure with the primary system. You must use the APPLIANCE_SERVER keyword to enable this feature, because the IBM Guardium system that is referenced by this keyword is the primary connection. You can specify additional IBM Guardium system by using the APPLIANCE_SERVER_FAILOVER_x keyword, where x = a digit from 1 to 5.

- APPLIANCE_SERVER_FAILOVER_1(IP address 1)

- APPLIANCE_SERVER_FAILOVER_2(host name 2)
- APPLIANCE_SERVER_FAILOVER_3(IP address 3)
- APPLIANCE_SERVER_FAILOVER_4(IP address 4)
- APPLIANCE_SERVER_FAILOVER_5(host name 5)

Example failover scenario

Audit data flows to the primary IBM Guardium system, **A**.

The TCP/IP connection from the IBM Guardium S-TAP for IMS agent to the primary IBM Guardium system fails.

A connection is made to the secondary IBM Guardium system, **B**.

Audit data is now flowing to the secondary IBM Guardium system, **B**.

The TCP/IP connection from the IBM Guardium S-TAP for IMS agent to the primary IBM Guardium system is reestablished.

Audit data now flows to the primary IBM Guardium system, **A**.

The IBM Guardium S-TAP for IMS agent and IBM Guardium system **B** disconnect.

Streaming to multiple Guardium systems

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

IBM Guardium S-TAP for IMS sends events to a single appliance until a ping occurs, or the number of records that is specified by **MEGABUFFER_COUNT** is reached. Audited DLI events are distributed amongst additional appliances in a round-robin sequence.

To enable multistreaming, you must specify *MULTI_STREAM* when you configure the **APPLIANCE_SERVER_LIST** parameter. The **APPLIANCE_SERVER** and **APPLIANCE_SERVER_[MULTI_STREAM]_[1-5]** parameters 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.

Enabling multistream support

Use the **APPLIANCE_SERVER** keyword to enable multistream support. The IBM Guardium system that is referenced by the **APPLIANCE_SERVER** keyword is the primary connection, and it provides the policy used to match DLI events. You can specify additional appliances by using the **APPLIANCE_SERVER_MULTI_STREAM_***n* keyword, where *n* is a digit from 1 - 5.

Specify up to 5 additional IBM Guardium system IP addresses or host names. For example:

- APPLIANCE_SERVER_MULTI_STREAM_1(IP address 1)
- APPLIANCE_SERVER_MULTI_STREAM_2(host name 2)
- APPLIANCE_SERVER_MULTI_STREAM_3(IP address 3)
- APPLIANCE_SERVER_MULTI_STREAM_4(IP address 4)
- APPLIANCE_SERVER_MULTI_STREAM_5(host name 5)

Keeping connections active when HOT_FAILOVER is enabled

When the HOT_FAILOVER feature is enabled by setting the **APPLIANCE_SERVER_LIST** parameter to *HOT_FAILOVER*, connections for each connected Guardium appliance are kept active by pings. (The following connection types are kept active: DLIO, DLIB, SMF, IMSL, and MLOG.)

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.

Chapter 8. IBM Security Guardium S-TAP for IMS on z/OS agent reference information

The IBM Guardium S-TAP for IMS agent provides access to database and appliance services, in support of the product's remote clients. The agent also reads audited DLI events placed in the z/OS System Logger log streams by the IMS Online and DLI/DBB batch Data collectors and sends the DLI events to the IBM Guardium system using TCP/IP connections.

Sample library members

Use the following sample library members shipped with IBM Guardium S-TAP for IMS to install and configure the product.

Table 7. Sample library members

Member	Type	Description
AUIAPPEV	DBD source statements	DBD source statements, used to define the optional APP_EVENT DBD
AUIA*STC*	JCL	Primary agent address space JCL
AUICONFG	CONFIG	Configuration file containing only the minimum required keywords
AUICONFX	CONFIG	Configuration file containing all available keywords
AUICPMOD	JCL	JCL to copy utility programs from SAUILOAD to SAUIIMOD data set
AUIEMAC1	MACRO	Edit macro to facilitate changes to other sample library members
AUIF*STC*	JCL	SMF data collection address space JCL
AUIFUSPL	JCL	JCL to create the SMF incomplete event spill file for an agent
AUIL*STC*	JCL	IMS archived log data collection address space JCL
AUILSTR1	JCL	JCL to add CFRM structures for batch and online log streams to a CFRM policy
AUILSTR2	JCL	JCL to add batch and online log streams to your CFRM environment
AUILSTR3	JCL	JCL to add DASD-only log streams to your LOGR environment
AUIMIG10	JCL	JCL used to assist in the upgrade from V9.0 to V10.1.3
AUIMLOG	JCL	JCL used to read the IMS RECONS, detect missing logs, and send notification to the Guardium system
AUIPING	REXX EXEC	EXEC used to determine the LPAR name, as found in the CVTSNAME field, and issue a PING to determine if the LPAR name is in the network DNS table
AUISMFDF	JCL	JCL sample, showing the creation of a GDG file base for SMF data collection
AUISMFDP	JCL	JCL sample, showing the use of program IFASMFDP to filter SMF record types
AUITCPD	JCL	JCL used to generate a network diagnostic report
AUIU*STC*	JCL	Common storage management utility address space JCL

Agent environment

The agent must be running before you can use product functions related to the IMS subsystems monitored by that agent.

Important: Before the agent is started, system services should be started, and completely available for use. Examples of system services include JES, TCP/IP and the associated DNS RESOLVER, XCF, and the z/OS System Logger.

APF authorization

For security, the agent must be APF-authorized before it can be run.

Agent job output

The primary output of the agent job consists of log messages written to the AUILOG DD. These messages provide status information about the ongoing operation of the agent, and also record additional messages if errors occur.

In the event of exceptional conditions, additional messages might be written to the SYSOUT DD. If an abend occurs, dump information can be written to the CEEDUMP and SYSUDUMP DDs, if they are supplied. That information can be used in diagnosis by product support.

Stopping the agent

When running on z/OS, the agent accepts standard z/OS /MODIFY and /STOP commands. When stopping the agent, all secondary address spaces controlled by the agent will also receive a stop request.

Important: System services, such as but not limited to the following, should remain available for use until the agent has completed termination: JES, TCP/IP and associated DNS RESOLVER, XCF and the z/OS System Logger.

From SDSF (or anywhere else that you can issue commands), you can issue one of these commands to the agent:

/STOP agent-job-name
This is the recommended command to use to stop the agent. It initiates a graceful agent shutdown, which causes the agent to:

1. Wait for all existing requests to finish.
2. Exit.

/MODIFY agent-job-name,STOP
Performs the same function as the /STOP agent-job-name command.

/MODIFY agent-job-name,FORCE
This initiates an agent hard stop which causes the agent to:

1. Initiate hard cancels on all running threads.
2. Exit as soon as the threads exit.

Note: Use of the FORCE option can result in DUMP-producing ABENDS.

Starting and stopping the secondary address spaces

This topic describes the **/MODIFY** commands to start and stop the secondary address spaces.

Commands to start and stop the SMF data collector address space

When the agent address space is started, secondary address spaces under the control of the agent may also be started. These include the SMF data collector address space (SAUISAMP member AUIF*STC*) which collects events using SMF log data as input and sends the events to the Guardium appliance. One IMS Archive Log event Data collector (SAUISAMP member AUIL*STC*) is also started for each IMS with an active collection.

Note: The following commands should be used against the agent's primary address space.

- **/MODIFY <jobname>,START COLLECTOR SMF**
- **/MODIFY <jobname>,STOP COLLECTOR SMF**

Optionally, the STOP command may be used to stop the SMF address space:

- **/STOP <jobname>**

Commands to start and stop the IMS Archive Log Data collector

There is no z/OS command to start the address space because the IMS Archive Log data collector address space is specific to an IMS definition with an active collection. The AUIL*STC* address is started by the agent address space, or activation of a collection.

Stopping a specific AUIL*STC* address space requires the use of the **/STOP <jobname>.<token>** command. The <token> value to be used can be found during AUIL*STC* startup in the AGENT JOBLOG.

In the following example, AAAAAAAC is the token value:

```
/S AUILRS22.AAAAAAAC
```

Or, when viewing the AUIL*STC* task in TSO SDFS, the token is displayed as the STEPNAME.

Chapter 9. Data collection

The collection process involves the gathering of audit event data at run time. Specify various filtering criteria to capture all relevant events and limit the amount of data that is collected and stored.

IBM Guardium S-TAP for IMS gathers audited events from the following sources:

- IMS database DLI calls performed from within IMS Online Control regions and DLI/DBB batch jobs
- SMF records
- IMS Log records from IMS System Log Data Sets (SLDS).

A single policy containing selection criteria that indicates the events to be audited, is applied to each source.

IMS database DLI calls

IBM Guardium S-TAP for IMS can filter audit events generated by database DLI calls by the following call types: Read, Update, Insert, and Delete.

Note: Database DLI calls that do not result in a DBPCB status code of blanks, GA, or GK, are not audited unless the IMS policy indicates that one or more non-blank DLI codes should be reported. DLI calls performed using an IOPCB or TPPCB are not audited.

Database DLI calls issued from specific PSBs and user IDs can be included or excluded from auditing. PSB names and user IDs can be specified for auditing using fully qualified names, or by using wildcard characters.

Further filtering can be performed by including or excluding specific database and segment names. Wildcard support is available for both the database and segment name.

When auditing IMS DLI calls, you can obtain the concatenated key value of segments that are audited for all or specific database DLI calls, as well as the segment data for UPDATE, and INSERT calls. The segment data can also be obtained for READ and UPDATE calls where these calls are logically linked in the Guardium appliance to provide a before and after image of updated segments.

SMF records

IBM Guardium S-TAP for IMS allows the filtering of audit events generated by access methods outside of IMS DLI services, including z/OS access methods such as VSAM or QSAM requests generated from z/OS batch jobs or TSO.

Some IMS Database Batch Utilities access IMS databases using access methods other the IMS Database DLI calls. As a result, the source of auditing records for these batch jobs will be the SMF records produced.

These audit events are based on z/OS SMF records and are processed from within the AUIF*STC* agent subtask. Policy criteria input for SMF data auditing is the same as for IMS DLI calls, but because of the nature of the SMF data, it is used differently.

The following data is not relevant, and therefore not used:

- DLI calls types
- PSB names
- Segment names

Database names are relevant because SMF data is based on data set names (part of the process that converts a policy to a filter, examines the IMS RECON data sets for artifacts in the RECON which relate to the INCLUDED database). These artifacts include database data set names (DSG/AREA/ADS) and

database image copy data sets for each database data set. The AUIF*STC* tasks also audit other IMS related data sets.

By default, these data sets have been included because changes to these data sets can have an effect on data integrity:

- IMS RECON data sets
- Logging data sets generated by IMS DLI/DBB batch jobs
- SLDS/RLDS data sets
- IMS Online log data sets (OLDS)

It is possible to ignore the auditing of these data set types, as well as the database image copy data sets, by adding a DUMMY DD statement to the AUIF*STC* JCL.

This table lists the data sets and corresponding DD DUMMY statement to include in the AUIFSTC JCL if you want to exclude the auditing of each of these types.

Table 8. Data sets and DD DUMMY statements

Data set Type	**IMS RECONS**	**IMS LOGS**	**IMS OLDS**	**DB Image Copies**
DD NAME	AUINRCN	AUINLOG	AUINOLD	AUINICS

Specify filtering of SMF events at the agent level, using access type or security violation, with the use of the SMF_AUDIT_LEVELS keyword in the configuration file. The keyword is pointed to by the AUICONFG DD statement of the agent (AUIA*STC*) JCL. Data set accesses to be audited are:

- OPEN for Read/Update
- Data set Alter/Create/Delete
- Any security product (such as RACF) violations

The auditing of these accesses can be specified at the agent level (for example, all IMS systems defined to the agent), or at the IMS level. See the *Changing the type of events audited using SMF records* section for more details.

Records from IMS system log data sets (SLDS)

IBM Guardium S-TAP for IMS allows the filtering of audit events that are generated by IMS Online Control regions, which are logged to IMS log data sets and are processed from within the AUIL*STC* started task.

Policy criteria input for IMS Log data auditing is the same as for IMS DLI calls, but is used differently because of the nature of IMS log data:

- DLI calls types are not relevant and therefore not used.
- Segment names are not relevant and therefore not used.
- PSB names are checked only when relevant to the event being examined.
- User IDs are checked only when relevant to the event being examined.
- DBD names are checked only when relevant to the event being examined.

In addition to filtering performed using the policy criteria, you can further filter IMS log data by event types, using the Guardium user interface. Using the IMSL_AUDIT_LEVELS keyword, you can set specific events to be audited, including:

- IMS Control Region Starts and Stops
- USER signon and signoffs
- Database OPEN/CLOSE
- DBD and PSB STARTS/STOPS/LOCK/UNLOCK

Occurrences of the DB DBDUMP command can also be audited. Auditing of these events can be specified at the agent level (for example, all IMS systems defined to the agent), or at the IMS level (for example, only for a specific IMS system). For more information, see *Changing the types of events audited using IMS SLDS records*.

Filtering stages

Stage 0, Stage 1, and Stage 2 filtering is available for Collector Agent audit event collection when processing DLI calls.

Filtering occurs at one or more of the stages, 0, 1, and 2, depending on what fields are included in your filter. As many audit events as possible are filtered at the earliest possible stage (0, 1, or 2). You can control filtering performance by the fields you include in the rules for the active collection profile.

Stage 0 filtering

Stage 0 filtering occurs immediately after IMS executes the DLI call and it is determined that the call is a candidate for auditing, meaning one of the supported DLI call types and blanks, or another acceptable DLI status code, is returned.

IBM Guardium S-TAP for IMS checks for an active policy for the IMS subsystem and determines if any rules governed by the active policy require the auditing of the DLI call type. If no policy is active, or no rules require the auditing of the DLI call type, processing control is returned to the application program. This is the most efficient form of filtering and should be used when possible.

Consider this example, wherein an active policy contains three rules:

- One rule only addresses INSERT requests.
- The second rule only addresses DELETE requests.
- The third rule only addresses UPDATE requests.

In this example, the READ DLI call is performed, and returns a status code of blanks. Since IBM Guardium S-TAP for IMS determines that no rules in the policy can reference a READ, processing control returns to the application program.

If the event that the DLI call performed in the example was an INSERT request, Stage 1 filtering would be invoked.

Stage 1 filtering

Stage 1 filtering occurs through the use of USERID and PSB name values.

For Stage 1 filtering to occur, all rules of the active policy must contain identical USERID and PSB name values. Any inconsistencies in these values between rules prevents Stage 1 filtering from occurring.

Stage 1 filtering allows DLI calls that should be rejected, due to USERID or PSB name, to be excluded from the list of values to be audited. This can be due to the items not being included, or being intentionally excluded.

The determination that the USERID or PSB is causing the DLI call to be rejected is made by call to the Stage 2 compiled filters. The call to the Stage 2 complied filters is made when the USERID or PSB name of the current DLI call is not the same as the USERID or PSB name of the previous DLI call made in the same processing region.

In this example, the processing flow is demonstrated when discussing a BMP:

- The first DLI call is made and passes through Stage 0 processing.
- Stage 2 filtering is invoked, and it is determined that DLI calls from this USERID should not be audited. The DLI call is not audited, and control is returned to the application program.
- The next DLI call is made, and the USERID is the same as the previous DLI call in the region. The previous DLI call was not audited due to the USERID value, therefore this DLI call will not be audited.

- This process continues until the BMP STEP terminates with only one DLI call going through to Stage 2 filtering, and the remaining DLI calls are rejected during Stage 1 processing.

The same benefit can be seen with DLI and DBB batch jobs, because the USERID and PSB will not change during the execution step.

This process benefits online transactions and other processing threads where multiple DLI calls are performed from within a single unit-of-work, as well as when DLI calls are performed using **C** and **D** IMS command codes where multiple segments are affected by a single DLI call and auditing might be required on more than one segment within the hierarchical path.

Stage 2 filtering

Stage 2 filtering occurs through the use of a filtering program that is compiled at the time of policy installation, using the criteria specified in the policy.

All DLI calls that are not rejected by Stage 0 and Stage 1 filtering are processed by the compiled filter. The compiled filter determines if the DLI call is to be audited based on all the policy criteria including DBD and segment name.

If the DLI call is to be audited, additional information is returned by the compiled filter, such as if the segment data and concatenated key should be included in the audited data block.

Policy pushdown

This topic describes the policy pushdown process of mapping policies to an IBM Guardium S-TAP for IMS collection profile.

When the IBM Guardium S-TAP for IMS agent starts, it establishes a dedicated connection to the Guardium appliance for the reading of installed policies. Immediately after the connection is established, any installed policies are pushed down to the IBM Guardium S-TAP for IMS agent by the Guardium appliance. The Guardium appliance pushes down a full policy to all connected IBM Guardium S-TAP for IMS agents each time a policy is installed or uninstalled from the Guardium appliance.

Upon receipt of a policy, the IBM Guardium S-TAP for IMS agent compares the applicable rules with the existing collections, and performs a differential install.

Differential install
A differential install of the policy indicates that only policies that have been modified since the last install are acted upon.

The following processing occurs in the IBM Guardium S-TAP for IMS agent upon receipt of a policy:

- The new policy is compared to the currently active policy if the new policy contains one or more rules.
  - If the policies are identical, no further processing is required.
- If the new policy does not apply to this subsystem, processing continues without any changes.
  - If there is an active policy, the collection continues using it.
  - If no policy is active, none is started.

Chapter 10. Creating and modifying IMS definitions

An IMS definition establishes a connection from your Guardium system to the IMS environment that you want to audit. To create and modify IMS definitions from the Guardium system interface, the agent address space (AUIA*STC*) must have a preestablished connection to the Guardium system.

Navigating to the IMS Definitions panel

IMS definitions can be created, modified, and deleted from the IMS Definitions panel of the Guardium system interface.

Procedure

1. From the **Administration Console** tab, select the **Local Taps** menu.
2. Select the **IMS Definitions** option.

IMS Definition fields

The following fields are available in the **IMS Definitions** panel for your use in definition an IMS entry. Required fields are indicated with an asterisk.

IMS Name

***IMS Entry Name**
A unique 1 - 8 character name to identify this IMS entry.

Description
An optional description of the IMS Entry.

***Agent Name**
The name of the agent that audits this IMS entry.

RECONs

The RECON data set names are used to logically link the IMS definition, the active policy, the IMS Online Control region, and the DLI/DBB batch jobs that are running on z/OS, to audit the correct IMS instances.

***RECON1 Data Set Name**
The RECON1 data set name that is used by IMS on z/OS.

***RECON2 Data Set Name**
The RECON2 data set name that is used by IMS on z/OS.

RECON3 Data Set Name
The RECON3 data set name that is used by IMS on z/OS.

IMS Data Sets

The IMS RESLIB data sets are used to determine the IMS release, during processing of the IMS System Log Data Sets (SLDS), using the AUIL*STC* address space. If more than one data set name is required, the data set names can be delimited by a comma.

***RESLIB Data Set Names**
A data set containing the IMS DFSVC000 module.

AUII050I Message Frequency
Message AUII050I provides the number of DLI calls that are considered for auditing, and the number of DLI calls that were audited, based on the auditing criteria of the active policy. This message is produced based on the number of DLI calls that are considered, based on the following formula:

Number of DLI calls in thousands (K) or Millions (M)

or, by using both the formula and the time interval since the last AUII050I message was issued.

Example: If you provide values of 100K (Number of DLI calls = 100,000) and 0100 (time interval of 1 hour), message AUII050I is issued when 100,000 DLI calls are seen by the product code, or by the 1 hour time interval, whichever comes first. The DLI counts and time interval reset when message AUII050I is issued.

Number of DLI calls
xxx K|M

Time Interval
HH:MM

Auditing Levels
Auditing levels can be set for both IMS Log and SMF events. For an explanation of the levels of auditing that are available for IMS Log and SMF events, see Chapter 4, “Configuration overview,” on page 11 for a description of the IMSL_AUDIT_LEVELS and SMF_AUDIT_LEVELS configuration keywords.

IMS LOG Events
Audit All IMS Log Events

Audit Control Region Starts/Stops

Audit User Signon/Signoff

Audit DBD Open/Close

Audit DBD/PSB/DUMP/START/STOP/LOCK/UNLOCK

SMF Events
Audit All SMF Events

Audit Dataset Open for Update

Audit Dataset Deletes

Audit Dataset Open for Read

Audit Dataset Create

Audit Dataset Alter

Audit Dataset RACF Violations

IMSPLEX data sharing and XRF considerations

When you are considering IMS data sharing and XRF systems, take the following IMSPLEX data sharing and XRF considerations into account.

IMSPLEX Data Sharing Considerations

Regardless of the number of LPARS that are involved, only one IMS definition is required in an IMS data sharing environment where all databases are shared by multiple IMS subsystems.

In an IMS data sharing environment where only a subset of databases is shared, an IMS definition must be created for each IMS subsystem with nonshared databases to be audited.

XRF Considerations

Only one IMS definition is required in an IMS XRF environment. IBM Security Guardium S-TAP for IMS on z/OS is not sensitive to which XRF partner is currently active. The product continues to produce audit data in the event of an XRF ACTIVE/BACKUP switch.

Adding an IMS definition

Add an IMS definition to the **IMS Definitions List** to include a defined IMS environment in the list of environments to be audited.

Procedure

1. From the **IMS Definitions List**, select the **Add** symbol, indicated by a plus sign, to the list of defined IMS systems.

   Enter the information in the **IMS Definitions** panel to define the new IMS environment to be audited.
2. Select **Apply** to save the new IMS definition.

Modifying an IMS definition

You can modify the attributes that are set for an IMS definition on the **IMS Definitions List**.

Procedure

1. Select the entry that you want to modify.
2. Modify the IMS definition fields.
3. Select **Apply** to save your changes.

Deleting an IMS definition

Delete an IMS definition from the **IMS Definitions List** to remove the IMS entry from the list of IMS environments to be audited.

About this task

IMS definitions can be deleted if no active IMS policies reference the IMS definition name. Only IMS definitions that are not part of an installed policy can be deleted.

Procedure

1. From the **IMS Definitions List**, select the **IMS Definition** that you want to delete.
2. Click the **Delete** icon.

   Click **OK** in the confirmation message to confirm the IMS entry deletion.

Chapter 11. Reference information

This chapter provides IBM Guardium S-TAP for IMS reference information.

Data collection monitors

IBM Guardium S-TAP for IMS collects data from IMS online and batch activities, SMF, IMS archived logs, and IMS RECON data sets, by using the following internal product monitors.

IMS Online Activity Monitor

The IMS Online Activity Monitor interfaces with IMS DL/I Language call analyzer module (DFSDLA00), and the IMS/VS Fast-Path Inter-region Communications Controller module (DBFIRC10), in order to be sensitive to the DL/I call type, and to access the data that is necessary for producing an audited event. When an INIT call is made to the IMS logger Exit routine (DFSFLGX0), interfaces to the IMS modules are activated, and they remain active until the DFSFLGX0 routine receives a TERM notification.

For the activity monitor to be recognized by the IMS Online region, the IMS control region must be stopped and restarted with the SAUIIMOD data sets included as the first data sets in the STEPLIB DD concatenation.

The IMS Online Activity Monitor and the agent communicate data collection criteria by using E/CSA control blocks. Determination of which DL/I calls and databases/segments is made at the time the DL/I call is performed, by using information that is derived from the data collection policy that is created through the IBM Guardium system's Access Rule definition process.

The z/OS System Logger transports the audit data from the IMS Online Activity Monitor to the agent. All IMS online systems that are controlled by an agent use the same z/OS System Logger log stream. This z/OS system log stream is unique to the agent, and only contains audited events from IMS Online regions.

IMS Batch Activity Monitor

The IMS Batch Activity Monitor interfaces with IMS DL/I language call analyzer module (DFSDLA00) in order to identify the DL/I call type and data that is necessary to produce an audited event. When the IMS Batch Exit routine (DFSISVI0) is invoked, the interface with the DL/I call analyzer is activated, and remains active until the batch step terminates.

The IMS Batch Activity Monitor and the agent use E/CSA control blocks to communicate data collection criteria. The DLI calls and databases/segments determination is made at the time the DL/I call is performed, by using information that is derived from the data collection policy, which is created on the IBM Guardium system. The audit data from the IMS Batch Data Collector to the agent is transported through the z/OS System Logger.

All IMS batch jobs that are controlled by an agent use the same z/OS System Logger log stream. This z/OS system log stream is unique to the agent, and only contains audited events from IMS Batch jobs.

IMS Online and Batch Data Collectors

The IMS Online and Batch Data Collectors run as separate threads under the control of the agent address space (AUIA*STC*). The function of the data collector is to read audited events from the z/OS System Logger log stream, and send the events to the IBM Guardium system for storage by using a TCP/IP connection.

Each thread maintains its own persistent TCP/IP connection to the Guardium system.

SMF Data Collector

The SMF Data Collector reads a subset of SMF records from SMF memory dump data sets to determine whether data sets associated with audited IMS artifacts were read, written, deleted, or renamed. Security violations against these data sets can also be reported.

IMS artifact associated data set types include database data sets, database image copy data sets, IMS log data sets (OLDS, SLDS and RLDS), and RECON data sets. The list of IMS artifact data sets to

be monitored during SMF data collection is derived from the data collection policy that is created through the IBM Guardium system.

As the processing of the SMF data sets is deferred, the data collection policy in force at the time of the SMF data set READ is the collection policy used, not the data collection policy in effect when the SMF event occurred. The names of the SMF memory dump data sets to be read is based on one or more SMF data set MASK values that are supplied by the use of one or more SMF_DSN_MASK keywords in the agent configuration file (AUICONFG). The data set names to that the SMF MASK refers reflects the SMF memory dump data sets that are created during offloading of the SMF recording data sets, or a copy of these data sets containing a subset of SMF record types that are created explicitly for the use of this product.

Because an agent can monitor SMF events from all LPARS within a SYSPLEX, all SMF data sets to be read must be accessible from the LPAR on which the agent runs. The SMF Data Collector periodically queries the z/OS catalog for new data set names that meet the SMF MASK value. When cataloged data sets are found, these data sets are dynamically allocated and read by the SMF Data Collector. Auditable events that are found are formatted, and sent to the IBM Guardium system by using a TCP/IP connection.

The SMF Data Collector creates and maintains its own TCP/IP connection to the IBM Guardium system. The frequency that the SMF Data Collector queries the z/OS catalog is determined by the option you set during configuration of this product. The SMF Data Collector can be configured to audit only a subset of events by use of available options when configuring the agent and defining the IMS appliance through the Guardium system interface. The SMF Data Collector is run as a started task under the control of the agent. An example of the JCL for this started task can be found in the SAUISAMP data set in the AUIF*STC* member.

Note: IBM Guardium S-TAP for IMS only reports audited events for SMF record types that are collected by SMF. If specific SMF record types are not collected by your appliance or SMF recording data set memory dump utility, the event cannot be reported. Refer to the "IMS Log types and SMF record types that are collected by IBM Guardium S-TAP for IMS" on page 69 topic for a list of SMF record types that are used by IBM Guardium S-TAP for IMS.

IMS Archived Log Data Collector

The IMS Archived Log Data Collector reads IMS Archived Log data sets (SLDS) and provides audit information about the following actions:

- IMS user signon and signoff
- IMS online region starts and stops
- Changes to the status of DBDs and PSBS within the IMS Online environment

The list of IMS artifacts to be monitored during IMS Archived Log collection is derived from the data collection policy you create, by using the Guardium system.

As the processing of the IMS Archived Log sets is deferred, the data collection policy in force at the time that the IMS Archived Log data sets are read is the collection policy used (as opposed to the data collection policy in effect when the IMS Archived Log event as written to the IMS log data set).

The IMS Archived Log Collector periodically queries the DBRC RECON data sets that are associated with an IMS that is defined to IBM Guardium S-TAP for IMS to determine if new SLDS data sets were created since the last RECON data set query. New data sets that are found are dynamically allocated and read. Audited events are sent to the IBM Guardium system by using a TCP/IP connection.

The IMS Archive Log Data Collector can be configured to audit only a subset of events, by using the options available when configuring the agent and defining the IMS appliance through the Guardium system interface. The IMS Archived Log Data Collector is run as a started task under the control of the agent. An example of the JCL for this started task can be found in the SAUISAMP data set in the AUIL*STC* member.

IBM Guardium S-TAP for IMS starts one AUIL*STC* task for each set of RECON data sets that is actively monitored with a data collection policy.

- If an IMS data sharing environment with five IMS subsystems that share a single set of RECON data sets exists, only one AUIL*STC* task is started.

- If two separate IMS subsystems by using two separate sets of RECON data sets are being monitored, two separate AUIL*STC* tasks are started.

  Note: To collect events from the IMS archived logs, the DFSSLOGP (Primary Output SLDS) data set must be created and cataloged by your IMS Log Archive Utility process (program DFSUARC0).

IBM Guardium S-TAP for IMS dynamically starts and stops the appropriate number of AUIL*STC* tasks as required.

IMS Missing Log Utility

The IMS Missing Log Utility analyzes IMS RECON data sets to confirm the existence of SLDS/RLDS data sets. This function can be included or excluded, as well as scheduled without regard to the execution cycle setting for the AUIL*STC* task. This utility is run by a job or started task (see SAUISAMP member AUIMLOG for an example). It processes the RECON data sets of IMS systems with active policies audited by the agent and pointed to by the configuration member that is defined in the AUICONFG DD statement in the AUIMLOG JCL. The IMS RECON data sets are analyzed in search of IMS SLDS and RLDS data sets. If these are found, the z/OS appliance catalog is queried by using the SLDS/RLDS data set name. If the SLDS/RLDS data set is not found, a missing log event is sent to the IBM Guardium system.

Note: The AUIMLOG utility must be run under the same user ID, and on the same LPAR, as the AUIA*STC* task.

Common Storage Management Utility

IBM Guardium S-TAP for IMS uses memory in E/CSA to provide information regarding active data collection policies to the IMS Batch and Online Activity Monitors.

An IBM Guardium S-TAP for IMS agent can be called to monitor IMS Online regions or DL/I batch jobs on many LPARS within a SYSPLEX. A started task is generated for execution on all LPARS of a SYSPLEX to read all active data collection policies and build the appropriate E/CSA control blocks. This started task is run when the IBM Guardium S-TAP for IMS agent starts and stops, as well as when a change is made to the state of any collection policy. An example of the JCL for this started task can be found in the SAUISAMP data set in the AUIUSTC member.

The LPARs where the AUIU*STC* task is run might be limited by adding the AUIU_EXCLUDE_LPAR keyword and LPAR names to the configuration file, which is specified by the AUICONFG DD statement in the AUIA*STC* JCL.

IMS Log types and SMF record types that are collected by IBM Guardium S-TAP for IMS

The following tables show the IMS log types and SMF records types and descriptions that are collected by IBM Guardium S-TAP for IMS.

Table 9. IMS Logtypes collected by IBM Guardium S-TAP for IMS

Log type number	IMS log type	IMS log type description
06	IMS/VS Accounting Record X'06'	IMS Online was started or stopped.
16	A **/SIGN** command was successfully completed.	A **/SIGN** command successfully completed.
20	A database was opened.	A database was opened.
21	A database was closed.	A database was closed.
4C	DB/PSB Activity	Activity that is related to database or PSB processing
59xx	DEDB ADS OPEN Log record	DEDB area data set was opened.
5922	DEDB ADS CLOSE Log record	DEDB area data set was closed.

Table 9. IMS Logtypes collected by IBM Guardium S-TAP for IMS (continued)

Log type number	IMS log type	IMS log type description
5923	DEDB ADS STATUS Log record	DEDB area data set status was changed.

SMF is used to obtain additional data set activity that is related to the monitored IMS databases and image copies.

Table 10. SMF record types and descriptions

SMF record Number	Type
00	IPL record
14	INPUT or RDBACK data set activity
15	OUTPUT, UPDATE, INOUT, or OUTIN data set activity
17	Scratch data set status
18	Rename non-VSAM data set
30	Common address space work, accounting information
60	VSAM volume data set updated
61	ICF catalog entry define
62	VSAM component or cluster opened
65	ICF delete activity
66	ICF alter activity
80	RACF operator record
89	Usage data

Note: When image copies are read, they are collected as SMF type 14. When image copies are written, they are collected as SMF type 15. Image copies are sequential files, with some exceptions. If the image copy is opened as a VSAM file, the image copy is collected as SMF type 60.

Remember: IBM Guardium S-TAP for IMS can only report events that are being collected by SMF. If an SMF record type in this table is not being collected at your site, IBM Guardium S-TAP for IMS cannot report that event.

Fields that are used for IMS policy pushdown

The following fields defined in the Guardium system **Access Rule Definition** panel are used by IBM Guardium S-TAP for IMS to create policies and rules. Use the following information as a guideline.

Table 11. Fields that are used for IMS Policy pushdown

Label	Hover text
Service Name	IMS names to which this rule applies (case sensitive)
Application User	INCLUDE/PSB or EXCLUDE/PSB
Database User	INCLUDE/USERID or EXCLUDE/USERID
Object	INCLUDE/read+update+delete+insert+data+image/DBNAME.SEGNAME or EXCLUDE/DBDNAME.SEGNAME

Service name/IMS name
Required.

Must be 1 -- 8 characters.

Mixed case is allowed, and field is case sensitive.

Wildcard characters are not allowed.

Application user/PSB
Must be 1 -- 8 characters.

All typed characters should be folded to uppercase.

Supports % as a wildcard character. % matches zero or more characters.

Note: If the keyword EXCLUDE is used, at least one INCLUDE must also be specified.

Database user/User ID
Must be 1 -- 8 characters.

All typed characters should be folded to uppercase.

Supports % as a wildcard character. % matches zero or more characters.

Note: If the keyword EXCLUDE is used, at least one INCLUDE must also be specified.

Object/Target DB/Segment
database_name must be 1 -- 8 characters.

segment_name must be 1 -- 8 characters.

wildcard_pattern supports % as a wildcard character. % matches zero or more characters.

All typed characters should be folded to uppercase.

Note: You must specify at least one INCLUDE with at least one DLI call type. DBD and segment must also be specified.

DLI Call Code
Used to generate audit records for DLI calls that result in a non-blank status codes. Non-blank status codes can indicate that the DLI call failed or completed with a warning.

The following DLI status codes can be audited:

- FD
- FW
- GA
- GB
- GD
- GE
- GK
- L2
- LB
- LS
- NI
- UC
- US
- UX

You can specify one or more DLI status codes.

For more information about DLI status codes, see the About DLI status codes information in the IBM Knowledge Center.

Audit
Used to limit the types of DLI calls to be audited.

NOHLVL causes audit information to be collected for only the target segment of a DLI Patch call (Command code C or D) instead of generating audit data for each segment of the hierarchical path. This can reduce the volume of audited data that is sent to, and stored by, the Guardium appliance in cases where the target segment concatenated key is sufficient for auditing purposes.

LTERM Filtering

Must be 1 -- 8 characters.

All typed characters should be folded to uppercase.

Supports % as a wildcard character. % matches zero or more characters.

Note: If the keyword EXCLUDE is used, at least one INCLUDE must also be specified.

By default, auditing is considered for any DLI call that has a blank/null LTERM (for example, from a BMP or other region type that does not present IMS with an LTERM value). When an LTERM value or a group of LTERMs is specified, an option box is presented to enable you to turn off BLANK LTERM auditing. Turning off BLANK LTERM auditing does not affect the auditing of BMPs; any other region types without an LTERM value are excluded from auditing.

Filtering DLI calls from specific IMS Region types

You can filter out DLI calls from specific IMS Region types. DLI calls that originate from one or more of these region types can be excluded from auditing consideration:

- AER
- BMP
- CICS
- DBCTL
- IFP
- MPP
- ODB

In the Guardium interface, click the pencil icon alongside the **Region Types to Exclude** field to open a set of check-boxes that enable you to remove regions from auditing

Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

This section details the process of sizing the z/OS System Logger Log Streams. The z/OS System Logger Log Stream is used to transport audited DLI call data from the IMS control region or DLI/DBB batch jobs to the IBM Guardium S-TAP for IMS agent (AUIAxxxx address space) where it is reformatted to a PROTOBUF protocol and sent to the target Guardium appliance.

Calculating the Optimal Log Stream Size

Filtering by using the IMS POLICY from the Guardium appliance occurs in the IMS Control region, therefore only DLI calls that are to be audited are written to the log stream(s).

For most users, the size of the log stream that is provided with the **LS_SIZE** parameter of the AUILSTR2/3 log stream definition member (LS_SIZE(100)) is appropriate to use when auditing accesses to sensitive data or when auditing DLI calls performed by a group, or groups, of users who have access to all databases for diagnostic purposes.

There might be instances where an **LS_SIZE** parameter value of 13500 (LS_SIZE(13500)) might be used, such as:

- during product testing, or
- when the number of audited DLI calls exceed twenty-five thousand DLI calls per second, or
- when the audited DLI calls include large concatenated key or large segment fields, which can occur when the IMS POLICY includes the +DATA keyword in the TARGET/DB INCLUDE filter statement

Note: Log stream sizing can be an iterative process. When attempting to audit many DLI calls, the CPU, memory, and disk storage capacity of the Guardium appliance should be considered.

Considerations

There are several variables that must be considered when sizing the log stream(s), including:

- the number of IXGWRITEs that are performed every second
- the average number of bytes written, or average buffer size written with each IXGWRITE calls
- the rate that the data is offloaded from the log stream
- the number/rate of IXGDELETEs that are performed

The average number of IXGWRITEs that are performed and the average number of bytes/average buffer size is determined by the volume of audited DLI calls and the size of the DLI call event data that is being captured.

IBM Guardium S-TAP for IMS uses a set of 35K buffers to hold the audited DLI call data. Each buffer is written to the log stream when it fills to capacity, or every five seconds. The time interval is used to ensure that audited DLI call data is sent to the Guardium appliance in a timely manner. Therefore, the frequency of IXGWRITEs can vary greatly depending on the IMS Policy and databases that are being accessed.

The log stream offload process IBM Guardium S-TAP for IMSis performed by the agent address space (AUIAxxxx). The agent address space constantly polls the log stream (once per second) looking for new data to process. When new data is found, the data is read by using the IXGBRWSE call. The data is formatted into a PROTOBUF protocol and sent to the Guardium appliance by using TCP/IP. The IBM Guardium S-TAP for IMS agent will continually read and process log stream data until no new data exists, at which time, polling every second will reoccur.

The log stream data is deleted by using the IXGDELETE call after every three blocks of data are successfully read and sent to the Guardium appliance. This ensures that audited data is not lost in the event of a communication loss between the IBM Guardium S-TAP for IMS agent and the Guardium appliance.

Using IBM Documentation

The System Logger Performance and Tuning section of the System Programmer's Guide to: z/OS System Logger provides a detailed description of the processes that are needed to tune the System Logger for use with IBM Guardium S-TAP for IMS and other products.

You can perform an analysis of the performance and efficiency of the initial log stream size by running program **`IBM program IXGRPT1`** and **`JCL IXGRPT2`** found in 'SYS1.PROCLIB'. This program uses the SMF88 records to help with log stream capacity planning.

SMF88 records can be collected by z/OS by providing the 88 value in the SMPRM parmlib member prior to a system IPL, or by using the z/OS command, "SET SMF=xx" (where xx is the suffix of the parmlib member).

Example:

```
SYS(TYPE(30,70:79,88,89,100,101,110)),
```

The IXGRPT1 utility will assemble sub-routine IXGRA1 and compile and link program IXGRPT1, which can be used to extract SMP88 records in preparation for analysis.

The IXGRPT2 JCL can be used to produce other SMP88/log stream reports.

Pertinent Report Fields

Some key fields provided in the System Logger Activity Report (IXGRPT1) are the BYT WRITTN TO INTERIM STORAGE, BYT WRITTN TO DASD, and STRUC FULL.

BYT WRITTN TO INTERIM STORAGE

The BYT WRITTN TO INTERIM STORAGE value (bytes written to interim storage) indicates the amount of data being written to the log stream during the SMP interval. This value can provide insight as to the volume of data being written to the log stream.

BYT WRITTN TO DASD

The BYT WRITTN to DASD value (bytes written to DASD offload data sets) indicates the number of bytes that were written to the DASD offload/overflow VSAM data sets.

This number indicates that the interim storage filled up, and in order to retain the data, a set of VSAM files are being used as overflow buffers. This number can rise and fall during the day as the volume of audited DLI calls increase and decrease.

Some use of the overflow VSAM files can be acceptable because spikes in audited DLI call data can certainly be expected due to the nature of IMS POLICY filtering. However, constant or extensive use of the VSAM overflow files indicate that the log stream should be sized larger.

STRC FULL

The STRC FULL (Structure Full) value indicates the number of times that the capacity of the CF structure was filled up without an offload occurring. This number should be zero in a properly sized log stream. Structure such as this can indicate that the volume of data written exceeds the offload capability of the IMS STAP agent to read, process, and delete audited data, and a larger structure size should be considered.

An abundance of Structure Full conditions will result in a degradation of performance when collecting audited DLI call data, and if not rectified, might result in data loss. This condition might result in IXGWRITE 0866 errors being issued in the IMS Control region address space.

Additional Resources

IBM provides a spreadsheet utility to assist in the analysis of the log stream SMF88 data and provide suggestions on how to define the log stream for more efficient use in your environment.

You can access the spreadsheet utility with the following link: ftp://www.redbooks.ibm.com/redbooks/SG246898. Read the `disclaimer.txt` file before using the tool.

Echoed XML statement definitions

IBM Guardium S-TAP for IMS echoes the XML statements that are produced by the Guardium appliance to represent an Audit Policy. These statements are issued to a physical data set, agent AUILOG DD, or both, as determined by the **`XML_ECHO_DATASET`** and **`XML_ECHO_AUILOG`** parameters. This topic provides definitions of all XML statements that could be echoed from the appliance by the S-TAP.

XML convention

Start of tag data
=<tag_name>

End of tag data
=</tag_name>

Null/empty tag
=<tag_name/>

See Sample XML file for an example of the XML representation of a valid policy.

IMS-specific statements

Table 12. IMS-specific XML statements

XML statement	Definition
<install-info>	Beginning of relevant policy information.
<artifacts>	Start of IMS definitions.
<ims>	Start of individual IMS-specific information.
<name>	Name of IMS as specified in the Guardium appliance policy.
<agent>	Name of the agent to which IMS is connected.
<description>	Appliance IMS description text.
<version>	Currently a value of zero (0).
<plexname>	Not populated.
<recons>	Start of the IMS-specific RECON data set list.
<recon seq="1">	RECON1 data set name. DSN terminated by </recon>.
<recon seq="2">	RECON2 data set name. DSN terminated by </recon>.
<recon seq="3">	RECON3 data set name. DSN terminated by </recon>.
<reslibs>	Start of IMS-specific RESLIB data sets.
<reslib seq="1">	RESLIB 1 in IMS STEPLIB concatenation. DSN terminated by </reslib>.

Log-specific statements

Table 13. Log-specific XML statements

XML statement	Definition
<dbdlibs/>	Not populated.
<psblibs/>	Not populated.
<thresholds-050i>	Start of message AUII050I message frequency parameters.
<max-count>	Number of DLI calls needed to prompt message AUII050I.
<max-time>	Max time interval (HHMM) between AUII050I messages.
<audit-levels>	Start of IMS Logger and SMF auditing criteria.
<collector name="ims">	Start of IMS Logger auditing criteria. Terminated by </collector>.
<audit-level>	Start of audit level criteria.
<signon-signoff value="true"/>	Audit IMS user sign-ons and sign-offs.
<signon-signoff value="false"/>	Do not audit IMS user sign-ons and sign-offs.
<start-stop value="true"/>	Audit IMS Control Region starts and stops.
<start-stop value="false"/>	Do not audit IMS Control Region starts and stops.
<db-open-close value "true"/>	Audit DBD Opens and Closes.
<db-open-close value "false"/>	Do not audit DBD Opens and Closes.

Table 13. Log-specific XML statements (continued)	
XML statement	**Definition**
<dbd-psb value="true/"	Audit DBD/PSB/Dump/Start/Stop/Lock/Unlock
<dbd-psb value="false/"	Audit DBD/PSB/Dump/Start/Stop/Lock/Unlock

SMF-specific statements

Table 14. SMF-specific XML statements	
XML statement	**Definition**
<collector name="smf">	Start of SMF auditing criteria. Terminated by </collector>.
<audit-level>	Start of audit-level criteria.
<read value="true"/>	Audit data sets when they are opened with READ intent.
<read value="false"/>	Do not audit data sets when they are opened with READ intent.
<update value="true"/>	Audit data sets when opened with UPDATE intent.
<update value="false"/>	Do not audit data sets when opened with UPDATE intent.
<delete value="true"/>	Audit data set DELETEs.
<delete value="false"/>	Do not audit data set DELETEs.
<create value="true"/>	Audit data set CREATEs.
<create value="false"/>	Do not audit data set CREATEs.
<alter value="true"/>	Audit VSAM data set ALTERs.
<alter value="false"/>	Do not audit VSAM data set ALTERs.
<racf-violations value "true"/>	Audit RACF security violations against data sets.
<racf-violations value "false"/>	Do not audit RACF security violations against data sets.

Policy-specific statements

Table 15. Policy-specific XML statements	
XML statement	**Definition**
<policies>	Start of policy information.
<collection-profile>	Displays the rules defined to the policy. The collection profile policy name appears in the collection-specific statement <collection> for a given <ims>.
<name>	Policy name. Naming convention is: *policy_IMS_name*.
<description>	Concatenation of descriptions of all policies pushed to the appliance.
<rules>	Start of individual policy rules.
<rule>	Start of rule instance.
<active>	Always a value of true.
<filters>	Start of PSB/USERID/LTERM INCLUDES/EXCLUDES within the rule.
<psb-filter>	PSB instance.

Table 15. Policy-specific XML statements (continued)	
XML statement	**Definition**
<name>	Name of PSB to be audited or ignored.
<type>	Value will be INCLUDE (audit) or EXCLUDE (ignore).
<lterm-filter>	LTERM instance.
<name>	LTERM to be audited or ignored.
<type>	Value will be INCLUDE (audit) or EXCLUDE (ignore).

Database/segment-specific statements

Table 16. Database/segment-specific XML statements	
XML statement	**Definition**
<targets>	Start of DBD/SEGMENT instances within the rule.
<segment-target>	Start of list of databases/segments to be INCLUDED/EXCLUDED.
<type>	Value will be INCLUDE (audit) or EXCLUDE (ignore).
<database-name>	Database to be audited or ignored.
<segment-name>	Segment to be audited or ignored.
<audit-get>	INCLUDE DLI GET calls.
<audit-insert>	INCLUDE DLI INSERT calls.
<audit-update>	INCLUDE DLI UPDATE (REPL) calls.
<audit-delete>	INCLUDE DLI DELETE (DLET) calls.
<capture-before-image>	INCLUDE link between DLI GH and DLI REPL calls.
<capture-segment-data>	INCLUDE segment data when segment is audited.
<hlvl-filter enabled="false">	Do not report hierarchical parent segment during DLI command calls.
<excluded-regions>	Do not audit DLI calls from these region types.

Collection-specific statements

Table 17. Collection-specific XML statements	
XML statement	**Definition**
<collections>	A grouping of the individual <collection> XML tags.
<ims>	IMS name connection to the collection.
<agent-name>	Agent name connection to the collection.
<name>	IMS name connection to the collection.
<collection-profile>	For each agent name and IMS name, IBM Guardium S-TAP for IMS establishes a connection to the collection profile.
<name>	Constructed name of the policy (*policy_IMS_NAME*).
<dli-status-codes>	Two-character DLI status codes to be audited. Terminated by FF value.

Quarantine information

Quarantine XML is only sent from the appliance when the quarantine is triggered by audited events that are sent to the appliance by the agent, and the quarantine is deemed to be in effect. This causes AI status codes (error opening database) to be returned to the application program in the DLI Status code PCB field (DBPCBSTC), and message AUIJ252W to appear in the IMS region or batch job.

Quarantine only works with full-function DLI calls because the AUI hook for Fast-Path occurs after the DLI call has completed. (The DLI call cannot be preempted.)

Table 18. Quarantine-specific XML statements

XML statement	Definition
<quarantine-lists>	Start of quarantine section.
<quarantine-list agent-name="*xxxxxxxx*" ims-name="*yyyyyyyy*"> >	Agent and IMS name are affected.
<quarantine-item>	Start of quarantine details.
<start-ts>yyyy-mm-dd-hh.mm.ss.000000	Quarantine start date/time.
<end-ts>yyyy-mm-dd-hh.mm.ss.000000	Quarantine end date/time.
<user-id>	User ID to be quarantined.

Sample XML file

This is an example of a valid audit policy.

```
<install-info>
  <artifacts>
    <ims>
      <name>IMSV14AH</name>
      <agent>AUI15A</agent>
      <description>IMS V14 Test IEACRX AUI10A27</description>
      <version>0</version>
      <plexname></plexname>
      <recons>
        <recon seq="1">IMSEA1.RECON1</recon>
        <recon seq="2">IMSEA1.RECON2</recon>
        <recon seq="3">IMSEA1.RECON3</recon>
      </recons>
      <reslibs>
        <reslib seq="1">IMSEA1.SDFSRESL</reslib>
      </reslibs>
      <dbdlibs/>
      <psblibs/>
      <thresholds-050i>
        <max-count>1K</max-count>
        <max-time>0015</max-time>
      </thresholds-050i>
      <audit-levels>
        <collector name="ims">
          <audit-level>
            <signon-signoff value="true"/>
            <start-stop value="true"/>
            <db-open-close value="true"/>
            <dbd-psb value="true"/>
          </audit-level>
        </collector>
        <collector name="smf">
          <audit-level>
            <read value="true"/>
            <update value="true"/>
            <delete value="true"/>
            <create value="true"/>
            <alter value="true"/>
            <racf-violations value="true"/>
```

```
          </audit-level>
        </collector>
      </audit-levels>
    </ims>
  </artifacts>
  <policies>
    <collection-profile>
      <name>policy_IMSV14AH</name>
      <description>---: Log Full Details With Values,Auv - Event All,IEA1_ALL_ST_AH</
description>
      <rules>
        <rule>
          <active>true</active>
          <filters/>
          <targets>
            <segment-target>
              <type>include</type>
              <database-name>%</database-name>
              <segment-name>%</segment-name>
              <audit-get>true</audit-get>
              <audit-insert>true</audit-insert>
              <audit-update>true</audit-update>
              <audit-delete>true</audit-delete>
              <capture-before-image>false</capture-before-image>
              <capture-segment-data>true</capture-segment-data>
            </segment-target>
          </targets>
          <audit/>
          <excluded-regions></excluded-regions>
        </rule>
      </rules>
    </collection-profile>
  </policies>
  <collections>
    <collection>
      <ims>
        <agent-name>AUI15A</agent-name>
        <name>IMSV14AH</name>
      </ims>
      <collection-profile>
        <name>policy_IMSV14AH</name>
      </collection-profile>
      <dli-status-codes>FDFWGAGBGDGEGKL2LBLSNIUCUSUXFFFF</dli-status-codes>
    </collection>
  </collections>
  <quarantine-lists/>
</install-info>
```

Additional causes of AUIA060W

Warning message AUIA060W can appear if the data set location is incorrect. Review these additional possible causes of the message if the explanation and recommendation provided by “AUIA060W” on page 85 do not resolve the warning.

Data set: <LOCATION> in use

Explanation

An attempt to dynamically allocate the data set failed because the data set was in use by another process. This warning might be temporary. The agent retries the data set 6 times in 3 seconds before skipping the policy XML echoing.

Response

If this message occurs several times without successful policy XML echoes, check to see that any running user report program is using the data set correctly or whether a TSO user might be editing the data set.

A dynamic allocation error occurred. Data set <LOCATION>, info code: <info-code>, error code: <error-code>.

Explanation

An attempt to dynamically allocate the data set failed. The specified information and error codes reflect the return and reason codes from the z/OS dynamic allocation services.

Response

Use the info code and error code to determine the cause of the dynamic allocation failure by referring to the *z/OS MVS Programming: Authorized Assembler Services Guide* in the IBM Knowledge Center. Correct the error and restart the agent.

Catalog Search Interface: error RC = <rc>, RSN = <rsn>.

Explanation

Using the z/OS Catalog Search Interface routine, the agent attempted to analyze whether the data set is a Generation Data Group (GDG) data set or a non-VSAM data set. An error occurred while calling the routine.

Response

Consult the *Return Codes for General Purpose Register 15* section of the *IBM Catalog Search Interface User's Guide* in the IBM Knowledge Center. Contact IBM Support if additional assistance is needed.

Data set "<LOCATION>" could not be deleted, info code: <code>, error code <code>.

Explanation

An attempt was made to delete and reallocate a non-VSAM non-GDG data set in the catalog.

Response

Ensure that the agent task has RACF (or other security product) authority to delete a data set that contains a high-level qualifier. Attempt to correct the security problem and restart the agent. If the error persists, contact IBM Support and provide the info and error codes.

XML echo data set <LOCATION> is of an unsupported type

Explanation

Only non-VSAM and GDG base data sets are supported.

Response

Ensure that the data set type is either a non-VSAM data set or a Generation Data Group. Restart the agent.

Chapter 12. Troubleshooting

Use the following topics to diagnose and correct problems that you experience with IBM Guardium S-TAP for IMS.

Messages and codes for

This information documents the messages and error codes issued by . Messages are presented in ascending alphabetical and numerical order.

Note: To set a z/OS message alert for messages that begin with AUII, or messages AUIJ250I and AUIJ252W, use single-dash formatting between the message number and message text. For all other messages, use a double-dash. For example:

AUIT031I--Starting the command listener thread
Format most message alerts with double-dashes between the message number and message text.

AUII056I - ZIIP PROCESSING ENABLED FOR IMS STAP
Format message alerts for AUII*, AUIJ250I, and AUIJ252W with a single dash between the message number and message text.

Error messages and codes: AUIAxxxx

The following information is about error messages and codes that begin with AUIA.

AUIA003E **Address Space *<name>* failed to start successfully on *<LPAR name>*.**

Explanation

An attempt by the agent to start the named support address space has failed.

User response

Check the named address space logs to identify why it was not able to start. In most cases, this occurs if an address space with that name is already online, there was a JCL error, or there was an issue resolving the loopback address host name. If further assistance is required, contact IBM Software Support.

AUIA004E **Address Space *<name> (<job number)>* failed to stop successfully on *<LPAR name>* within the timeout period and was abandoned.**

Explanation:
The specified address space did not stop within the time out period and was consequently abandoned by the master address space.

User response:
Check the named address space logs to identify why it did not stop. If further assistance is needed, contact IBM Software Support.

AUIA005I **Starting address space *<name>* on *<LPAR name>*.**

Explanation:
The agent has automatically started the support address named.

User response:
This is an informational message only.

AUIA006I **Address Space *<name> (<job number>)* is online on *<LPAR name>*.**

Explanation:
The agent has successfully started the support address space named.

User response:
No action is required.

AUIA007I **Stopping address space *<name> (<job number>)* on *<LPAR name>*.**

Explanation:
The agent has automatically stopped the support address space named.

User response:
No action is required.

AUIA008I **Address Space *<name> (<job number>)* on *<LPAR name>* is offline.**

Explanation:
The named address space has successfully stopped.

User response:
No action is required.

AUIA009E **Address space *<name>* is not active.**

Explanation

The specified address space that the master address space was attempting to control is not online.

User response

Correct and retry.

AUIA010E **Address Space *<name>* is already active.**

Explanation:
This message indicates that the address space with the specified name is active already and was expected to be. This message occurs when starting the BATCH (or SMF) collector if they are already running.

User response:
Verify that the address space is already running. If the address space is not online and the message occurs, contact IBM Software Support.

AUIA021I **MODIFY command *<command text>* sent to Address Space *<name>*.**

Explanation:
The MODIFY command *<command text>* sent to address space named.

User response

No action is required.

AUIA022I ***<Collector name>* collector is disabled: interval is set to *<value>*.**

Explanation

Named collector is disabled because the interval value is less than or equal to zero.

User response

If this was not intentional, fix the interval value and restart the agent address space.

AUIA023I ***<Collector name>* collector is disabled: proc name for the collector address space has not been specified in the configuration.**

Explanation:
The specified collector is disabled because the procedure name for the collector address space has not been specified in the configuration.

User response:
To enable this collector, specify the procedure name for collector address space. If the procedure name is specified and this message still occurs, contact IBM Software Support.

AUIA024I ***<Collector name>* collector is disabled: not configured.**

Explanation:
The specified collector is disabled because it has not been configured.

User response:
To enable this collector, configure it using the Guardium user interface. If the specified collector is configured and the message still occurs, contact IBM Software Support.

AUIA027E **Abend occurred while validating *<log stream>*. Abend code = *<code>*, RSN = *<reason>*.**

Explanation:
The Log Stream *log stream* validation failed with abend code *code* and reason code *reason*.

User response:
Contact IBM Software Support.

AUIA028S **Agent *agent-name* on *PLEX name* for S-TAP version *S-TAP version* is already online. *(ADS_SHM_ID=<Memory Segment ID>)***

Explanation:
The specified agent is already online. Agent names must be unique per sysplex.

User response:
Change the *agent-name* and restart the agent, or shut down the other agent.

AUIA029I ***collector* collector is disabled: no Audit IMS Log Events are selected for IMS source *IMS*.**

Explanation:
An Audit IMS Log Event must be selected for the IMS source *IMS* for the collector to be enabled.

User response:
To enable the collector, select an Audit IMS Log Event for the IMS source.

AUIA030I ***collector* collector started successfully.**

Explanation:
The specified collector started.

User response:
No action is required.

AUIA031I ***collector*** **collector stopped successfully.**

Explanation:
The specified collector stopped.

User response:
No action is required.

AUIA033I **(GDM) Attempting to establish link with the appliance.**

Explanation:
The agent is attempting to establish a connection to one of the appliances specified in the agent configuration.

User response:
No action is required.

AUIA034S **(GDM) An attempt to establish the link to the appliance failed.**

Explanation:
The agent could not establish a connection to any of the appliances specified in the configuration.

User response:
Contact your network administrator or IBM Software Support.

AUIA035W **(GDM) Link failed over to a secondary appliance. [host=*host*, port=*port*]**

Explanation:
The agent lost connection to the primary appliance and switched to the specified secondary appliance.

User response:
No action is required.

AUIA036I **(GDM) Link to primary appliance established. [host=*host*, port=*port*]**

Explanation:
The agent has connected to the specified primary appliance.

User response:
No action is required.

AUIA037I **(GDM) Link to primary appliance restored. [host=*host*, port=*port*]**

Explanation:
The agent has reconnected to the specified primary appliance.

User response:
No action is required.

AUIA038S **(GDM) Link to the appliance lost.**

Explanation:
All attempts to connect to the appliances specified in the configuration have failed.

System action:
Any new policies defined in the appliance will not be pushed down to the IBM Guardium S-TAP for IMS agent.

User response:
Verify network connectivity to the appliance. Contact your network administrator or IBM Software Support.

AUIA041I **Guardium policy processing failed due to prior errors.**

Explanation:
The Guardium policies could not be processed.

User response:
Check the log for previous errors.

AUIA042W **The Guardium policy is not applicable.**

Explanation:
One or more of the policy rules cannot be used by the current agent.

User response:
Check the log for previous errors to determine why the policy is not applicable and fix the policy definition.

AUIA043I **The Guardium policy reader thread started.**

Explanation:
The Guardium policy reader thread started.

User response:
No action is required.

AUIA044I **The Guardium policy reader thread is terminating.**

Explanation:
The Guardium policy reader thread is stopping.

User response:
No action is required.

AUIA045I **The guardium policy reader thread is terminating due to prior errors.**

Explanation:
The policy reader thread is stopping due to previously reported errors.

User response:
Check the previously issued messages to determine why the policy reader is terminating.

AUIA048I ***auiu_taskname*** **is configured to start only on *lpar-name*.**

Explanation:
The configuration file pointed to by the AUICONFG DD statement contains an AUIU_EXCLUDE_LPAR

statement that has the ***ALL** parameter supplied as the excluded LPAR name.

System action:
The AUIUSTC task is scheduled only on the home LPAR where the agent is running.

User response:
To schedule the AUIUSTC task for another LPAR, remove or correct the AUIU_EXCLUDE_LPAR statement.

AUIA049W ***auiu_task_name* is configured to not start on *lpar_name* but will be started on *lpar_name* because *aui_agent_name* runs on *lpar_name***

Explanation:
The **AUIU_EXCLUDE_LPAR** configuration parameter, found in the AUICONFG SAMPLIB member, was used in an attempt to prevent the AUIU task from executing on the LPAR named.

System action:
The request to exclude this LPAR from AUIU processing is ignored because the specified LPAR is also where the agent is executing.

User response:
Remove the LPAR name from the AUICONFG samplib member's **AUIU_EXCLUDE_LPAR** parameter. The change will be implemented at the next restart of the agent.

AUIA050W ***auiu_task_name* is configured to not start on *lpar_name* but no such system exists.**

Explanation:
The specified *lpar_name* has been included as part of the LPARS that are specified in the **AUIU_EXCLUDE_LPAR** configuration keyword. The specified *lpar_name* was not found in the list of members of either the SYSJES or *lpar_name* XCF groups.

System action:
Processing continues.

User response:
This message might indicate that the lpar_name is not available or that there is an error in the specified lpar_name.

AUIA051I ***auiu_task_name* is configured to not start on *lpar_name* and will not be started on *lpar_name*.**

Explanation:
The **AUIU_EXCLUDE_LPAR** configuration, parameter found in the AUICONFG SAMPLIB member, was used in an attempt to prevent the AUIU task from executing on the specified LPAR.

System action:
An instance of the AUIU task is not routed to the excluded LPAR.

User response:
None.

AUIA052I **Discovered <plex-name> system <system-name>.**

Explanation:
This LPAR name was found as a member of the XCF group when performing a z/OS IXCQUERY on the PLEXNAME of SYSJES XCF GROUPS.

System action:
Processing continues

User response:
No action is required.

AUIA053I **Agent configuration option *<option>* has been updated to *<value>*.**

Explanation:
This message indicates that command such as: **/f AUIASTC,SET CONFIG** *<option>* **ON/OFF** processed successfully.

User response:
No action is required.

AUIA054I **Agent configuration option *<option>* is set to *<value>*.**

Explanation:
This message indicates that command such as: **/f AUIASTC,GET CONFIG** *<option>* processed successfully.

User response:
No action is required.

AUIA055I **The agent is waiting for start-up information from the appliance.**

Explanation:
The agent has determined that there is no checkpoint information available for this agent in E/CSA, and is awaiting this data to be sent from the appliance.

System action:
The agent waits up to 30 seconds for the checkpoint information, and if none is received, processing continues by using default checkpoint values, such as current blocks from the z/OS log-streams, and SMF and SLDS data sets that were created no earlier than the previous day.

User response:
No action is required.

AUIA056I **Starting the agent collectors.**

Explanation:

The agent is starting the auditing threads.

System action:
The agent starts the DLIO/DLIB/AUIL/AUIF auditing threads.

User response:
No action is required.

AUIA057I **Issuing request to capture agent status.**

Explanation

A command, such as **/f AUIASTC,STATUS**, has been issued for processing.

User response

No action is required.

AUIA058I **Request to capture agent status has completed successfully.**

Explanation:
A command, such as **/f AUIASTC,STATUS** has processed successfully.

User response:
No action is required.

AUIA059I **Policy XMl echo**

Explanation:
If the **XML_ECHO_AUILOG(Y)** keyword exists in the AUICONFG, this message will be followed by the echo of all active XML policies on the AUILOG.

System action
As an example, the first three lines of the echo appear as follows:

```
<?xml version="1.0" encoding="IBM-1047"
standalone="yes"?>
<!-- 2019-03-25-13.35.57.354196 -->
<install-info>
```

User response:
For more information, see "Echoed XML statement definitions" on page 74.

AUIA060W **Policy XML echo to data set skipped: *<MESSAGE> <LOCATION>***

Explanation

The XML of the policy that was installed from the was not echoed to the specified location due to the specified message. If the **&Data_Set_Name** parameter contains z/OS system variables, <LOCATION> reflects the data set name after symbol substitution has been done.

<MESSAGE> <LOCATION> can be:

- The installed policy has not been changed. The echo is skipped if the newly installed policy has not changed since it was last installed.
- The data set location is not valid. Incorrect use of a system symbol in the **&Data_Set_Name** parameter can invalidate the location. Additional requirements:
  - The data set name must not exceed 44 characters.
  - The segment length must be greater than zero and less than or equal to 8.
  - The first character in each segment must be a letter (A – Z), #, @, $, or hyphen.

System action:
Processing continues.

User response:
Correct the **&Data_Set_Name** parameter and restart the agent. If the error persists, see Additional causes of AUIA060W .

AUIA061I **Policy XML echo to data set *<LOCATION>* completed.**

Explanation:
The agent has completed the XML echo of all active policies that were installed from the . *<LOCATION>* is the data set name specified by the **&Data_Set_name** parameter of the **XML_ECHO_DATASET** keyword.

System action:
The data set name reflects the z/OS system variable substitution and the Generation Data Group extension if either exists in the **&Data_Set_name** parameter.

User response:
No action is required.

Error messages and codes: AUIBxxxx

The following information is about error messages and codes that begin with AUIB.

AUIB300I **CONNECTION TO z/OS SYSTEM *type* LOG STREAM WAS SUCCESSFUL - LOG STREAM NAME: *log_stream_name*, LOG STREAM TYPE: *XCF-BASED*/*DASD_ONLY*, CHECKPOINT VALUE: *check_point_value*, CHECKPOINT PTR: *address_of_checkpoint***

Explanation:
The connection to the log-stream name (*log_stream_name*) configured to process *log_stream_type* events completed successfully.

System action:
Processing continues

User response:
No action is required.

AUIB302I **DRAIN REQUEST FOR *type* LOG STREAM HAS COMPLETED. LOG STREAM: *name*.**

Explanation:
A DRAIN request, which reads all data from the z/OS log stream, has completed.

System action:
The AUIASTC tasks prepare to terminate.

User response:
No action is required.

AUIB305I **DRAIN COMPLETE FOR LOG STREAM *log-stream name***

Explanation:
A DRAIN request used to flush read all existing events from the log-stream-name indicated has completed successfully

System action:
The log-stream reader thread will start the termination phase.

User response:
No action is required.

AUIB306E **INVALID RECORD FOUND IN *log-stream* LOG STREAM -RECORD IMAGE SNAPPED TO AUI$NAP DD**

Explanation:
When reading DLI call audit records from the z/OS System log stream, a malformed audit record was encountered or the version of the audit record was not recognized.

System action:
Processing continues after writing a SNAP/DUMP of the offending record to the AUI$NAP DD.

User response:
First, verify that the S-TAP version that is running in the IMS Control Region and/or Batch Region is the same as is running in the agent. If adjusting the version does not resolve the issue, forward the AUI $NAP output to IBM Software Support.

AUIB700I **type: *LOGSTREAM CHECKPOINT INFORMATION* - LOG STREAM NAME: *log-stream-name* - CHECKPOINT VALUE: *check_point_value* - LAST UPDATED (UTC): *date_time***

Explanation:
This message provides the highest block ID for the log stream. This is used as the starting checkpoint for processing data from this log stream.

System action:
Processing continues.

User response:
No action is required.

Error messages and codes: AUIFxxxx

The following information is about error messages and codes that begin with AUIF.

AUIF002I **SMF log reader interval set to *<n>* minutes.**

Explanation:
The subtask that reads event data from SMF log data sets is scheduled to perform every <n> minutes.

User response:
No action is required.

AUIF003E **Command *<command>* failed; interval value must be between *<lower-bound>* and *<upper-bound>*.**

Explanation
This message indicates that *<command>* such as:

```
/f AUIASTC,SET INTERVAL <number>
```

failed because of incorrect *<number>* value. Correct value must be between <lower-bound> and <upper-bound>.

User response:
Use an interval value between *<lower-bound>* and *<upper-bound>*. If that does not resolve the issue, contact IBM Software Support.

AUIF501I **NO NEW CATALOGED SMF DATA SETS FOUND FOR SMF MASK: *smf_mask_value***

Explanation:
When scanning the z/OS catalog for new data sets that meet the indicated SMF mask value (*smf_mask_value*) and have not been processed by the product, it was determined that no z/OS data sets meet that criteria.

System action:
The process will continue to examine other SMF Mask values.

User response:
No action is required.

AUIF502I **PROCESSING SMF DATA SET: *smf_data_set_name***

Explanation:
Processing has started for a SMF data set.

System action:
Events will be obtained from the SMF data set based on collection profile criteria.

User response:
None.

AUIF503I **PROCESSING COMPLETE FOR SMF DATA SET: *smf_data_set_name***

Explanation:
Processing of the SMF data set has completed.

System action:
Processing continues with other candidate SMF data sets.

User response:
No action is required.

AUIF505I **SMF AUDITING IS DISABLED AT THE AGENT LEVEL**

Explanation:
Auditing of SMF events has been disabled at the agent level, as instructed by the settings chosen in the Guardium user interface.

System action:
The auditing of events sourced from SMF data sets is not performed.

User response:
No action is required.

AUIF506I **SMF AUDITING IS DISABLED AT THE IMS LEVEL. IMS NAME: *ims_name***

Explanation:
Auditing of SMF events has been disabled at the IMS level for the IMS named (*ims_name*) by use of the Guardium interface and the IMS Auditing Levels editor.

System action:
The auditing of events sourced from SMF for the IMS named is not performed.

User response:
If this is a desired action, then no response is needed. If SMF events should be audited for this IMS, then the IMS configuration should be modified by using the Guardium interface and the IMS Auditing Levels to select any or all SMF events you want to audit.

AUIF507E **PROCESSING FAILED FOR SMF DATA SET: *data set name***

Explanation:
Processing failed during the reading of the data set, specified by name in the message text.

System action:
The collection process terminates.

User response:
Determine the cause of the failure and correct it by reviewing previously issued S-TAP and z/OS messages.

AUIF508I **SCANNING RECON DATA SETS FOR IMS ARTIFACT DATA SETS. RECON1: *recon1_dsn* RECON2: *recon2_dsn* RECON3: *recon3_dsn***

Explanation:
The AUIFSTC task has started to scan the RECON data sets looking for database data sets, Image copy data sets and optionally IMS SLDS to be audited using SMF records.

System action:
The RECON data sets are read using the specified DSN.

User response:
No action is required.

AUIF702I **SMF MASK CHECKPOINT INFORMATION - MASK VALUE : *SMF_mask* - LAST DSN READ: *SMF_dsn* - LAST UPDATED (UTC): *date_time***

Explanation:
This message provides the SMF data set mask (*SMF_mask*) and the last SMF data set read (*SMF_dsn*) that matched that mask. This information is used as a checkpoint to indicate which SMF data sets have already been processed, and should not be re-read by the AUIFstc tasks.

System action:
Processing continues.

User response:
No action is required.

Error messages and codes: AUIGxxxx

The following information is about error messages and codes that begin with AUIG.

AUIG001S **An unexpected error occurred (/path/to/file.c, linenum).**

Explanation:
An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response:
Contact IBM Software Support.

AUIG002S **An unexpected error occurred with token "token1" (/path/to/file.c,linenum).**

Explanation:
An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response:
Contact IBM Software Support.

AUIG003S **An unexpected error occurred with tokens "token1" and "token2" (/path/to/file.c,linenum).**

Explanation:
An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response:
Contact IBM Software Support.

AUIG004S **An unexpected error occurred with tokens "token1", "token2", "token3", and "token4" (/path/to/file.c,linenum).**

Explanation:
An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response:
Contact IBM Software Support

AUIG005S **An unexpected error occurred with tokens "token1", "token2", and "token3" (/path/to/file.c,linenum).**

Explanation:
An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response:
Contact IBM Software Support.

AUIG006S **An unexpected error occurred with tokens "token1" and "token2" (/path/to/file.c,linenum).**

Explanation:
An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response:
Contact IBM Software Support.

AUIG014E **dataspace create return code = *return-code-hex*, reason = *reason-code-hex***

Explanation:
An attempt to create a data space for spill usage has failed. Spill capability might not be available.

User response:
Examine the return code and reason code, and take appropriate action to ensure that data spaces can be created.

AUIG015W **MALLOC: big alloc coming *memory_size* from GDM Read Buffer**

Explanation:
More than 10,485,760 bytes was required in order to process collection policies pushed from the .

System action:
Processing continues.

User response:
No action is required.

AUIG016S **MALLOC: zero alloc from *<site>*.**

Explanation:
Zero bytes was required in order to process collection policies pushed from the Security Guardium system.

User response:
Contact IBM Software Support.

AUIG017S **MALLOC: negative malloc *memory size* at site *site*.**

Explanation:
Negative number of bytes required in order to process collection policies pushed from the Security Guardium system.

User response:
Contact IBM Software Support.

AUIG018S **MALLOC failed, got NULL for size *<memory_size>* at site *<site>*.**

Explanation:
Attempt to allocate memory failed.

User response:
Contact IBM Software Support.

AUIG045E **Write failed, sd=*bbbb* desired write len *length* buffer at *address*, ret code *xxxx* reason 0x*yyyyzzzz***

Explanation:
An attempt to read or write to a socket has failed. This error might occur if is connected to a peer that is offline.

System action:

The system attempts to reestablish the connection to the peer in order to read or write the data.

User response:
Identify the cause of the failure by using the *z/OS UNIX System Services Messages and Codes SA23-2284-xx* manual to look up the return and return codes that are provided in the message text, where *bbbb* is an internal code, *xxxx* is the return code, and *yyyyzzzz* is the reason code. Use the *zzzz* value to determine the error code, as described in the Reason codes (errnojrs) section of the *z/OS UNIX System Services Messages and Codes* manual.

AUIG046E **Failure to resolve address for host *'HOST'*, ret code *return-code*, reason *hex-value*.**

Explanation:
An attempt to resolve the given hostname failed.

User response:
Verify that the hostname is specified correctly and is resolvable. Contact IBM Software Support if hostname is correct and resolvable.

AUIG047E **Set sockopt failed, level = *hex-value*, option = *hex-value*, ret code *return-code*, reason *hex-value*.**

Explanation:
An attempt to set a socket option failed.

User response:
Contact IBM Software Support

AUIG048E **Get sockopt failed, ret code *return-code*, reason *hex-value*.**

Explanation:
An attempt to set a socket option failed.

User response:
Contact IBM Software Support.

AUIG049E **BPXFCT failed, ret code *<return-code>*; reason *<reason-code>*.**

Explanation:
The system BPXFCT call failed while attempting to set socket blocking mode.

User response:
See the *MVS Programming: Authorized Assembler Services Guide* for more information about the specified information and error codes.

AUIG050E **Read failed ret code *xxxx* reason 0x*zzzzzzzz***

Explanation:
An attempt to read or write to a socket has failed. This error might occur if is connected to a peer that is offline.

System action:
The system attempts to reestablish the connection to the peer in order to read or write the data.

User response:
Identify the cause of the failure by using the z/OS USS Return Codes and Reason Codes to look up the return and reason codes that are provided in the message text, where *xxxx* is the return code and *zzzzzzzz* is the reason code.

AUIG051I **TCP write disabled**

Explanation:
TCP/IP processing has been disabled.

System action:
The Guardium appliance will not receive data.

User response:
No action is required.

AUIG052I **Write to megabuffer disabled**

Explanation:
TCP/IP buffer has been disabled.

System action:
Processing continues.

User response:
No action is required.

AUIG053I **Unexpected payload received *<hexadecimal string>*. Payload ignored.**

Explanation:
An unexpected string of data was received by the agent from the Guardium appliance or associated firewall. The string does not conform to the format that is normally associated with a pushed-down policy or other expected data.

System action:
The string is ignored and normal processing continues.

User response:
If this message appears occasionally, no action is required. If this message appears frequently, contact IBM Support to diagnose whether a problem exists with the Guardium appliance or firewall.

AUIGF120I **Trace Settings: Compilation 0, Requested Runtime 0, ECSA Flag 32, Actual Runtime 0...**

Explanation:
This message is produced during the compilation of a filter, using the policy information that was specified.

System action:
Processing continues.

User response:
No action is required.

AUIGF201I **Valid stage zero filter criteria found.**

Explanation:
The collection profile compilation process found that the collection profile criteria will allow for Stage zero filtering of IMS DLI events based on USERIDs or PSB names.

System action:
Processing continues.

User response:
No action is required.

AUIGF202I **No valid stage zero filter criteria found.**

Explanation
The collection profile compilation process found that the collection profile criteria is not conducive to providing Stage 0 filtering for IMS DLI events. The reasons may include:

- No USERIDS or PSBS were specified in the selection criteria.
- Multiple RULES were defined and differences in the USERID and/or PSB specifications in each rule were different.

System action:
Processing continues without Stage Zero filtering capability.

User response:
If Stage 0 filtering is desired, adjust the USERID and PSB specifications in each rule to be the same.

Error messages and codes: AUIIxxxx

The following information is about error messages and codes that begin with AUII.

Note: To set a z/OS message alert for messages that begin with AUII, use single-dash formatting between the message number and message text. For example: `AUII056I - ZIIP PROCESSING ENABLED FOR IMS STAP`

AUII017I **S-TAP for V10.1.3 initialization complete using RECON1 DSN: *recon1_dsn***

Explanation:
IBM Guardium S-TAP for IMS has initialized in the DLI/DBB batch job or IMS control region environment. For successful auditing to occur, the RECON1 DSN indicated in this message should match the RECON1 DSN associated with the IMS definition you have created.

User response:
No action is required.

AUII018E **initialization failed**

Explanation:
IBM Guardium S-TAP for IMS was unable to initialize in this IMS Control region. The monitoring of IMS databases will not occur.

System action:
IMS processing continues without auditing capabilities.

User response:
Examine the JES log for other messages to determine the reason for the initialization failure.

AUII019E **termination failed**

Explanation:
IBM Guardium S-TAP for IMS was unable to terminate cleanly.

System action:
The termination of the IMS online region of DLI/DBB batch job step continues.

User response:
This error indicates that an environmental error has occurred. Examine the JES log for other AUI messages to determine the reason for the termination failure.

AUII020E **UNABLE TO FIND RECON1 DATA SET NAME**

Explanation:
An attempt to find the RECON1 data set name used by the IMS Online control region or DLI/DBB batch job step has failed. The RECON1 data set name is critical to the determination of the collection profile used to audit IMS events.

System action:
IMS processing continues without the IMS auditing feature.

User response:
Determine why the RECON1 data set name is not available for this IMS control region or DLI/DBB batch job step. An in-stream RECON1 DD statement must be present in the JCL, or a RECON1 MDALIB member being present in the JOB/STEPLIB DD concatenation is required.

AUII021E **BLDL FAILED FOR ACTION MODULE *module_name***

Explanation:
An attempt to find a required processing module (module_name) has failed.

System action:
IMS processing continues without auditing.

User response:
Examine the STEPLIB/JOBLIB DD concatenation to ensure the SAUIIMOD product data set is included.

AUII022E **INSUFFICENT STORAGE AVAILABLE FOR *module_name* ACTION MODULE (*stg_type*)**

Explanation:
An attempt to obtain storage for the module named (*module_name*) has failed. The storage type field (*stg_type*) indicates if the storage required is 31bit or 24bit based.

System action:
IMS processing continues without IMS auditing available.

User response:
Increase the region size used by the job step (REGION=).

AUII023E **IMODULE DIRLOAD FAILED FOR ACTION MODULE *module_name***

Explanation:
The DIRLOAD IMS service has failed.

System action:
IMS processing continues with auditing.

User response:
Determine the cause of the error from the IMS Messages and Codes manual and correct the error. If necessary, contact IBM Software Support.

AUII024E **Unable to locate IMS SCD address.**

Explanation:
An attempt to locate the IMS SCD during product initialization has failed.

System action:
IMS processing continues without auditing.

User response:
Verify that you are attempting to run the product using a supported IMS release. Contact IBM Software Support for further assistance.

AUII025E **Unable to locate IMS SSCD Extension address.**

Explanation:
An attempt to locate the IMS SSCD Extension address has failed.

System action:
IMS processing continues without auditing.

User response:
Verify that you are attempting to run the product using a supported IMS release. Contact IBM Software Support for further assistance.

AUII026E **UNABLE TO LOCATE THIS IMS SSCT ADDRESS**

Explanation:
The IMS SCCT address cannot be located by the IMS S-TAP initialization process.

System action:
IMS processing continues without auditing capabilities.

User response:
Contact IBM Software Support.

AUII027E **INSUFFICIENT STORAGE AVAILABLE FOR AUIPLOG CONTROL BLOCK**

Explanation:
An attempt to obtain E/CSA to hold the AUIPLOG module has failed.

System action:
IMS processing continues without auditing.

User response:
Investigate E/CSA usage on the LPAR.

AUII028E **IMODULE LOAD OF ACTION MODULE *module_name* FAILED**

Explanation:
An attempt to LOAD module module_name using IMS services has failed.

System action:
An attempt to LOAD module module_name using IMS services has failed.

User response:
Verify that the SAUIIMOD product data set is available in the STEPLIB/JOBLIB data set concatenation. Contact IBM Software Support for further assistance.

AUII029E **DFSTCBTB LOCATE SERVICE CALL FAILED**

Explanation:
A call to the IMS DFSTCBTB service has failed.

System action:
IMS processing continues without auditing.

User response:
Contact IBM Software Support.

AUII031E **STAP FOR IMS INTERNAL LOGIC ERROR *(rc)***

Explanation:
initialization found a logic error.

System action:
IMS processing continues without auditing.

User response:
Contact IBM Software Support.

AUII038E ITASK CREATE FOR ACTION MODULE *module_name* FAILED

Explanation:
DA call to the DFSCIR IMS service to create an ITASK has failed.

System action:
IMS processing continues without auditing.

User response:
Contact IBM Software Support.

AUII040E ODBA LOAD OF DFSISSI0 FAILED

Explanation:
An attempt to LOAD IMS module DFSISSI0 has failed.

System action:
IMS processing with auditing continues. The product will be unable to determine the correct USERID for events driven from ODBA threads.

User response:
Contact Software Support.

AUII041E ODBA HOOK POINT NOT FOUND (module_name)

Explanation:
An attempt to locate a hook point in the indicated module (module_name) has failed.

System action:
IMS processing with auditing continues. The product will be unable to determine the correct USERID for events driven from ODBA threads. An output DD: AUI $NAP is dynamically allocated to SYSOUT, and the area where the hook point was to be located is snapped out to this AUI$NAP DD.

User response:
Provide the AUI$NAP output to IBM Software Support.

AUII042W ZIIP PROCESSOR NOT AVAILABLE ON THIS LPAR

Explanation:
The AUIZIIP DD statement has been found in the IMS Control Region JCL, which indicates that the zIIP processor should be considered for use when filtering DLI calls and writing to the z/OS System Logger. IMS STAP has determined that zIIP processing is not available on this LPAR.

System action:
Processing continues exclusively using general processors.

User response:
Remove the AUIZIIP DD statement and restart the IMS sub-system.

AUII043W THIS IMS IS NOT CONNECTED TO WORKLOAD MANAGER

Explanation:
A request to process DLI call filtering and z/OS System Logger writes on a zIIP processor has been rejected as the IMS sub-system is not connected to the z/OS Workload Manager.

System action:
Processing continues exclusively using general processors.

User response:
No action is required.

AUII044E ZIIP PROCESSING REQUEST HAS BEEN REJECTED

Explanation:
A request to process DLI call filtering and z/OS System Logger writes on a zIIP processor has been rejected.

System action:
Processing continues exclusively using general processors.

User response:
Review previously issued AUII messages to determine the root cause of the request rejection.

AUII046E NAME/TOKEN SERVICE *service-name* SERVICE FAILED (*name value*)

Explanation:
An attempt to drive the z/OS name/token service has failed.

System action:
IMS processing continues without auditing.

User response:
Contact IBM Software Support

AUII049E DEDB CALL ANALYSIS INIT FAILURE RC = *return code*

Explanation:
An attempt insert product code in the DEDB call analysis area has failed.

System action:
IMS processing with DEDB event auditing disabled. An output DD: AUI$NAP is dynamically allocated to SYSOUT, and the area where the code insertion was to be located is snapped out to this AUI$NAP DD.

User response:

Provide the AUI$NAP output to IBM Software Support.

AUII050I S-TAP FOR IMS AUDIT STATISTICS

Explanation
This message provides statistics regarding the number of DLI events which have been processed. This message is issued when:

- The number of DLI calls specified in the message frequency section of the Guardium client's IMS Data Set definition screen has been reached.
- The time specified in the AUII050I message frequency section of the Guardium client's IMS Data Set definition screen has elapsed.
- The collection profile for the IMS is made in active.
- The DLI/DBB batch job or IMS Online Control Region terminates.

The description of values are as follows:

DLI CALLS RECEIVED
This value indicates the number of IMS DLI calls which had the potential of being audited. This number can be more or less than the number of actual DLI calls performed, because:

- DLI PATH calls which effect multiple segments within a hierarchical path are treated and counted as individual DLI calls.
- DLI calls types which are not included in any RULE of the active collection profile are not counted as they are immediately rejected.

DLI CALLS AUDITED
This value indicates the number of IMS DLI calls which resulted in a DLI event being written to the z/OS System Logger Log-stream for transmittal to the Guardium Appliance.

IXGWRITE ERRORS
This value indicates the number of z/OS System Logger IXGWRITE calls which have failed. One of more AUIJ304E messages will precede the issuance of the AUII050I message if the number of IXGWRITE errors is greater than zero. A non-zero value for the IXGWRITE ERRORS and a zero value for the DLI CALLS LOST DUE TO IXGWRITE ERRORS section of this message indicates that the IXGWRITE errors were subsequently retried and the IXGWRITE calls were then completed successfully.

DLI CALLS LOST DUE TO IXGWRITE ERRORS
A non-zero value in this section indicates that DLI calls which were audited and either:

- Could not be placed into a log-stream data buffer (indicated by the issuance of message AUIJ307A).
- Audited events already in the data buffer could not be written to the z/OS System Logger Log-Stream using the IXGWRITE call and the collection profile for the IMS has been deactivated or the DLI/DBB batch job or IMS Online Control region has been terminated (indicated by the issuance of message AUIJ304E).

System action:
Processing continues.

User response:
No action is required. This is an informational message only.

AUII052I USING IMS STAP V10.1.3 MODULE *Module_name APAR# Build_date*

Explanation:
These messages are issued by the IMS S-TAP code in the IMS Control region during startup to broadcast the maintenance level of the programs that are in use by .

System action:
Processing continues.

User response:
No action is required.

AUII055I ZIIP PROCESSING HAS BEEN REQUESTED FOR IMS STAP

Explanation:
The AUIZIIP DD statement has been found in the IMS Control Region JCL, which indicates that the zIIP processor should be considered for use when filtering DLI calls and writing to the z/OS System Logger.

System action:
IMS STAP attempts to create an environment to support zIIP processing.

User response:
If this was not intended, remove the AUIZIIP DD statement and restart the IMS sub-system.

AUII056I ZIIP PROCESSING ENABLED FOR IMS STAP

Explanation:
The request for zIIP support for IMS STAP and this IMS Control Region has been acted on and all initialization processes have completed successfully.

System action:
IMS STAP will schedule DLI call filtering and writes to the z/OS System Logger as a zIIP eligible enclave SRB.

User response:
If this was not intended, remove the AUIZIIP DD statement and restart the IMS sub-system.

AUII057I ***process_type* PROCESSING FAILED *RC*: return_code *RSN*: reason_code**

Explanation:
The AUIZIIP DD statement has been found in the IMS Control Region JCL, which indicates that the zIIP processor should be considered for use when filtering DLI calls and writing to the z/OS System Logger. A process (process_type) used to enable zIIP processing has failed.

System action:
The request to enable zIIP processing is rejected and general processor will be used.

User response:
Review IBM supplied documentation for the process which failed using the return and reason codes (*return_code/reason_code*) to determine the cause of the failure.

AUII058A **STAP FOR IMS COMPONENT HAS ABENDED**

Explanation:
The S-TAP for IMS component has abnormally ended, causing auditing to disable.

User response:
Contact IBM Software Support

AUII060W **Potential waited PST=*xxxxxxxx* (PST# = *yyyy*)**

Explanation:
This warning message indicates that IBM Guardium S-TAP for IMS has detected a dependent region that has been waiting for an event to be audited for at least 15 seconds. The dependent region is identified by the PST address *xxxxxxxx*. The PST# value specified as *yyyy* is the region number in hexadecimal format.

System action:
IBM Guardium S-TAP for IMS attempts to process the dependent region.

User response:
If the dependent region continues processing, then no action is required. If the dependent region remains in a wait state, then it must be stopped or cancelled. Before you stop or cancel the dependent region, take an SVC dump of the IMS Control region and provide it to IBM Software Support for analysis.

AUII061I **Potential Waited PST xxxxxxxx (PST#= zzzz) RELEASED.**

Explanation:
This message is a response to message AUII060W (Potential Waited PST xxxxxxxx (PST#= zzzz)). This message indicates that the corresponding IPOST was performed, and the PST is no longer in a WAIT state.

System action:
IMS Processing continues.

User response:
No action is required.

AUII120I **NO COLLECTIONS ACTIVE FOR THIS IMS INSTANCE**

Explanation:
Initialization has completed successfully for , but no collections were found that pertain to this batch job or IMS control region.

System action:
Processing continues.

User response:
No action is required.

AUII172I ***AUIprogram* LOADED EXIT *imsexit* FROM DATA SET: *data set name***

Explanation:
The *AUIprogram* named found an occurrence of the *imsexit* later within the JOBLIB/STEPLIB concatenation, and has loaded it.

System action:
The *imsexit* will be invoked with R13 pointing to the save area originally provided by IMS, as well as its own 512 byte work area, provided in the SXPLAWRK field of the IMS Standard User Exit Parameter list, immediately following each execution of *AUIprogram*.

User response:
For the *imsexit* to run, no action is required. If the *imsexit* should not be run in this environment, remove the data set from the JOBLIB/STEPLIB concatenation and restart the IMS control region or batch job.

AUII173E **IMS RELEASE *ims-vrl* IS NOT SUPPORTED**

Explanation:
The IMS release being used is not support by this version of the product.

System action:
IMS processing continues without auditing.

User response:
Review supported IMS releases for the release of this product.

AUII174E **LOAD OF SERVICE MODULE *module_name* FAILED RC = *return_code***

Explanation:
LOAD OF SERVICE MODULE *module_name* FAILED RC = *return_code*

User response:
Ensure that the SAUIIMOD product data set is included in the STEPLIB/JOBLIB DD concatenation.

AUII175I **NON_ZERO RC FROM EXIT *exit_name*: RC = *return_code***

Explanation:
The *exit_name* indicated returned a non-zero return code value of *return_code* as specified.

System action:
The return code value is returned to IMS.

User response:
Correct the *exit_name* program if the non-zero value was returned in error. Review the IMS Customization Guide or IMS Exit Routine Reference for more information.

AUII176E ***module_name service_type* SERVICE ERROR: RC: *return_code* RS: *reason_code***

Explanation:
The *service_type* invoked by the specified *module_name* has failed.

System action:
IMS processing continues without auditing.

User response:
Review all subsequent AUI error messages to diagnose the problem.

AUII177E ***module_name* FOUND WITH RENT/REUS ATTRIBUTE IN NON_APF ENVIRONMENT**

Explanation:
Program *module_name* had the RENT/REUS attribute on in a non-APF-Authorized environment. is unable to load the program.

System action:
Processing continues with the exit cascading feature disabled.

User response:
Re-link the exit with the NOREUSE attribute.

AUII178E **DATA SET NAME: *dsn***

Explanation:
This message is issued in conjunction with a previous message (for example, AUII176E) to indicate an associated data set.

User response:
Check the log for the previously issued, associated message and take the action that is advised in that message.

Error messages and codes: AUIJxxxx

The following information is about error messages and codes that begin with AUIJ.

AUIJ005W **UNABLE TO LOAD MESSAGE TABLE *table_name* RSN: *reason_code* WILL USE AUIMGENU**

Explanation:
An attempt to perform a z/OS LOAD of the message table named (*table_name*) failed. The reason for the failure is described in the reason code field (*reason_code*). The default U.S. English message table will be used. This message follows the AUI006E message.

System action:
Processing continues while using the U.S. English message table.

User response:
Determine and correct the cause of the message table load failure.

AUIJ006E **LOAD FAILED FOR MESSAGE TABLE *table_name* RSN: *reason_code***

Explanation:
A z/OS LOAD attempt failed for the message table (*table_name*) indicated.

System action:
If the table name is the U.S. English message table, (AUIMGENU) processing will terminate. Other table names will cause the product to attempt to use the U.S. English message table after issuing the AUIJ005W message continue processing.

User response:
Determine and correct the cause of the message table load failure.

AUIJ007E **PROGRAM *program_name* IS NOT EXECUTING APF-AUTHORIZED**

Explanation:
The program specified requires APF-Authorization to perform its function.

System action:
The program terminates.

User response:
Ensure that all data sets included within the STEPLIB DD concatenation of the JCL where this message appeared are APF authorized.

AUIJ008I **ATTEMPTING TO CONNECT TO THE GUARDIUM S-TAP APPLIANCE. TCP/IP Address: *ip_address*, PORT: *port_number*, PING RATE: *ping_rate***

Explanation
An attempt is being made to establish a connection with the Guardium S-TAP appliance using the named TCP/IP address (*ip_address*) and PORT number (*port_number*).

PING RATE (*ping_rate*) indicates how often a message is sent to the appliance to provide the appliance with confirmation that the connection is active. The PINGS are sent at the rate indicated (*ping_rate*) which is shown in hour, minutes, and second (*hh:mm:ss*) format.

System action:
The connection to the Guardium S-TAP appliance is attempted.

User response:
No action is required.

AUIJ009E **LOAD FAILED FOR MODULE *module_name*. R1: *abend_code* R15: *reason_code***

Explanation:
An attempt to perform a z/OS LOAD of the named module (module_name) has failed

System action:
The function terminates.

User response:
Ensure that all required product data sets are included in the STEPLIB DD concatenation of the JCL where this message appeared. The value in R1 (*abend-code*) indicates the ABEND code that would have occurred if the failure had not been trapped by the product. The value in R15 (*reason_code*) indicates the reason code associated with the abend. Documentation regarding the abend codes and possible resolutions can be found in the *IBM z/OS MVS™ System Code* manual or equivalent.

AUIJ010I **IMS STAP *ver* HAS STARTED.**

Explanation:
The agent component, using the specified base code level, has started.

System action:
Processing continues.

User response:
No action is required.

AUIJ011I ***function_type* CALL TO GUARDUIM S-TAP APPLIANCE SUCCESSFUL**

Explanation
The function request (*function_type*) to the Guardium S-TAP appliance completed successfully. This message usually follows the AUIJ008I message indicating that the connection request has been initiated.

Function request values which can be displayed are:

INIT-DLIB
Connection request from the tasks which transmits DLI/DBB batch events.

INIT-DLIO
Connection request from the task which transmits IMS Online DLI events.

INIT_LOG
Connection request from the task which transmits IMS Archive log events.

INIT-SMF
Connection request from the task which transmits SMF events.

System action:
Processing continues.

User response:
No action is required.

AUIJ012I **NUMBER OF *event_type* EVENTS SENT TO APPLIANCE: *counter***

Explanation:
By default, this message is issued every 100,000 events sent to the appliance or approximately every 18 minutes. You can modify this frequency by using the agent parameter keyword **DLIFREQ**. This message provides a status of data being collected and sent to the Guardium S-TAP appliance. The count provided (*counter*) is the number of events since the last message was issued. The type of events (*event_type*) can include DLIB (events captured from IMS DLI/DBB batch jobs), DLIO (events captured from IMS Online regions) SMF (events captured from SMF auditing), IMSL (events captured from IMS archive log processing), and MLOG (missing IMS logs found during IMS Archive log processing).

System action:
Processing continues.

User response:
None action is required.

AUIJ013E ***stap_call* TO GUARDUIM S-TAP APPLIANCE FAILED *(call source)* IP ADDRESS: *ip_address* STAP_RC = *rc1* STAP_RS = *rs1* GDM_RC = *rc2* PB_RC = *rc3* GDML_RC = *rc4* GDML_RS = *rs2***

Explanation:
The requested call *(call_type)* to the Guardium S-TAP appliance has failed. A non-zero value GDM_RC field indicates an error.

System action:

The process terminates.

User response
Determine the cause of the failure by checking the return and reason code.

- If GDM_RC is not zero, one or more of the PB_RC, GDML_RC and GDML_RS will be set.
- If STAP_RC and STAP_RS are zero but GCM_RC or PB_RC is not zero, an internal error is indicated. Contact IBM Software Support.
- If STAP_RC and STAP_RS are not zero, contact IBM Software Support.

AUIJ014E **OPEN FAILED FOR DD *dd_name***

Explanation:
A z/OS OPEN of the data set(s) referenced by the DD named (*dd_name*) failed.

System action:
Processing terminates.

User response:
Examine the JES log for z/OS issued IEA messages issued regarding this DD statement and take appropriate action.

AUIJ015E **THIS IMS RELEASE IS NOT SUPPORTED. IMS NAME: *ims-name*, VRL: *ims_version***

Explanation:
The IMS named (*ims-name*) was found to be of a release which is not supported by this version of the product.

System action:
Processing terminates.

User response:
Review the software requirements documented in this user's guide for a list of IMS releases that are supported by this version of the product.

AUIJ016E **UNABLE TO INITIALIZE APPLIANCE INTERFACE *(connection_type)***

Explanation:
An attempt to establish a connection with the appliance has failed.

System action:
Processing terminates.

User response:
This error is usually due to the TCP/IP address specified in the **<appliance-server>** parameter of the AUICONFG or other member used in the AUICONFG DD statement used to provide the agent with configuration information being incorrect. This error can also occur if the target of the TCP/IP address is unresponsive.

AUIJ017I **PRIMARY STAP CONNECTION RESTORED *(connection_type)* - SUCCESSFULLY CONNECTED TO IP ADDRESS: *ip_address* - PORT : *port***

Explanation:
Multiple appliances are defined to IBM Guardium S-TAP for IMS, and the primary appliance (ip_address + port) was unavailable for some period of time. This message indicates that the primary appliance has become available and is now being used.

System action:
Processing continues sending data to the primary appliance.

User response:
No action is required.

AUIJ018W **PREVIOUS STAP CONNECTION FAILED *(connection_type)* - SUCCESSFULLY CONNECTED TO IP ADDRESS: *ip_address* - PORT : *port***

Explanation:
Multiple appliances are defined to the IMS STAP the connection to the active appliance has failed. This message indicates that another secondary appliance (ip_address + port) is now active.

System action:
Processing continues sending data to the secondary appliance.

User response:
No action is required.

AUIJ019E **STAP CONNECTION FAILED: NO CONNECTIONS AVAILABLE *(connection_type)* - IP ADDRESS: *ip-address* - PORT : *port***

Explanation:
The connection to the active appliance (ip_address + port) has failed and there are no secondary appliances available for use.

AUIJ020I **All EVENTS HAVE BEEN WRITTEN FROM SPILL AREA TO APPLIANCE *(connection_type)***

Explanation:
All audited events that were buffered to the spill area have been sent to the appliance.

User response:
No action is required.

AUIJ021W **EVENTS ARE BEING WRITTEN TO THE SPILL AREA *(connection_type)***

Explanation:
A connection to the appliance has been interrupted, and the spill area is being used to buffer audited events until the appliance connection can be reestablished

System action:
Processing continues. Audited events are buffered in the spill area.

User response:
Investigate the cause of the appliance connection interruption and correct.

AUIJ022W SPILL AREA IS FULL: EVENT DATA IS BEING LOST *(connection_type)*

Explanation:
A connection to the appliance was interrupted. The spill area was being used to buffer audited events until the appliance connection can be reestablished. The number of audited events that were generated exceeded the number that could be held in the spill area.

System action:
Processing continues. Audited events are discarded.

User response:
Investigate the cause of the appliance connection interruption and correct. Look for message AUIJ024W, which is issued at task termination or when a connection is reestablished, for the number of lost events.

AUIJ023E SPILL AREA IS NOT AVAILABLE *(connection_type)*

Explanation:
An attempt to use the spill area to buffer audited events is unsuccessful.

System action:
Processing continues. Audited events are discarded.

User response:
Specify a value of 1 through 1024 in the SAUISAMP AUICONFG member <SPILL-SIZE> parameter. Review any z/OS error or warning messages that might indicate why the spill area allocation failed.

AUIJ024W NUMBER OF *type* EVENTS LOST *count*

Explanation:
Attempts to buffer audited events in the spill area have failed. This message indicates the type of audited events (DLIO, DLIB, SMF etc) which were lost (*type*), and the number that were lost (*count*).

System action:
Processing continues. Audited events are discarded.

User response:
Investigate the cause of the appliance connection interruption and correct.

AUIJ042W ZIIP PROCESSING NOT AVAILABLE ON THIS LPAR (type)

Explanation:
A request to process data, using a zIIP enabled enclave, has failed because the Workload Manager feature is not available.

System action:
Processing continues, using GCPU (General Central Processor Unit) services.

User response:
Remove the ZIIP_AGENT_DLI(Y) keyword from the configuration file that is in use, or change the parameter from Y to N.

AUIJ044W ZIIP PROCESSING REQUEST HAS BEEN REJECTED *(connection_type)*

Explanation:
An attempt to create a zIIP enabled enclave has failed.

System action:
Processing continues using GCPU services.

User response:
Determine the cause of the failure by reviewing previously issued AUIJ0331E messages and take corrective action.

AUIJ055I ZIIP PROCESSING REQUESTED FOR *type* PROCESSING

Explanation:
The use of a zIIP enabled enclave has been requested by the use of the ZIIP_AGENT_DLI(Y) configuration file keyword.

System action:
An attempt is made to create the enclave.

User response:
No action is required.

AUIJ056I ZIIP PROCESSING ENABLED FOR type PROCESSING, ENCLAVE TOKEN: *value*

Explanation:
A zIIP enabled enclave has been requested and successfully created.

System action:
Processing continues.

User response:
No action is required.

AUIJ057W ZIIP PROCESSING FOR *type* EVENTS HAS BEEN DISABLED DUE TO ERRORS - PROCESSING WILL CONTINUE USING GCPU

Explanation:
zIIP processing was requested, however due to previously reported errors, this mode of processing could not be enabled.

System action:
Processing continues using General Central Processing Unit (GCPU) resources only.

User response:
Review the processing log looking for error and warning messages that were issued prior to this message to help determine why zIIP processing could not be initiated.

AUIJ058W ZIIP PROCESSING FOR *type* EVENTS HAS BEEN DISABLED - TRACING IS ENABLED BY THE USE OF THE AUI$NAP JCL STATEMENT

Explanation:
Event tracing has been enabled through the addition of the AUI$NAP DD SYSOUT=* JCL statement in the agent JCL. The use of zIIP processing has been disabled because event tracing cannot coexist with the zIIP environment.

System action:
All processing continues with event tracing on. Processing occurs on the General Central Processing Unit (GCPU).

User response:
If the addition of the AUI$NAP DD statement was not intentional, remove it from the agent JCL.

AUIJ201E VSAM ERROR ENCOUNTERED

Explanation

FUNCTION
vsam_function

RPL/RECORD TYPE
rpl/record_value

R15
return_code

R0
reason_code

CSI-CALL
function_call

SUBRTN
pgm_routine

While accessing the VSAM repository, an internal logic error was encountered.

System action:
Processing terminates.

User response:
There are no user actions available for this failure. Contact IBM Software Support with the content of this message.

AUIJ202E VSAM ERROR ENCOUNTERED

Explanation
While accessing the VSAM repository, an internal logic error was encountered.

FUNCTION:
vsam_function

R15:
return_code

ACBOFLGS:
acboflag_value

CSI-CALL:
function_call

SUBRTN:
pgm_routine

System action:
Processing terminates.

User response:
There are no user actions available for this failure. Contact IBM Software Support with the content of this message.

AUIJ203E VSAM ERROR ENCOUNTERED

Explanation
While accessing the VSAM repository, an internal logic error was encountered.

FUNCTION:
vsam_function

RPL/RECORD TYPE
rpl/record_value

FDBWD:
rpl_fdbwd

OPTCD:
rpl_optcd

CSI-CALL:
function_call

SUBRTN:
pgm_routine

System action:
Processing terminates.

User response:
There are no user actions available for this failure. Contact IBM Software Support with the content of this message.

AUIJ250I AUDITING IMS EVENTS. COLLECTION PROFILE NAME: *collection_profile_name* IMS

NAME: *ims_name* AGENT NAME: *agent name* EXCLUDED REGIONS: *region_types*

Explanation:
The auditing of IMS events proceeds by using the collection profile (*collection_profile_name*) that is associated with the IMS definition (*ims_name*). The agent name indicates which agent is processing the audited data. Various region types might have been excluded from auditing, such as AER, BMP, CICS, DBCTL, IFP, MPP, ODBA, or NONE.

System action:
Auditing continues.

User response
No action is required.

Note: To set a z/OS message alert for this message, use single-dash formatting between the message number and message text; for example, AUIJ250I - AUDITING IMS EVENTS.

AUIJ251E **COMPILED FILTER BUILD FAILED. COLLECTION PROFILE NAME : *collection _profile_name* RC: *return_code* RSN: *reason_code***

Explanation:
An attempt at building a compiled filter using the collection profile named (*collection_profile_name*) failed.

System action:
Processing terminates, auditing will not be performed.

User response:
Contact IBM Software Support.

AUIJ252W **GUARDIUM QUARANTINE IS IN EFFECT; DBPCB STATUS CODES OF *AI* MAY OCCUR**

Explanation:
The Guardium appliance has detected a list of users for whom access is to be restricted for a period of time. This list is based on policy rules and criteria that are set by the Guardium administrator who maintains the auditing rules in your environment.

System action:
Processing continues. If a user in the list of quarantined user IDs attempts to issue DB/DLI calls, the DLI call fails. A DB PCB status code of AI, or an AIB return/reason code of 110/C, is returned to the application program.

User response
If access to IMS databases terminate with a DB PCB status code of AI, or an AIB return/reason code of 110/C, contact the Guardium administrator who maintains the auditing rules in your environment to obtain the reason for the quarantine.

Note: To set a z/OS message alert for this message, use single-dash formatting between the message number and message text; for example, AUIJ252W - GUARDIUM QUARANTINE IS IN EFFECT

AUIJ255I **AUII050I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name***

Explanation:
This message echoes message AUII050I, which is generated by the S-TAP code, and can appear in the IMS control region and the DLI/DBB batch job output. This message only appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

System action:
Processing continues.

User response:
No action is required. See the explanation for message AUII050I for details regarding the available output fields.

AUIJ256I **AUIJ250I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID : *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name***

Explanation:
This message echoes message AUIJ250I, which is generated by the S-TAP code, and can appear in the IMS control region and the DLI/DBB batch job output. This message only appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

System action:
Processing continues.

User response:
No action is required. See the explanation for message AUIJ250I for details regarding the available output fields.

AUIJ257I **AUII120I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name***

Explanation:
This message echoes message AUII120I, which is generated by the S-TAP code, and can appear in the IMS control region and the DLI/DBB batch job output. This message only appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

System action:
Processing continues.

User response:
No action is required. See the explanation for message AUII120I for details regarding the available output fields.

AUIJ258I **AUII052I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name***

Explanation:
This message echoes message AUII052I, which is generated by the S-TAP code, and can appear in the IMS control region and the DLI/DBB batch job output. This message only appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

System action:
Processing continues.

User response:
No action is required. See the explanation for message AUII052I for details regarding the available output fields.

AUIJ259I **JOBNAME *job_name* USING IMS STAP V10.1.3 MODULE: *pgm_name* APAR: *fix_number* DATE: *fix_date***

Explanation:
This message echoes message AUII052I, which is generated by the S-TAP code, and can appear in the IMS control region. This message appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

User response:
No action is required.

AUIJ303W ***request_type* REQUEST FOR LOG STREAM *log_stream_name* FAILED - RC: *return_code* RS: *reason_code* - WILL CONTINUE TO RETRY**

Explanation:
A request (*request_type*) made to the indicated log stream (*log_stream_name*) has failed. This is a recoverable situation and the request will be retried.

System action:
Processing will continue with the request being retried.

User response:
No action is required.

AUIJ304A **IXGCONN REQUEST FOR LOG_STREAM *log_stream_name* FAILED with RC = *return_code* and RS= *reason_code***

Explanation:
An attempt to connect to the z/OS System Logger log-stream, by using the IXGCONN function, has failed.

System action:
Auditing is disabled, but IMS continues processing.

User response:
Correct the issue that has caused the IXGCONN failure; then, uninstall and reinstall the policy to cause IMS to reattempt the connection. Or, correct the issue; then, stop and restart the agent to cause IMS to reattempt the IXGCONN call.

AUIJ304E **IXGWRITE REQUEST FOR *<log-stream-name>* FAILED - RC: *return_code* RS: *reason_code***

Explanation:
An attempt to write to the z/OS System Logger log-stream using the IXGWRITE function has failed.

System action:
One occurrence of this message is issued once per error type (RC + RSN) within the each issuance of message AUII050I. IXGWRITE calls continues until the collection policy for the IMS system is uninstalled, or the DLI/DBB batch job or IMS control region terminates.

User response:
Examine the description of the IXGWRITE error using the RC and RSN codes provided in the IBM z/OS MVS Programming: Assembler Services Reference, Vol. 2 (IAR-XCT) or equivalent, under the IXGWRITE Macro description, and take corrective action. The most common reason for the appearance of this message is the volume and the rate (number of events per second) of DLI events exceeds the capacity of the current z/OS System Logger log stream definition.

AUIJ307A **AUDITED EVENTS ARE BEING LOST DUE TO IXGWRITE ERRORS AND/OR BUFFER SHORTAGES**

Explanation:
A number of attempts to write audited events to the z/OS System Logger Log-stream have failed which has caused has resulted in available space in the data buffers being exhausted. This has resulted in DLI events which are to be audited to be discarded.

System action:
DLI events continue to be audited at attempts to write exiting data buffers to the z/OS System Logger Log-stream until. The number of DLI events which were rejected are noted in subsequent AUII050I message.

User response:

Review any AUIJ304E messages which have been issued to determine the cause of the z/OS System Logger Log-stream Write failures.

AUIJ307E ***thread_type* THREAD IS TERMINATING DUE TO PROCESSING ERRORS.**

Explanation:
The agent has determined that a fatal error or abend occurred in the thread type indicated.

System action:
Processing that is associated with this thread will not occur.

User response:
Examine previously issued error or abend messages to determine the corrective action to be taken. Then, restart the agent.

AUIJ330E **REQUIRED DATA SET IS NOT CATALOGED. - TYPE: *dsn_type*, DSN: *data_set_name***

Explanation:
The data set name indicated (data_set_name) was not found in the z/OS catalog.

System action:
Processing terminates

User response:
Specify the name of a cataloged data set.

AUIJ331E ***service_name* SERVICE FAILED - RC: *return_code* - RSN: *reason_code***

Explanation:
A z/OS service (*service_name*) failed when executed.

System action:
Processing terminates.

User response:
Determine the cause of the failure by using the return and reason codes provided. Contact IBM Software Support for additional assistance.

AUIJ332E **DATA SET IS NOT VALID WITHIN CONTEXT USED - TYPE: *data_set_type,* DSN: *data_set_name*, REASON: *reason***

Explanation:
The data set indicated (*data_set_name*) is not of a type valid for use where it is defined. The reason for the rejection of this data set is found in the REASON field (*reason*).

System action:
Processing terminates

User response:
Specify a data set of the correct type.

AUIJ333E **Service *SERVICE FAILED* for *DATA SET*: *dsn - R15: return_code***

Explanation:
A z/OS LOCATE or OBTAIN service failed when it was run against the specified data set dsn.

System action:
Processing terminates.

User response:
Ensure that the data set names exists, and has not been migrated. Determine the cause of the failure by examining the LOCATE/OBTAIN MACRO return codes found in the *IBM DFSMSdfp Advanced Services* manual. Contact IBM Software Support for additional assistance

AUIJ335W ***dd_name* DD IS PRESENT IN THIS JCL, *dsn_types* WILL NOT BE AUDITED**

Explanation:
The AUIF*stc* task has encountered a DD in the JCL that prevents a specific type of data set from being audited by SMF.

System action:
Accesses to the data set types that are specified in the text of this message are not audited.

User response:
If you want to audit accesses to these types of data sets, remove the DD statement. See the Data sets and DD DUMMY statements table in the SMF records section of this user's guide for information on which DDs affect which data set types.

AUIJ400E **INSUFFICIENT MEMORY - MODULE NAME: *program_name* - MEMORY SEGMENT TYPE: *seg_type***

Explanation:
An attempt at obtaining memory in program (*module_name*) has failed due to insufficient memory being available.

System action:
Processing terminates

User response:
Increase the region size of the started task where this message appeared. Restart the started task and retry the request.

AUIJ401E **MODULE *module_name* FAILED DURING ATTACH of *program_name* - RETURN CODE: *return_code***

Explanation:
An attempt to perform a z/OS ATTACH of the program_name by module module_name has failed.

System action:
Processing terminates.

User response:
Determine the cause of the failure by using the return code (*return_code*) provided. Correct and restart the task that issued the message. Contact IBM Software Support for further assistance if need.

AUIJ402E **CATALOG SERVICE REQUEST FAILED - MODULE NAME: *module_name* - RC: *return_code* RSN: *reason_code***

Explanation:
An attempt use the catalog interface has failed.

System action:
Processing terminates

User response:
Contact IBM Software Support.

AUIJ403E **DYNAMIC ALLOCATION FAILURE - FUNCTION : *function_code* - DSN: *data-set-name* - RC: *return_code* RSN: *reason_code***

Explanation:
An attempt to issue a dynamic allocation function (*function_code*) using the data set name indicated (*data_set_name*) has failed.

System action:
Processing terminates.

User response:
Using the *return_code* and *reason_code* determine the cause for the failure. Correct and retry the request.

AUIJ404E **DYNAMIC ALLOCATION FAILURE - FUNCTION: *function_code* -DDN: *dd_name* - RC: *return_code* RSN: *reason_code***

Explanation:
An attempt to issue a dynamic allocation function (*function_code*) using the DD name indicated (*dd_name*) has failed.

System action:
Processing terminates.

User response:
Using the *return_code* and *reason_code* determine the cause for the failure. Correct and retry the request.

AUIJ406W **TOO MANY RULES SPECIFIED IN POLICY, REQUEST HAS BEEN TRUNCATED. POLICY: *policy_name*. RULE LIMIT: *max_number_of rules_allowed***

Explanation:
Preprocessing of the rules associated with the indicated policy (*policy_name*) determined that the number of rules that were specified in the policy exceeded the rule limit of *max_number_of rules_allowed*. Allowing an excessive number of rules causes memory constraint and performance issues.

System action:
The contents of subsequent rules are discarded. Processing continues using all previous rule content.

User response:
Review the rules that are included in the policy, and edit the policy to combine the rule content where permissible. If the resulting policy still requires a greater number of rules than the rule limit permits, contact IBM Software Support.

AUIJ407I ***number* DATA SETS ADDED TO POLICY *policy_name* FILTER**

Explanation:
This message provides the number of data set names that are used as input when building the compiled filter for SMF processing.

System action:
Processing continues.

User response:
No action is required.

AUIJ408E **POLICY *name* RESULTED IN OVER 102400 DATA SETS TO BE AUDITED; DATA SET RESULT SET HAS BEEN TRUNCATED**

Explanation:
The specified policy has found over 102,400 data sets to audit based on the databases that are specified in the policy rules and the IMS SLDS and RLDS RECON entries. The data set occurrence limit per policy is 102,400 per IMS definition due to memory constraints.

System action:
Remaining dataset names for the DBD that is being processed is included in the list to be audited, which might cause the 102,400 dataset limit to be slightly exceeded. The process that determines the DBD and DSN pairings is terminated, no additional rules within the policy are processed, and a filter is created for the policy based on the 102,400 (or more) dataset names. Normal processing continues.

User response:
Consider changing the policy rules to audit fewer databases or modify the rules to reduce or avoid multiple rules from auditing the same databases. Consider reviewing the IMS RECON dataset that is looking for IMS SLDS and RLDS, database image copy data sets, or database DSG/area data sets, which no longer physically exist but remain listed in the RECON.

Delete the RECON references that are no longer needed.

AUIJ500I **STARTING *cycle_type* CYCLE**

Explanation:
The task is starting the processing cycle specified.

System action:
Processing starts for the cycle specified.

User response:
No action is required.

AUIJ501I **NO NEW CATALOGED SMF DATA SETS FOUND FOR SMF MASK: - *smf_mask_value***

Explanation:
The SMF processing cycle has determined that no new, unprocessed data sets which meet the SMF mask value have been found.

System action:
The task waits for the start of the next cycle.

User response:
No action is required.

AUIJ504I ***cycle_type* CYCLE COMPLETE**

Explanation:
The cycle has completed.

System action:
The task waits for the start of the next cycle.

User response:
No action is required.

AUIJ521W **CONTROL BLOCK AUIDCCOM NOT FOUND**

Explanation:
A critical E/CSA control block was not found.

System action:
Processing terminates.

User response:
Contact Software Support.

AUIJ510I **ALTERNATE RECON DATA SETS FOUND FOR IMSNAME *imsname*: RECON1: *alt_dsn_1*; RECON2: *alt_dsn_2*, RECON3: *alt_dsn_3***

Explanation:
The AUIARCN DD was found in the JCL. The *imsname* that was used when installing the active IMS policy was found in the AUIARCN file, along with alternate RECON data sets names (*alt_dsn_1/2/3*).

System action:
Processing continues.

User response:
No action is required.

AUIJ511E **ALTERNATE RECON DATA SET NOT CATALOGED; DSN: *alt_dsn***

Explanation:
When attempting to validate the *alt_dsn* value, the data set was not found in the catalog.

System action:
Processing continues to validate other specified data set names.

User response:
Correct the data set name or catalog the data set.

AUIJ512E **ALTERNATE RECON DATA SET NOT A VSAM FILE; DSN: *alt_dsn***

Explanation:
When attempting to validate the *alt_dsn* value, the data set was found to in a format invalid for processing. The data set name must be in VSAM format.

System action:
Processing continues to validate other specified data set names.

User response:
Correct the data set name or catalog the data set.

AUIJ513E **NO VALID ALTERNATE RECON DATA SETS FOUND FOR IMS *imsname*; PROCESSING TERMINATED**

Explanation:
The data set validation was completed, and no valid alternate RECON data set names found for the IMSNAME.

System action:
Processing terminates.

User response:
Add or correct valid RECON data set names.

AUIJ522E **INSUFFICIENT E/CSA STORAGE AVAILABLE FOR *control_block* CONTROL BLOCK**

Explanation:
Insufficient E/CSA storage was available to hold the specified control block.

System action:
Processing terminates.

User response:
Determine the cause of the E/CSA shortage.

AUIJ609I ***event_types* ARE BEING EXCLUDED (*excluded_by*)**

Explanation:

If the *excluded_by* value is AGENT, then the reporting of *event_types* is excluded due to the specification of certain configuration keywords. If the *excluded_by* value is IMS, these events are excluded as directed by the IMS definition.

System action:
Occurrences of these event types are not reported.

User response:
If you want to view reports of this event type, review and modify the agent configuration file (SMF_AUDIT_LEVELS or IMSL_AUDIT_LEVELS keywords) or the Guardium system IMS definition, using the **Auditing Levels** tab.

AUIJ800E **REQUIRED DD STATEMENT IS MISSING: *dd-name***

Explanation:
A critical error has occurred due to a missing DD statement.

System action:
Processing terminates.

User response:
This message occurs if a product JCL has been edited and a DD statement has been deleted or omitted. If this is not the case, check for any dynamic allocation error messages. If none are present, or are not user resolvable, contact IBM Software Support.

AUIJ860E **VSAM FILE DEFINITION ERROR - DDN: *dd_name* - REASON: *definition_error***

Explanation:
When validating the VSAM repository, an allocation definition error was found.

System action:
Processing terminates.

User response:
The VSAM repository requires specific values for the attribute, LRECL, key length and key position. Review the SAUISAMP product distribution data set member AUISJ001 for the correct file definition specifications.

AUIJ999E **AN INTERNAL LOGIC ERROR HAS OCCURRED - MODULE: module_name RSN: reason_code**

Explanation:
An internal logic error has occurred.

System action:
Processing terminates

User response:
Contact IBM Software Support.

Error messages and codes: AUILxxxx

The following information is about error messages and codes that begin with AUIL.

AUIL002I **Archive log reader interval set to *<number> <time interval in hours/ minutes>*.**

Explanation:
The Archive log reader is scheduled to process archive logs as specified.

User response:
No action is required.

AUIL003E **Command *<command-text>*failed; interval value must be between *<lower-bound>* and *<upper-bound>*.**

Explanation:
This message indicates that <*command*>, such as: **/f AUILSTC,SET INTERVAL number** failed because of incorrect *number* value. Correct values must be between <*lower-bound*> and <*upper-bound*>.

User response:
Use an interval value between <*lower-bound*> and <*upper-bound*>. If that does not resolve the issue, contact IBM Software Support.

AUIL600I **NO NEW CATALOGED IMS LOG DATA SETS FOUND**

Explanation:
After examining the RECON data sets, it has been determined that no new IMS SLDS data sets were found that have yet to be processed by the product.

User response:
No action is required.

AUIL601I **PROCESSING IMS LOG DATA SET: *ims_log_data_set_name***

Explanation:
Processing has started for the IMS SLDS data set indicated (*ims_log_data_set_name*)

System action:
Processing continues.

User response:
No action is required.

AUIL602I **PROCESSING COMPLETE FOR IMS LOG DATA SET: *ims_log_data_set_name***

Explanation:
Processing of the IMS SLDS data set has completed.

System action:
Processing continues with other candidate IMS SLDS data sets.

User response:
No action is required.

AUIL603I **SCANNING RECON DATA SETS FOR IMS LOGS TO PROCESS. RECON1: *recon1_dsn* - RECON2: *recon2_dsn* - RECON3: *recon3_dsn***

Explanation:
To determine the candidate IMS SLDS data sets to be read, the IMS RECON data sets must be queried. This message indicates that this query process has started.

System action:
Processing continues.

User response:
No action is required.

AUIL605I **RECON DATA SET SCAN COMPLETE**

Explanation:
This message follows the AUIL603I message and indicates that the scan of the RECON data sets is complete.

System action:
Processing continues.

User response:
No action is required.

AUIL606W **RECON HAS NOCATDS SPECIFIED, RESULTS MAY NOT BE ACCURATE**

Explanation:
When examining the RECON data sets the NOCATDS option was found to be on, meaning any log data sets found might not be cataloged.

System action:
Processing continues.

User response:
The function that produces this message relies on the log data sets existing in the z/OS catalog or having been in the z/OS catalog at one time. Having the NOCATDS option on in the RECON data sets might negate the validity of further processing, if the SLDS data sets are not cataloged.

AUIL607W **THERE ARE NO ACTIVE IMS POLICIES FOR AGENT *agent_name***

Explanation:
A request to query the RECON data sets of IMS systems defined under the named agent found that there were no IMS systems audited by the agent with an active profile. The function that produces this message relies on having at least one IMS system with an active collection policy.

System action:
Processing terminates.

User response:
Install a collection policy for an IMS under of the control the agent.

AUIL701I **IMS LOG CHECKPOINT INFORMATION - IMSID: *IMS_name_from_policy* - RECON1 DSN: *dsn_of_RECON1* - CREATING SSID: *SSID_from_PRILOG* - LAST DSN READ: *dsn_of_SLDS* - LAST UPDATED (UTC): *date_time***

Explanation:
This message provides the name of the IMS SLDS that was last read when processing data for the SSID (*SSID_from_PRILOG*) found in the set of the DBRC RECON data sets (*dsn_of_RECON1*). This information is used as a checkpoint to indicate which SLDS data sets have already been processed, and should not be re-read by the AUILstc tasks.

System action:
Processing continues.

User response:
No action is required.

Error messages and codes: AUIPxxxx

The following information is about error messages and codes that begin with AUIP.

AUIP001E **A protobuf message schema violation was detected; value *value* is not a valid boolean value.**

Explanation:
The specified value is not valid.

User response:
Contact your administrator or IBM Software Support.

AUIP002E **A protobuf message schema violation was detected; value *value* is not a valid double value.**

Explanation:
The specified value is not valid.

User response:
Contact your administrator or IBM Software Support.

AUIP003E **A protobuf message schema violation was detected; value *value* is not a valid integer value.**

Explanation:
The specified value is not valid.

User response:
Contact your administrator or IBM Software Support.

AUIP004E **A protobuf message schema violation was detected; required message *message* property *property* is not present.**

Explanation:
The specified message property is not present.

User response:
Contact your administrator or IBM Software Support

AUIP005E **A protobuf message schema violation was detected; required message *message* sub-message *submessage* is not present.**

Explanation:
The specified message submessage is not present.

User response:
Contact your administrator or IBM Software Support.

AUIP006S **A severe error occurred during protobuf message parsing; an unknown exception occurred.**

Explanation:
An error occurred while parsing a protobuf message.

User response:
Contact your administrator or IBM Software Support.

AUIP007E **A protobuf message schema violation was detected; property name *property* is invalid.**

Explanation:
The specified property name is not valid.

User response:
Contact your administrator or IBM Software Support.

AUIP008E **A protobuf message schema violation was detected; property *property* value *value* is invalid.**

Explanation:
The specified property value is not valid.

User response:
Contact your administrator or IBM Software Support.

AUIP009E **A protobuf message schema violation was detected; message name 'name' is invalid.**

Explanation:
The specified message name is not valid.

User response:
Contact your administrator or IBM Software Support.

AUIP010E **A protobuf message schema violation was detected; message name *name* is invalid (expected *expected name*).**

Explanation:
The specified message name is not valued.

User response:
Contact your administrator or IBM Software Support.

AUIP011E **A protobuf message schema violation was detected; value *value* is not a valid bytes value.**

Explanation:
The specified value is not valid.

User response:
Contact your administrator or IBM Software Support.

AUIP012E **A protobuf message schema violation was detected; value *value* is not a valid unsigned integer value.**

Explanation:
The specified value is not valid.

User response:
Contact your administrator or IBM Software Support.

AUIP013E **An error occurred while parsing item text: String is empty.**

Explanation:
A policy message contained an item field with an empty value.

User response:
Contact your administrator or IBM Software Support.

AUIP014E **An error occurred while parsing item text: text.**

Explanation:
A policy message contained an item field with a value *text* could not be parsed successfully.

User response:
Contact your administrator or IBM Software Support.

AUIP015E **Failed to send error message to appliance: *host/port*.**

Explanation:
The IBM Guardium S-TAP for IMS agent was unable to send the error message to the specified appliance.

User response:
Contact your administrator or IBM Software Support.

AUIP016E **Policy rule <rule> was ignored: IMS name is empty.**

Explanation:
The specified policy rule was ignored because it does not apply to any IMS subsystem, or the IMS name is empty.

User response:
Contact your administrator or IBM Software Support.

Error messages and codes: AUIRxxxx

The following information is about error messages and codes that begin with AUIR.

AUIR002E **The provided *parameter 'value'* is too long; should be less than or equal to *maximum length* characters.**

Explanation:
The value of the specified *parameter* exceeds the maximum length *maximum length*.

User response:
Specify a shorter value that does not exceed the specified limit for the parameter.

AUIR004E **A maximum of *maximum* data sets are allowed for the *names* libs and a total of *libs-count* were specified.**

Explanation:
The maximum number of data sets was exceeded for the libs specified.

User response:
Limit the number of data sets for the specified libs to *maximum*.

AUIR006E **The parameter *parameter* can't be empty.**

Explanation:
The parameter value must be specified in the agent configuration.

User response:
Update agent configuration, or contact your administrator.

AUIR007W **Policy_rule_item *<item-name>* for Policy_rule *<rule-name>* has conflicting *<value-name>* values.**

Explanation:
The Guardium policy was processed but there are conflicting fields in the definition. Only one of the policies has been applied.

User response:
Check the policy definition, and change the specified values to eliminate the conflict.

AUIR008W **IMS 050i Max Time threshold was changed from "2460" to "2359".**

Explanation:
An invalid time value was supplied through the use of the **Message AUII050I Frequency** field of the IMS definition screen of the Guardium appliance. The invalid value was automatically corrected by the agent.

System action:
Processing continues.

User response:
When convenient, update the invalid time value in the IMS definition to a value within the range of 00:10 -- 23:59.

Error messages and codes: AUITxxxx

The following information is about error messages and codes that begin with AUIT.

AUIT001E **The specified user ID *userid* is not defined or does not have an OMVS segment defined.**

Explanation

You specified a user ID that is not defined or does not have an OMVS segment defined.

User response

was unable to authenticate the specified user. Either specify a valid user ID, or if the user ID is valid, see your security administrator to have an OMVS segment defined for the user ID.

AUIT006S **The product is not properly configured to authenticate users.**

Explanation:
is not properly configured to authenticate users.

User response:
An error occurred while authenticating a remote user request. The error code indicates that the installation configuration required to allow this authentication has not been completed. See “IBM Guardium S-TAP for

IMS agent" on page 2 for more information about how to complete the required configuration.

AUIT008E **The configuration file *filename* is invalid; the root element *element* is not <agent-config>.**

Explanation

The configuration file identified in the message is invalid.

User response

The contents of the specified configuration file are invalid. Correct the file contents to specify <agent-config> as the root XML element.

AUIT010E **An error occurred while opening the configuration file *filename message text***

Explanation

An error occurred while opening the configuration file identified in the message. Additional error information is also contained within the message.

User response

Use the specified message text to diagnose the error that occurred. Specify a valid configuration file that is not in use by any other process.

AUIT012I **Performing discovery of available locations.**

Explanation

The agent is looking for available locations.

User response

No action is required.

AUIT013I **agent is terminating.**

Explanation

The agent is terminating.

User response

No action is required.

AUIT014I **Connected to server *<host>* on port *<port>*.**

Explanation

The Security Guardium S-TAP for IMS agent task has connected to the S-TAP to the specified host and port.

User response

No action is required.

AUIT015I **Attempting connection to server *<host>* on port *<port>*.**

Explanation

The Security Guardium S-TAP for IMS agent is attempting to connect to the specified host and port number.

User response

No action is required.

AUIT017I **Discovered subsystem *subsystem-id*.**

Explanation

The agent has discovered the identified subsystem.

User response

No action is required.

AUIT019I **agent started on *<lpar _name> (<lpar_ip>)*.**

Explanation

The IBM Guardium S-TAP for IMS agent has started.

User response

No action is required.

AUIT020I **Starting the socket selector thread (thread *thread id*).**

Explanation

The agent is starting the identified socket selector thread.

User response

No action is required.

AUIT023I **Received shutdown request.**

Explanation

The agent has received a shutdown request.

User response

No action is required.

AUIT025I **The socket selector thread is terminating.**

Explanation

The agent socket selector thread is terminating.

User response

No action is required.

AUIT028E **An error occurred while authenticating user *user-id error-text*.**

Explanation

An unexpected return code was returned by the *pthread_security_np()* callable service.

User response

Ensure that the configuration required to use this service has been completed. See "IBM Guardium S-TAP for IMS agent" on page 2 for more information about the required configuration. Check the agent job log for additional messages which might be generated.

AUIT031I **Starting the command listener thread (thread *thread-id*).**

Explanation

The agent is starting the command listener thread.

User response

No action is required.

AUIT032I **Received stop command: *command-text*.**

Explanation

The agent received a STOP command.

User response

No action is required.

AUIT033I **Received modify command: *command-text*.**

Explanation

The agent received a MODIFY command.

User response

No action is required.

AUIT034S **agent is terminating due to hard stop request.**

Explanation

agent is terminating due to a user /MODIFY FORCE command.

User response

No action is required.

AUIT044E **The connection to the server has been lost.**

Explanation:
The agent task is unable to communicate with the agent.

User response:
Resolve any network connectivity issues, then try logging in again.

AUIT047E **agent ended with RC = *[rc].***

Explanation:
Due to a prior error, the agent has ended with the specified return code.

User response:
Contact IBM Software Support.

AUIT048I **Issuing request to capture service dump.**

Explanation:
A command, such as **/f AUIASTC,DUMP/DDX**, has been issued for processing.

User response:
No action is required.

AUIT049I **Request to capture service dump has completed successfully.**

Explanation:
A command, such as **/f AUIASTC,DUMP/DDX** has processed successfully.

User response:
No action is required.

Error messages and codes: AUIUxxxx

The following information is about error messages and codes that begin with AUIU.

AUIUR002I **Migrate Utility for started.**

Explanation:

The utility to migrate the configuration of an older version of the product to the current product version has started.

User response:

No action is required.

AUIUR003I **Agent record *<agent name>* was not found in the repository.**

Explanation:
An attempt to read an agent record from the repository while migration failed as the record was not found.

System action:
The agent record migration fails, processing continues.

User response:
Check the configuration file for agent and repository names and use the Guardium user interface to verify that the specified agent definition is presented in specified repository.

Error messages and codes: AUIXxxxx

The following information is about error messages and codes that begin with AUIX.

AUIX013E **A shared memory error occurred on "*service name*": *error message*.**

Explanation

This error can occur in the primary agent address space. When the error occurs, the primary agent address space will shut down with a CC of 12. This startup error indicates that attempts to create a shared memory segment failed because of an already existing shared memory segment that never belonged to, or currently does not belong to, the primary agent address space.

This message can occur in the secondary address space if the <id> elements in the **ADS_SHM_ID** and **ADS_LISTENER_PORT** parameters do not match in the AUICONFG configuration member that is used by the agent primary address space and the secondary address spaces.

User response:
Edit SAUISAMP member AUICONFG (or the customized AUICONFG) and specify the correct <id> elements in the **ADS_SHM_ID** and **ADS_LISTENER_PORT** parameters.

AUIX014E **An XML schema violation was detected; value *value* is not a valid boolean value.**

Explanation

An XML schema violation was detected; value *value* is not a valid boolean value.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM Software Support.

AUIX015E **An XML schema violation was detected; value *value* is not a valid double value.**

Explanation

An XML schema violation was detected; value *value* is not a valid double value.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM Software Support.

AUIX016E **An XML schema violation was detected; value *value* is not a valid integer value.**

Explanation

An XML schema violation was detected; value *value* is not a valid integer value.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM Software Support.

AUIX017E **An XML syntax error was detected at offset *offset*; expected *expected-value*, found *found-value*.**

Explanation

An XML syntax error was detected at offset *offset*; expected *expected-value*, found *found-value*.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM Software Support.

AUIX018E **An XML schema violation was detected; required element *element* attribute *attribute*\" is not present.**

Explanation

An XML schema violation was detected; required element *element* attribute *attribute* is not present.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM Software Support.

AUIX019E **An XML schema violation was detected; required element *<element>* child *<child-element>* is not present.**

Explanation:
The XML schema must contain the specified elements.

User response:
Correct the XML schema and retry.

AUIX020E **Memory allocation failed (*number* bytes).**

Explanation

Memory allocation failed (*number* bytes).

User response

Contact IBM Software Support.

AUIX021E **An XML schema violation was detected; element *element* child *child-number* has wrong type.**

Explanation

An XML schema violation was detected; element *element* child *child-number* has wrong type.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM Software Support.

AUIX022E **An XML syntax error was detected; character reference *character-reference* is invalid.**

Explanation

An XML syntax error was detected; character reference *character-reference* is invalid.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM Software Support.

AUIX023E **An XML syntax error was detected; entity reference *entity-reference* is invalid.**

Explanation

An XML syntax error was detected; entity reference *entity-reference* is invalid.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM Software Support.

AUIX024E **An XML syntax error was detected; more than one element was found at the root of the document.**

Explanation

An XML syntax error was detected; more than one element was found at the root of the document.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM Software Support.

AUIX025E **An XML syntax error was detected; no element was found at the root of the document.**

Explanation

An XML syntax error was detected; no element was found at the root of the document.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM Software Support.

AUIX026E **An XML syntax error was detected; text was found at the root of the document.**

Explanation

An XML syntax error was detected; text was found at the root of the document.

User response

Contact IBM Software Support.

AUIX027S **A severe error occurred during XML parsing; an unknown exception occurred.**

Explanation

A severe error occurred during XML parsing; an unknown exception occurred.

User response

Contact IBM Software Support.

AUIX028E The command line option *<option name>* is invalid.

Explanation

The command line option, which is specified in the message text, is invalid.

User response

Correct the command line option and retry the operation. Review the IBM Guardium S-TAP for IMS client/server environment information for valid options.

AUIX034S A severe error occurred during command line processing; an unknown exception occurred.

Explanation

A severe error occurred during command line processing; an unknown exception occurred.

User response

Contact IBM Software Support.

AUIX035E The operation completed successfully.

Explanation

The operation completed successfully.

User response

No action is required.

AUIX036E The address family is not supported by the protocol family (*socket-return-code*).

Explanation

The address family is not supported by the protocol family (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX037E The operation is still in progress (*socket-return-code*).

Explanation

The operation is still in progress (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX038E Permission is denied (*socket-return-code*).

Explanation

Permission is denied (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX039E The network is down (*socket-return-code*).

Explanation

The network is down (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX040E No buffer space is available (*socket-return-code*).

Explanation

No buffer space is available (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX041E Too many sockets have been opened (*socket-return-code*).

Explanation

Too many sockets have been opened (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX042E The protocol is not supported (*socket-return-code*).

Explanation

The protocol is not supported (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX043E **The WSAStartup routine was not called (*socket-return-code*).**

Explanation

The WSAStartup routine was not called (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX044E **The protocol is the wrong type for the socket (*socket-return-code*).**

Explanation

The protocol is the wrong type for the socket (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX045E **The socket type is not supported (*socket-return-code*).**

Explanation

The socket type is not supported (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX046E **The destination network is unreachable (*socket-return-code*).**

Explanation

The destination network is unreachable (*socket-return-code*).

User response

Specify the correct host name or IP address.

AUIX047E **The socket handle is invalid (*socket-return-code*).**

Explanation

The socket handle is invalid (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX048E **The address is already in use (*socket-return-code*).**

Explanation

The address is already in use (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX049E **The function call was interrupted (*socket-return-code***

Explanation

The function call was interrupted (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX050E **The requested address is not available (*socket-return-code*).**

Explanation

The requested address is not available (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX051E **The connection was aborted (*socket-return-code*).**

Explanation

The connection was aborted (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX052E **The connection was refused by the partner (*socket-return-code*).**

Explanation

The connection was refused by the partner (*socket-return-code*).

User response

Verify that the correct port number was specified, and that the partner application has been started and is available.

AUIX053E **The connection was reset by the partner (*socket-return-code*).**

Explanation

The connection was reset by the partner (*socket-return-code*).

User response

The partner application ended the network connection. If this is unexpected, diagnose the partner application failure. Otherwise, no action is required.

AUIX054E The network message is too long (*socket-return-code*).

Explanation

The network message is too long (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX055E The network dropped the connection when reset (*socket-return-code*).

Explanation

The network dropped the connection when reset (*socket-return-code*

User response

Contact IBM Software Support.

AUIX056E An invalid parameter was specified (*socket-return-code*).

Explanation

An invalid parameter was specified (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX057E The socket is not connected (*socket-return-code*).

Explanation

The socket is not connected (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX058E The operation is not supported (*socket-return-code*).

Explanation

The operation is not supported (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX059E The socket has been closed (*socket-return-code*).

Explanation

The socket has been closed (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX060E The socket is already connected (*socket-return-code*).

Explanation

The socket is already connected (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX061S An unknown error occurred (*socket-return-code*).

Explanation

An unknown error occurred (*socket-return-code*).

User response

Contact IBM Software Support.

AUIX062E A socket error occurred on *socket-operation* with RC = *return code*: *message-text*.

Explanation

A socket error occurred.

User response

Use the specified message text to diagnose the error.

AUIX063E A socket select error occurred: *message-text*.

Explanation

A socket select error occurred.

User response

Use the specified message text to diagnose the error.

AUIX064E **An XML schema violation was detected; expected root element *element-expected*, but found *element-found* instead.**

Explanation

An XML schema violation was detected; expected root element *element-expected* , but found *element-found* instead.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM Software Support.

AUIX066E **An XML schema violation was detected; element *element* value *value* is invalid.**

Explanation

An XML schema violation was detected; element *element* value *value* is invalid.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM Software Support.

AUIX067E **An XML schema violation was detected; element name *element* is invalid.**

Explanation

An XML schema violation was detected; element name *element* is invalid.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM Software Support.

AUIX068E **An XML schema violation was detected; element name *element-found* is invalid (expected *element-expected*).**

Explanation

An XML schema violation was detected; element name *element-found* is invalid (expected *element-expected*).

User response

Contact IBM Software Support.

AUIX074E **An abend occurred: *<abend code>*.**

Explanation:
This message indicates a callable service abend has occurred. Additional diagnostic information might be present in the message when applicable.

User response:
Contact IBM Software Support.

AUIX076E **An XML schema violation was detected; element *element* attribute *attribute* value *value* is invalid.**

Explanation

An XML schema violation was detected; element *element* attribute *attribute* value *value* is invalid.

User response

Contact IBM Software Support.

AUIX085E **A dynamic allocation error occurred: info code = *info-code*, error code = *error-code*.**

Explanation

A dynamic allocation error occurred: info code = *info-code*, error code = *error-code*.

User response

See the *MVS Programming: Authorized Assembler Services Guide* for more information about the specified information and error codes.

AUIX086E **A dynamic concatenation error occurred: info code = *info-code*, error code = *error-code*.**

Explanation

A dynamic concatenation error occurred: info code = *info-code*, error code = *error-code*.

User response

See the *MVS Programming: Authorized Assembler Services Guide* for more information about the specified information and error codes.

AUIX087E **A dynamic free error occurred: info code = *info-code*, error code = *error-code*.**

Explanation

A dynamic free error occurred: info code = *info-code*, error code = *error-code*.

User response

See the *MVS Programming: Authorized Assembler Services Guide* for more information about the specified information and error codes.

AUIX088E **An invalid dynamic allocation parameter was specified: code = *parm-code*.**

Explanation

An invalid dynamic allocation parameter was specified: code = *parm-code*.

User response

Contact IBM Software Support.

AUIX093S **An unexpected error occurred (*file-name*, *line-number*).**

Explanation

An unexpected error occurred (*file-name*, *line-number*).

User response

Contact IBM Software Support.

AUIX094S **An unexpected error occurred with token *token*, (*file-name*, *line-number*).**

Explanation

An unexpected error occurred with token *token*, (*file-name*, *line-number*).

User response

Contact IBM Software Support.

AUIX095S **An unexpected error occurred with tokens *token* and *token* (*file-name*, *line-number*).**

Explanation

An unexpected error occurred with tokens *token* and *token* (*file-name*, *line-number*).

User response

Contact IBM Software Support.

AUIX096S **An unexpected error occurred with tokens *token*, *token* and *token* (*file-name*, *line-number*).**

Explanation

An unexpected error occurred with tokens *token*, *token* and *token* (*file-name*, *line-number*).

User response

Contact IBM Software Support.

AUIX097S **An unexpected error occurred with tokens *token*, *token*, *token*, and *token* (*file-name*, *line-number*.**

Explanation

An unexpected error occurred with tokens *token*, *token*, *token*, and *token* (*file-name*, *line-number*.

User response

Contact IBM Software Support.

AUIX098E **A thread error occurred on *thread-operation* : *message-text*.**

Explanation

A thread error occurred on *thread-operation* : *message-text*.

User response

Use the specified message text to diagnose the error.

AUIX101E **An event error occurred on *event-operation* : *message-text*.**

Explanation

An event error occurred on *event-operation* : *message-text*.

User response

Use the specified message text to diagnose the error.

AUIX104E **A mutex error occurred on *mutex-operation* : *message-text*.**

Explanation

A mutex error occurred on *mutex-operation* : *message-text*.

User response

Use the specified message text to diagnose the error.

AUIX109E **A semaphore error occurred on *semaphore-operation* : *message-text*.**

Explanation

A semaphore error occurred on *semaphore-operation* : *message-text*.

User response

Use the specified message text to diagnose the error.

AUIX110I The network connection has been disconnected.

Explanation

The network connection has been disconnected.

User response

No action is required.

AUIX114E A dynamic allocation query error occurred: info code = *info-code*, error code = *error-code*.

Explanation

A dynamic allocation query error occurred: info code = *info-code*, error code = *error-code*.

User response

See the *MVS Programming: Authorized Assembler Services Guide* for more information about the specified info and error codes.

AUIX115E An input command error occurred on \"*command-operation*\": *message-text*.

Explanation

An input command error occurred on \"*command-operation*\": *message-text*.

User response

Contact IBM Customer Support.

AUIX116I Received input command: *command-text*.

Explanation

Received input command: *command-text*.

User response

No action is required.

AUIX122I Build date *component* = *date*.

Explanation

Build date *component* = *date*.

User response

No action is required.

AUIX123W The action was cancelled.

Explanation

The action was cancelled.

User response

No action is required. The operation was cancelled due to user or administrator request.

AUIX124S The task is not running APF-authorized.

Explanation

The task is not running APF-authorized.

User response

The load library, and the load libraries for all of the IMS subsystems accessed, must be APF-authorized. See "IBM Guardium S-TAP for IMS agent" on page 2 for more information about the required configuration steps.

AUIX126E A DLL error occurred on *dll-operation* : *message-text*

Explanation

A DLL error occurred on *dll-operation* : *message-text*

User response

Contact IBM Customer Support.

AUIX127S An error occurred while opening log file *file-name*.

Explanation

An error occurred while opening log file *file-name*.

User response

Contact IBM Customer Support.

AUIX142E An XML schema violation was detected; element *element* value *value* is invalid: expected min *<min-value>* and max *<max value>*.

Explanation:

The *element-value* given for *element-name* is out of the range and must be within *min-value* and *max-value*.

User response:
Correct the value for the *element-name* in the configuration.

AUIX143E **An XML schema violation was detected; element *element* attribute *value* value *value* is invalid: expected min *<minimum>* and max *<maximum>*.**

Explanation:
The element attribute value is not valid.

User response:
If the error occurred while reading the agent configuration file, update the configuration. Otherwise, contact IBM Software Support.

AUIX149E **Data set *[data set]* is not cataloged.**

Explanation:
The data set specified in the message text has not been cataloged.

User response:
Allocate the data set.

AUIX150E **Invalid data set *'data set'*: Data set name must not exceed 44 characters.**

Explanation:
MVS data sets cannot exceed 44 characters.

User response:
Correct the data set entry, then retry.

AUIX151E **Invalid data set *{'data set'}*: The segment length must be greater than 0 and less than or equal to 8.**

Explanation:
The specified data set name has one or more segments that are not between 1 and 8 characters.

User response:
Specify a data set where each segment contains more than 0 characters and 8 or fewer characters.

AUIX152E **Invalid data set *'name'*: The first character in each segment must be alphabetic (A-Z) or national (#, @, $).**

Explanation:
The data set name provided does not is not a valid name and does not satisfy the MVS data set naming requirements.

User response:
Correct the data set name and try again.

AUIX153E **Invalid data set *'<data set>'*: The non-first characters in the segments must be alphabetic (A-Z), numeric, national (#, @, $), or hyphen.**

Explanation:
The non-first characters in the segments must be alphabetic (A-Z), numeric, national (#, @, $), or hyphen.

User response:
Specify a data set where non-first characters in the segments is alphabetic (A-Z), numeric, national (#, @, $), or hyphen.

AUIX154E **Invalid data set *'<data set>'*: The non-first characters in the SMF segments must be alphabetic (A -- Z), numeric, national (#, @, $), hyphen, asterisk (*) or percent (%).**

Explanation:
The non-first characters in the SMF segments must be alphabetic (A -- Z), numeric, national (#, @, $), hyphen, asterisk (*) or percent (%).

User response:
Specify a data set where non-first characters in the SMF segments is alphabetic (A -- Z), numeric, national (#, @, $), hyphen, asterisk (*) or percent (%).

AUIX155E **Data set *<data set>* is not APF-authorized.**

Explanation:
The specified data set requires APF authorization.

User response:
The specified data set must be APF-authorized. See Chapter 4, “Configuration overview,” on page 11 for more information about the required configuration steps.

AUIX156E **Invalid data set *'<data set>'*: The first character in SMF segment must be alphabetic (A -- Z) or national (#, @, $), asterisk (*) or percent (%).**

Explanation:
The first character in SMF segment must be alphabetic (A -- Z) or national (#, @, $), asterisk (*) or percent (%).

User response:
Specify a data set where first character in SMF segments must be alphabetic (A -- Z) or national (#, @, $), asterisk (*) or percent (%).

AUIX160E **A dynamic allocation query error occurred: info code = *<info-code>*,**

error code = *<error-code>*, DD name = *<dd-name>*.

Explanation:
A dynamic allocation query error occurred with the specified information code, error code, and DD name.

User response:
See the *MVS Programming: Authorized Assembler Services Guide* for more information about the specified info and error codes.

AUIX183E **The number of file descriptors (sockets) has exceeded maximum = *<number>*.**

Explanation:
The active program holds too many file or socket descriptors and exceeded system maximum = *<number>*.

User response:
Contact your system administrator or IBM Software Support.

Error messages and codes: AUIYxxxx

The following information is about error messages and codes that begin with AUIY.

AUIY001E **A callable services abend *abend* has occurred.**

Explanation:
This message indicates a callable service abend has occurred. Additional diagnostic information is be present in the message when applicable.

User response:
Contact IBM Software Support.

AUIY002E **GPRS *number-number*: *hex-value hex-value hex-value hex-value***

Explanation:
This message indicates an CSI abend has occurred. Additional diagnostic information is present in the message when applicable.

User response:
No action is required.

AUIY003E **Active module not found.**

Explanation:
This message indicates a CSI abend has occurred. Additional diagnostic information is present in the message when applicable.

User response:
No action is required.

AUIY004E **Active module = *module-name*, load point = *hex-address*, offset = *hex-address***

Explanation:
This message indicates a CSI abend has occurred. Additional diagnostic information is present in the message when applicable.

User response:
No action is required.

AUIY005E **PSW = *string string***

Explanation:
This message indicates a CSI abend has occurred. Additional diagnostic information is present in the message when applicable.

User response:
No action is required.

AUIY006E **Callable service invocation failed with return code = *return-code* and reason code = *reason-code***

Explanation:
A service requested by the agent task has failed.

User response:
View the JES log of the agent task to determine the data set name and reason for the error. Contact IBM Software Support if you are unable to resolve the error.

AUIY007I **Invoking callable service *callable service*.**

Explanation:
The specified callable service has been invoked successfully.

User response:
No action is required.

AUIY008I **Returned from callable service *service-name***

Explanation

Returned from a callable service that is identified in the message.

User response

No action is required.

AUIY009E **Invalid data set mask: *data set mask*.**

Explanation:
The specified data set mask is not valid.

User response:
Enter a valid data set mask and retry.

Error messages and codes: AUIZxxxx

The following information is about error messages and codes that begin with AUIZ.

AUIZ002E ***dd-name*** **DD has already been allocated.**

Explanation:
The *dd-name* DD needed for the task, has been previously allocated.

System action:
The task terminates with a return code of 12.

User response:
dd-name DD is dynamically allocated. Ensure that the *dd-name* DD is not present in the task JCL. If the *dd-name* is not present in the JCL, contact IBM Software Support.

AUIZ003W **Attached to existing shared memory segment.**

Explanation:
This message corresponds to message AUIZ008W. This message indicates that the memory segment has been cleaned, and is being reused.

User response:
No action is required.

AUIZ004S **Shared memory segment key verification failed ('*key-value*').**

Explanation:
Shared memory segment validation failed. This usually implies that the shared memory segment is owned by another product or system.

User response
Change shared memory segment id and restart the agent:

```
ADS_SHR_MEM_ID
```

AUIZ005S **Shared memory segment eyecatcher 'value' invalid.**

Explanation:
Shared memory segment validation failed. This implies that the shared memory segment is owned by another product or system.

User response
Change shared memory segment ID and restart the agent:

```
ADS_SHR_MEM_ID
```

AUIZ007S **The master address space failed to respond to a connect request.**

Explanation:
A secondary address space failed to connect to the master address space.

User response:
Check the **listener-port** in the **address-space-manager-config** section of the configuration and verify that it matches in both AUICONFG and members of the primary address space and secondary address spaces.

AUIZ008W **agent failed to shut down properly last time.**

Explanation:
When the agent is restarting, the persistent memory object indicates that the agent was abnormally cancelled or terminated without going through the proper clean-up routines, for example, Estae processing. This message might also indicate that another instance of the agent is currently executing.

User response:
Verify that there is only one instance of this agent running.

AUIZ009S **Attempts to attach to shared memory segment *segment key* failed.**

Explanation
This error message always occurs in conjunction with error message AUIX013E.

This startup error indicates that attempts to create a shared memory segment failed because of an already existing shared memory segment that never belonged to, or currently does not belong to, the primary agent address space.

This message can occur in the secondary address space if the <id> elements in the <address-space-manager-config> parameters of the AUICONFG config member that is used by the agent primary address space and the secondary address spaces(s) do not match.

User response:
Edit SAUISAMP member AUICONFG (or the customized AUICONFG) and specify a different <id> element in the <address-space-manager-config> section.

AUIZ010W **Configuration value for *<parameter>* is set below the allowed minimum of *<limit>*.**

Explanation:
Configuration parameter is not valid: *<parameter>* should be not less than *<limit>*.

User response:
Change the parameter to comply with the requirements.

AUIZ011W **Configuration value for *<parameter>* is set above the allowed maximum of *<limit>*.**

Explanation:
Configuration parameter is not valid: **<parameter>** should exceed the *<limit>*.

User response:
Change the parameter to correspond to the requirements.

AUIZ012I **Log-server: listening on port *<port>*.**

Explanation:
Identifies the port number that the Log-server is listening to.

User response:
No action is required.

AUIZ013E **Log-server: no available port was found in the range *<min-port>-<max-port>*.**

Explanation:
No available port was found in specified range. This usually implies that the range of ports is used by other installations or products.

User response:
Contact IBM Software Support.

AUIZ014W **Log-server: invalid data received from client *<client-ip>* (*<header-data>*).**

Explanation:
This message indicates that an unexpected connection occurred from *<client-ip>* to log-server port.

System action:
The connection is refused, and processing continues.

User response
This warning message can be produced during a system-level port security scan. If you do not want to receive this message, suppress it by using the configuration parameters **LOG_FILTER(E)** and **LOG_FILTER_MSGS_ID(AUIZ014W)**.

If a port scan was not active when this message was received, it indicates that an unknown message was received by the log-server port. Contact IBM Software Support.

AUIZ020W **Configuration parameter *parameter-name* was ignored: duplicate value specified *specified-value*.**

Explanation:
The specified configuration parameter *parameter-name* cannot contain a value that has already been specified for a related parameter.

User response:
Fix the duplicate value *specified-value* and restart the agent.

AUIZ021E **Configuration parameter *option* can't be empty.**

Explanation:
The configuration parameter *option* contains an invalid value.

User response:
Check the valid values for the *option* and correct the configuration file.

AUIZ022E **At least one active appliance is required.**

Explanation:
No appliances were specified in the agent configuration, or all specified appliances were disabled.

User response:
Check agent configuration and add enabled appliances to configuration.

AUIZ023E **Duplicate appliance specified: *host/port*.**

Explanation:
Specified appliance (*host/port*) are duplicates of another appliance specified in the configuration.

User response:
Update or remove duplicate appliances in the agent configuration.

AUIZ024E **Duplicate appliance priority specified: *priority*.**

Explanation:
Two or more appliances with duplicate priority (*priority*) were specified.

User response:
Update or remove appliances with duplicate priorities in the agent configuration.

AUIZ025E **Spill size can't be zero if more than one appliance is enabled.**

Explanation:
Spill size should be greater than zero if two or more active appliances are specified.

User response:
Specify a valid spill size.

AUIZ026E **Configuration parameter *<option>* value *<value>* is invalid; expected list *<value-list>*.**

Explanation:
The configuration parameter *<option>* contains an invalid value.

User response:
Check the valid values for the *<option>* and correct the configuration file.

AUIZ027W **Host name can't be resolved *<host-name>*.**

Explanation:
An attempt was made to determine the IP address of the host name that was indicated through the use of the z/OS *getaddrinfo* service. The attempt failed.

System action:
If the host name is not the local LPAR, processing continues. The TCP/IP address for any events that occur on this LPAR will not be sent to the appliance for reporting. If the host name is the local LPAR where the agent (AUIAstc task) is running, the local host name and IP address will be used for INTER and INTRA task communications.

User response:
The z/OS network administrator must verify that the LPAR name exists in the DNS table.

AUIZ028E **Configuration parameter *element-name* value *element-value* is invalid: expected min *value-min* and max *value-max*.**

Explanation:
The *element-value* given for *element-name* is out of the range and must be within *min-value* and *max-value*.

User response:
Correct the value for the *element-name* in the configuration.

AUIZ029E **Property *property-name* not found in config.**

Explanation:
A required property *property-name* could not be loaded from the configuration file because it has been incorrectly specified, specified multiple times, or not specified at all.

User response:
Update configuration file and add *property-name* with an appropriate value.

AUIZ030E **Configuration parameter *parameter-name* value *parameter-value* is not valid long value.**

Explanation:
The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *long*.

User response:
Correct the configuration value.

AUIZ031E **Configuration parameter *parameter-name* value *parameter-value* is not valid unsigned long value.**

Explanation:
The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *unsigned long*.

User response:
Correct the configuration value.

AUIZ032E **Configuration parameter *parameter-name* value *parameter-value* is not valid short value.**

Explanation:
The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *short*.

User response:
Correct the configuration value.

AUIZ033E **Configuration parameter *parameter-name* value *parameter-value* is not valid unsigned short value.**

Explanation:
The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *unsigned short*.

User response:
Correct the configuration value.

AUIZ034E **Configuration parameter *parameter-name* value *parameter-value* is not valid boolean value.**

Explanation:
The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *boolean*.

User response:
Correct the configuration value.

AUIZ035E **Configuration parameter *parameter-name* value *parameter-value* is not valid double value.**

Explanation:
The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *double*.

User response:
Correct the configuration value.

AUIZ036E **Configuration parameter *element-name* value *element-value* length is invalid: expected min *length-min* and max *length-max* characters.**

Explanation:
The *element-value* given for *element-name* is too long and its length must be within *length-min* and *length-max*.

User response:
Correct the value for the *element-name* in the configuration file.

AUIZ037I **Collection profile *profile* uninstalled successfully.**

Explanation:
The specified collection profile uninstalled.

User response:
No action is required.

AUIZ038I **Collection profile *profile* installed successfully.**

Explanation:
The specified collection profile installed.

User response:
No action is required.

AUIZ039I **Guardium policy processing started.**

Explanation:
The agent has received a policy message from the appliance and has started to process it.

User response:
No action is required.

AUIZ040I **Guardium policy processing finished [active = *<number1>*, installed = *<number2>*, uninstalled = *<number3>*].**

Explanation:
The Guardium policy has been processed. The active, installed, and uninstalled values indicate the number of processed collection profiles.

User response:
No action is required.

AUIZ041E **Profile for IMS source *ims_name* was ignored: unknown IMS.**

Explanation:
The agent received an IMS policy from the which does not relate to this agent instance.

System action:
The policy is ignored by this agent.

User response:
No action is required.

AUIZ041W **Profile for IMS source *ims_name* was ignored: unknown IMS.**

Explanation:
The agent received an IMS policy from the which does not relate to this agent instance.

System action:
The policy is ignored by this agent.

User response:
No action is required.

AUIZ042W **IMS artifact *ims-name* was ignored: invalid IMS definition.**

Explanation:
During policy pushdown, an *ims-name* was specified for one of the rules that does not exist in the Guardium appliance.

User response:
Contact IBM Software Support.

AUIZ043E **XCF callable service invocation failed: function *function-name*, RC = *nn*, reason code = *hhhhhhhh*, AUIU proc name = *proc-name*, ADS_SHR_MEM ID = *nn*.**

Explanation:
An error occurred attempting to retrieve AUIU tokens from the CF.

User response:
If the LPAR is not a sysplex member, no action is necessary. If the LPAR is a sysplex member, please contact IBM Software Support.

AUIZ044S **Shared memory segment version *S-TAP version found* is not compatible with expected *expected version*.**

Explanation:
An attempt to attach to a shared memory segment failed because of version mismatch. This might indicate that the shared memory segment that is identified by ADS_SHR_MEM_ID is already in use by an older version of the product, or another product.

User response:

Verify and change the ADS_SHR_MEM_ID that is specified in the agent configuration.

AUIZ045E **AUICONFG DD must be allocated.**

Explanation:
The address space requires an AUICONFG DD to be specified in the JCL.

User response:
Update the JCL for the address space to include an AUICONFG DD.

AUIZ046E ***module-name* callable service invocation failed: RC = *return-code*, reason code = *reason-code*.**

Explanation:
Invocation of the specified module failed due to the specified *return-code* and *reason-code*.

User response:
Contact IBM Software Support.

AUIZ047E **Specified spill file *data_set_name* does not exist.**

Explanation:
During agent startup, the SMF spill file that is named in the configuration parameter SMF_SPILL_FILE(dsn) was not found.

System action:
The agent terminates.

User response:
Determine why the file cannot be located. Correct any errors, and restart the agent.

AUIZ048E **Problem encountered for *<spill>*, *<problem area>*: required *<req>*, received *<res>*.**

Explanation

This spill data set *<spill>* could not be validated. The *<problem area>* with the parameters *<req>* and *<res>* gives additional details.

User response

Fix the issue in the *<problem area>* using the required *<req>* value. If necessary, contact IBM Software Support for additional help.

AUIZ049E **z/OS call failure for *<spill>*, *<problemarea>*: RC= *<rc>*, RSN= *<rsn>*.**

Explanation:
An attempt to validate the spill data set has caused an error with the z/OS services. A *<problemarea>* value with return code *<rc>* and reason code *<rsn>* are returned. If the *<problemarea>* value is *OBTAIN*, and the *<rc>* value is 4, the spill database in question might have been migrated. In that case, the spill database should be recalled before processing continues.

User response:
If a migrated data set is not the problem, contact IBM Software Support.

AUIZ050E **Specified Log Stream 'xxx.xxx.xxx' does not exist**

Explanation:
The z/OS log stream name that was specified in the **LOG_STREAM_DLIO** or **LOG_STREAM_DLIB** AUICONFG DD input stream does not exist.

System action:
The agent address space terminates.

User response:
Correct the log stream name that you provided, or customize and run the AUILSTRx Log Stream definition jobs that are located in the SAUISAMP product data set.

AUIZ051E **Problem encountered while validating *log-stream-name*. Function: *request: CONNECT*, RC = *xx*, RSN = *zzzz*.**

Explanation:
There was a failed attempt to validate the z/OS System Logger Log-Stream, through the use of an IXGCONN call.

System action:
Processing terminates.

User response:
Determine the cause of the failure by examining the return and reason codes for the IXGCONN macro. These can be found in the manual, *IBM MVS Programming: Authorized Assembler Services References*.

AUIZ052E **Abend occurred while validating *<log stream>*. Abend code = *<code>*, RSN=*<reason>*.**

Explanation

The Log Stream *<log stream>* validation failed with abend code *<code>* and reason code *<reason>*.

User response

Contact IBM Software Support.

AUIZ053E **Logging subsystem failed to initialize successfully.**

Explanation:

This error can occur for several reasons. It is preceded by the specific occurrence that caused the logging subsystem to fail during initialization.

User response:
Review previously issued error messages to determine the cause of the logging failure.

AUIZ054E **The Batch DLI log Stream and Online DLI log stream names must be different.**

Explanation:
The log stream name specified for LOG_STREAM_DLIO and LOG_STREAM_DLIB must be different.

User response:
Specify different log streams for batch and online in the agent configuration.

AUIZ055E **Shared memory segment ID *<shm-id>* is not available for use.**

Explanation:
The shared memory segment ID *<shm-id>* that is specified in the configuration file is not available, or is used by another task.

User response:
Check the available *<shm-id>* and update the confugration files. Contact IBM Software Support if *<shm-id>* is set correctly.

AUIZ056E **Shared memory segment ID *segment_id* is owned by agent *agent_name* and cannot be attached.**

Explanation:
The shared memory segment that was identified by the <id> parameter within the address-space-manager-config section of the agent configuration file is already used by the specified agent, *agent_name*.

System action:
The agent terminates because it is unable to use the shared memory segment.

User response:
To avoid a collision with other agents running on the LPAR, change or include the <id> value in the address-space-manager_config section of the agent configuration file.

AUIZ057E **A configuration syntax error was detected at line *<number>*; expected "*<token1>*", found "*<token2>*".**

Explanation:
An invalid value was found in the AUICONFG file and the indicated line.

System action:
Processing terminates.

User response:
Review Chapter 5, “Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent,” on page 19 for information about permissible configuration values. Correct the syntax error and restart the agent.

AUIZ058I **Collection profile *<profile-name>* updated successfully.**

Explanation:
The active collection profile *<profile-name>* has been updated during policy installation.

User response:
No action is required.

AUIZ059E **Configuration parameter *<option>* value *<value>* is invalid: the first character must be alphabetic.**

Explanation:
The configuration parameter *<option>* contains an invalid value.

User response:
Review the valid values for the *<option>* and correct the configuration file.

AUIZ060E **The master address space did not respond within 60 seconds.**

Explanation:
The IBM Guardium S-TAP for IMS agent did not send the policy report to the Memory Management Utility (AUIU*STC*) task within 60 seconds of establishing the connection.

System action:
The AUIU*STC* task terminates with RC=12.

User response:
Contact IBM Software Support.

AUIZ061I **AUIHOST file has been detected.**

Explanation:
The AUIHOST DD statement has been detected in the JCL.

System action:
The IP address for participating LPARs are resolved by the information contained in this file and described by message AUIxxxI.

User response:
If this was not intended, remove the DD statement.

AUIZ062I **AUIHOST file LPAR name/DNS name overrides in use: `CVTS_LPAR_NAME(DNS_NAME)`**

Explanation:
The AUIHOST DD has provided an override for the host named.

System action:

The **DNS_NAME** is the value that is used to perform the gethostbyname call in order to obtain the relevant IP address.

User response:
Verify that the supplied **LPAR_NAME** and **DNS_NAME** values are correct.

AUIZ063E **AUIHOST file format is invalid. RECFM must be FB; LRECL must be 80.**

Explanation:
The file format that was provided by using the AUIHOST DD is incorrect.

System action:
The address space terminates.

User response:
Verify that the supplied file is a Fixed Block (FB) sequential file, has a logical record length (LRECL) of 80 bytes, and is a either a sequential file or a member of a Partitioned Data Set (PDS or PDS/E). Correct the error and restart the address space.

AUIZ064E **AUIHOST file contains invalid syntax <*line number and string*>**

Explanation:
The AUIHOST file supplied contains a record with invalid syntax.

System action:
The address space terminates.

User response:
Review the "Overriding the TCP/IP DNS resolver table" on page 46 topic to verify the required syntax. Correct the record and restart the address space.

AUIZ065W **IMS STAP <*name*> TCP/IP streaming disabled due to user settings.**

Explanation:
Simulation mode is on because the **STAP_STREAM_EVENTS** parameter has been set to N.

System action:
Events will not be streamed to the Guardium system.

User response:
To stream events to the Guardium system, set the **STAP_STREAM_EVENTS** parameter to Y.

AUIZ066E **Configuration parameter "DLIFREQ" value *value* is invalid: expected 10K-999K, 1M-10M.**

Explanation:
In the AUICONFG file, the DLIFREQ parameter value is outside of the permitted range. Valid values for the DLIFREQ parameter are 10K -- 999K, or 1M -- 10M.

System action:
The AUIA*xxx* task terminates.

User response:
Correct the DLIFREQ parameter value.

AUIZ067W **Configuration parameter <*parameter*> value <*wrong value*> is not valid. <*Value*> will be used instead.**

Explanation:
Configuration parameter is not valid: <*parameter*> should match <*value*>.

User response:
Change the parameter to correspond to the requirements.

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

A

About this information vii
accessibility
  overview 4
address spaces
  starting 57
  stopping 57
agent
  auditing IMS data set access 41
  changing the name of the SMF address space JCL 41
  changing the retention period of incomplete SMF event 41
  changing the types of events audited using SMF records 41
  configuration keywords
    controlling the frequency of SMF z/OS catalog queries 41
    required configuration keywords 41
  configuring 19, 33
  customizing 19
  disabling SMF auditing at the agent level 41
  overview 2
  security 34
  starting the agent 34
  stopping the agent 34
APF authorization
  for libraries 7
APP_EVENT
  examples 38
auditing
  configuration keywords 41
  disabling IMS SLDS 48
  events 44
  IMS data set access 44
  setting up environment 35
AUIA060W
  additional causes 79
AUIEMAC1 edit macro
  variables 13

C

changes and enhancements to this version 1
common load modules
  copying 37
Common Memory Management address space JCL name
  changing 49
Common Storage Management Utility 2
components
  Guardium system 2
configuration keywords
  specifying multiple SMF data set masks 43
cookie policy 129
CVTSNAME
  LPAR name 46

D

data collection 59
data collection monitors 67
DBRC RECON data sets
  security 8
DD DUMMY statement
  excluding auditing 59
DLI calls
  capturing 35
DLIFREQ
  modifying AUIJ012I frequency 34
documentation
  accessing 3
  sending feedback 3

E

edit macro AUIEMAC1 13

F

filtering stages
  stage 0 filtering 61

G

Guardium 2
Guardium system
  configuring multiple Guardium systems 51
  multistreaming 51

I

IMS archived log data sets 60
IMS cataloged procedures
  customizing 35
IMS DLI calls 59
IMS Policy pushdown 70
installation
  hardware and software requirements 5
  sample library members 55

L

legal notices
  cookie policy 129
  notices 129
  programming interface information 129
  trademarks 129
links
  non-IBM Web sites 130
LOAD library
  APF authorizing 7
LPAR name
  CVTSNAME 46

M

mapping policies to a collection profile 62
messages and codes 81
Messages and codes 81

N

notices 129

O

Operator commands 9
overview 1

P

policy pushdown 62
programming interface information 129

Q

quarantine 9

R

reader comment form 3
RECON data sets
    SLDS processing 45
    SMF processing 45

S

sample library members 55
screen readers and magnifiers 4
security
    DBRC RECON data sets 8
    OMVS segment 7
service information 3
SMF dump data sets 59
stage 1 filtering 61
stage 2 filtering 61
support information 3

T

TCP/IP connections 7
technotes 3
trademarks 129

U

upgrading
    from V9.0
        creating E/CSA checkpoint blocks 11
    from V9.1 or V10.0 12

X

XML statements
    sample policy 78

Z

zIIP
    auditing functions 37
    using 37

Product Number: 5655-ST9

SC27-8022