IBM InfoSphere Guardium S-TAP for IMS on z/OS
Version 8 Release 2

User's Guide

SC19-3344-00

IBM InfoSphere Guardium S-TAP for IMS on z/OS
Version 8 Release 2

User's Guide

SC19-3344-00

Note:
Before using this information and the product it supports, read the information in “Notices” on page 123.

This edition applies to Version 8 Release 2 of IBM InfoSphere Guardium S-TAP for IMS on z/OS (product number 5655-STM) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Tables

About this information

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

- Steps for installing and configuring IBM InfoSphere Guardium S-TAP
- System requirements and prerequisites
- Processes for the effective use of IBM InfoSphere Guardium S-TAP

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

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

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

Always check the IMS Tools Product publications Web page for the most current version of this publication:

www.ibm.com/software/data/db2imstools/imstools-library.html

Who should read this book

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

Service updates and support information

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

http://www.ibm.com/support/entry/portal/Overview/Software/Information_Management/IMS_Tools

Highlighting conventions

This information uses the following highlighting conventions:

- **Boldface** type indicates commands or user interface controls such as names of fields, folders, icons, or menu choices.
- `Monospace` type indicates examples of text that you enter exactly as shown.
- *Italic* type indicates variables that you should replace with a value, to indicate the titles of other publication, and to emphasize significant terms.

How to read syntax diagrams

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

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

```
►►──required_item─────────────────────────────────────────────────────►◄
```

- Optional items appear below the main path.

```
►►──required_item──┬───────────────┬──────────────────────────────────►◄
                   └─optional_item─┘
```

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

```
                   ┌─optional_item─┐
►►──required_item──┴───────────────┴──────────────────────────────────►◄
```

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

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

```
►►──required_item──┬─required_choice1─┬───────────────────────────────►◄
                   └─required_choice2─┘
```

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

```
►►──required_item──┬──────────────────┬───────────────────────────────►◄
                   ├─optional_choice1─┤
                   └─optional_choice2─┘
```

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

```
                   ┌─default_choice──┐
►►──required_item──┼─────────────────┼────────────────────────────────►◄
                   ├─optional_choice─┤
                   └─optional_choice─┘
```

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

```
                   ┌──────────────────┐
                   ▼                  │
►►──required_item────repeatable_item──┴───────────────────────────────►◄
```

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

```
                   ┌─,────────────────┐
                   ▼                  │
►►──required_item────repeatable_item──┴───────────────────────────────►◄
```

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

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

How to look up message explanations

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

Searching an information center

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

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

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

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

Using a Web search

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

Using LookAt

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

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

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

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

How to send your comments

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

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

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

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

IBM InfoSphere Guardium S-TAP for IMS on z/OS (also referred to as InfoSphere Guardium S-TAP) is a 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 for auditors.

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

- Data collection— InfoSphere Guardium S-TAP can collect and correlate many different types of information:
  - Accesses to databases and segment from IMS Online regions.
  - Access to databases and segments from IMS DLI/DBB batch jobs.
  - Access to database, image copy and RECON data sets and security violations as recorded by SMF.
  - IMS Online region START and STOP, database and PSB change of state activity and USER sign-on and sign-off as recorded in the IMS Archived Log data sets.
- Administration user interface—Provides auditors with flexible options for user management and auditing profiles.

InfoSphere Guardium S-TAP components

InfoSphere Guardium S-TAP consists of 6 main components: the administration user interface, a server, an agent, a Common Storage Management Utility, a VSAM repository, and the Guardium Appliance.

Administration user interface

The Administration user interface is a graphical user interface (GUI) that enables product administrators to perform administrative tasks.

Data collection profiles, product user and group profiles, IMS system definitions, and other configuration parameters, can be maintained through the Administration user interface.

The Administration user interface can run on any hardware capable of executing Windows XP, Windows Vista, or Windows 7.

Server

The InfoSphere Guardium S-TAP server provides communications between the Administration user interface and other components of the product.

The server stores the information received from the Administration user interface in a VSAM file on the z/OS host for use by the other components of the product.

An example of the JCL to be used may be found in member AUISssid of the SAUISAMP installation data set.

Agent

The IBM InfoSphere Guardium S-TAP for IMS agent is responsible for coordinating the collection of audited data.

An IBM InfoSphere Guardium S-TAP for IMS agent collects data from a single IMS system, multiple IMS systems that share a common set of RECON data sets, or multiple IMS systems using diverse RECON data sets. The agent maintains the necessary communications links to exchange information with the server, IMS Online and Batch data collectors and activity monitors, as well as the IMS Archive Log data set and SMF activity monitors. The agent also provides data collection schemas to the activity monitors on which detail the IMS artifacts are to be audited, and to what level.

The agent executes as a started task on the z/OS host. An example of the JCL to be used may be found in member AUIAssid of the SAUISAMP installation data set.

- 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 necessary data to produce an audited event. These interfaces to the IMS modules are activated when an INIT call is made to the IMS Logger Exit routine (DFSFLGX0) supplied with the product and remain active until the DFSFLGX0 routine receives a TERM notification.

    Note: 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 the use of E/CSA control blocks. Determination of which DL/I calls and data bases/segments is made at the time the DL/I call is performed, using information derived from the data collection profile created using the Administration user interface.
  - The z/OS System Logger is used to transport the audit data from the IMS Online Activity Monitor to the agent. All IMS online systems 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 be sensitive to the DL/I call type and necessary data to produce an audited event. This interface to the DL/I call analyzer is activated when the IMS Batch Exit routine (DFSISVI0) supplied with the product is invoked, and remains active until the batch step terminates.
  - The IMS Batch Activity Monitor and the agent use of E/CSA control blocks to communicate data collection criteria. Determination of which DLI calls and data bases/segments is made at the time the DL/I call is performed, using information derived from the data collection profile created using the Administration user interface. The audit data from the IMS Batch Data Collector to the agent is transported through the z/OS System Logger.

  - All IMS batch jobs 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 Data Collector
  - The IMS Online and Batch Data Collectors execute under the control of the agent. Both data collectors execute within the same started task address space under separate execution threads. The function of the data collector is to read audited events from the z/OS System Log-Stream and send the events to the Guardium Appliance for storage using a TCP/IP connection.
  - Each execution thread maintains its own persistent TCP/IP connection to the Guardium Appliance. A sample of the JCL used for this started task may be found in the SAUISAMP data set in the AUIBssid member.
- SMF Data Collector
  - The SMF Data Collector reads a subset of SMF records from SMF DUMP data sets to determine if any data sets associated with audited IMS artifacts were read, written, deleted or renamed. Security violations against these data sets may 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 profile created by using the Administration User Interface.
  - As the processing of the SMF data sets is deferred, the data collection profile in force at the time of the SMF data set read will be the collection profile used, not the data collection profile in effect when the SMF event occurred. The names of the SMF DUMP data sets to be read is based on one or more SMF data set MASK values supplied during agent configuration through the Administration user interface. The data set names to which the SMF MASK refer may reflect the SMF DUMP data sets which are created when offloading the SMF recording data sets or a copy of these data sets containing a sub-set of SMF record types, created explicitly for the use of this product.
  - As 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 executes. The SMF Data Collector periodically queries the z/OS catalogue for any new data set names which meet the SMF MASK value. When catalogued data sets are found, these data sets are dynamically allocated and read by the SMF Data Collector. Any auditable events found are formatted and sent to the Guardium Appliance using a TCP/IP connection.
  - The SMF data Collector creates and maintains its own TCP/IP connection to the Guardium Appliance. The frequency that the SMF Data Collector queries the z/OS catalogue is determined by a user supplied option set during product configuration/customization. The SMF Data Collector may be configured to only audit a sub-set of events by use of available options when configuring the agent and defining the IMS system through the Administration user interface. The SMF Data Collector is executed as a started task under the control of the agent. An example of the JCL for this started task may be found in the SAUISAMP data set in the AUIFssid member.

Note: IBM InfoSphere Guardium S-TAP for IMS on z/OS only reports audited events for SMF record types that are collected by SMF. If specific SMF record types are not collected by your system or SMF recording data set dump utility, the event cannot be reported. Please refer to SMF record types topic within the Reference Information section for a list of SMF record types used by IBM InfoSphere Guardium S-Tap for IMS on z/OS.

- IMS Archived Log Data Collector
  - The IMS Archived Log Data Collector reads IMS Archived Log data sets (SLDS) and provides audit information concerning the following:
    - IMS User Sign-on and Sign-off
    - 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 profile created by using the Administration user interface.
  - As the processing of the IMS Archived Log sets is deferred, the data collection profile in force at the time of the IMS Archived Log data set read will be the collection profile used, not the data collection profile in effect when the IMS Archived Log event occurred.
  - The IMS Archived Log Collector periodically queries the DBRC RECON data sets associated with an IMS defined to IBM InfoSphere Guardium S-Tap for IMS on z/OS in order to determine if any new SLDS data sets have been created since the last RECON data set query. Any new data sets found are dynamically allocated and read, with audited events being sent to the Guardium Appliance using a TCP/IP connection.
  - The IMS Archive Log Data Collector may be configured to only audit a sub-set of events by use of available options when configuring the agent and defining the IMS system through the Administration user interface. The IMS Archived Log Data Collector is executed as a start-task under the control of the agent. An example of the JCL for this started task may be found in the SAUISAMP data set in the AUILssid member.
  - IBM InfoSphere Guardium S-TAP for IMS on z/OS starts one AUILssid task for each set of RECON data sets being actively monitored with a data collection profile.
    - If an IMS data sharing environment with five IMS sub-systems sharing a single set of RECON data sets exists, only one AUILssid task will be started.
    - If two separate IMS sub-systems using two separate sets of RECON data sets are being monitored, two separate AUILssid tasks will be started.

    Note: To collect events from the IMS archived logs, the DFSSLOGP data set (Primary Output SLDS) data set must be created and cataloged by your IMS Log Archive Utility process (Program DFSUARC0).
  - Any IMS SLDS or RLDS data sets found in the RECON data sets, which are not found in the z/OS catalog, are flagged as missing-logs. The names of these data sets are sent to the appliance as missing-log events.
  - IBM InfoSphere Guardium S-TAP for IMS on z/OS dynamically starts and stop the appropriate number of AUILssid tasks as required.
- Common Storage Management Utility
  - IBM InfoSphere Guardium S-TAP for IMS on z/OS uses memory in E/CSA to provide information regarding active data collection profiles to the IMS Batch and Online Activity Monitors, as well as the IMS Archived Log Data Collector.
  - As an IBM InfoSphere Guardium for IMS on z/OS agent may be called upon 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 profiles from the VSAM repository

and build the appropriate E/CSA control blocks. This stated task is driven when the IBM InfoSphere Guardium for IMS on z/OS agent starts and stops, as well as when a change is made to that state of any collection profile. An example of the JCL for this started task may be found in the SAUISAMP data set in the AUIUssid member.

- VSAM Repository
  - IBM InfoSphere Guardium S-TAP for IMS on z/OS requires the use of a repository to hold agent configuration data, as well as information regarding the IMS sub-systems the agent should monitor. Since the agent may be required to monitor IMS systems on various LPARS within a SYSPLEX, the VSAM repository must be accessible from all LAPRS within the SYSPLEX.

    Note: Neither VSAM RLS (Record Locking) nor Transactional VSAM is required for the use of this repository, nor is either supported.

Uses for IBM InfoSphere Guardium S-TAP for IMS on z/OS

IBM InfoSphere Guardium S-TAP for IMS on z/OS provides a comprehensive view of business activity occurring within one or more IMS environments.

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

Prerequisites

The following sections describe hardware and software prerequisites for IBM InfoSphere Guardium S-TAP for IMS on z/OS V8.2.

Hardware requirements

This topic describes the hardware required to operate IBM InfoSphere Guardium S-TAP for IMS on z/OS V8.2.

Administration user interface clients

All of the following are required:

- Any hardware capable or running Java 1.5 or higher.
- Any hardware capable of running Windows XP, Windows Vista or Windows 7.

Server and agent

Any hardware capable of running z/OS 1.8 or higher.

Software requirements

This topic describes the software required for IBM InfoSphere Guardium S-TAP for IMS on z/OS V8.2.

Client

One of the following Windows operating systems.

- Windows XP professional (32bit)
- Windows Vista
- Windows 7

Note: Windows Vista and Windows 7 are supported without Aero enabled. If Aero graphics are enabled when the Administration user interface is run, Windows Vista and Windows 7 will disable the Aero graphics for the time the Administration user interface is executing.

Server and agent

- z/OS Version 1 Release 8 or higher.
- IMS V9, V10, V11 or V12.
- It is recommended that IMS databases be registered with DBRC.

User ID authorities required for installation

This topic describes z/OS USERID authorities needed to install the IBM InfoSphere Guardium S-TAP for IMS on z/OS V8.2 product.

The z/OS USERID of the installer of this product must have authority to:

- Define z/OS System Log-streams
- Update the IMS catalogued procedure data set members DLIBATCH and DBBBATCH to include product load libraries

JAWS for Windows

For JAWS for Windows screen reader to work with InfoSphere Guardium S-TAP, the latest Java Access Bridge software must be installed. Java™ Access Bridge for the Microsoft Windows Operating System Version 2.0.1 or greater is available for purchase online.

In addition to installing the latest Java Access Bridge, the following manual configuration steps must be performed if the installer does not correctly detect and configure the default JRE that comes installed with your InfoSphere Guardium S-TAP client.

To manually configure the Java Access Bridge:

1. Copy the files "jaccess-1_4.jar" and "access-bridge.jar" from the Java Access Bridge install directory to `%DB2TOOLS%\JRE150\jre\lib\ext`, if they do not already exist there.
2. Edit the file “%DB2TOOLS%\JRE150\jre\lib\accessibility.properties”, so that it appears as follows:

```
#
# @(#)src/propfiles/accessibility.properties, jawbridge, jawdev_wi32, 20060111 1.1.1.5
# ===========================================================================
# Licensed Materials - Property of IBM
# "Restricted Materials of IBM"
#
# IBM SDK, Java(tm) 2 Technology Edition, v5.0
# (C) Copyright IBM Corp. 1998, 2005. All Rights Reserved
#
# ===========================================================================
#
#
# Load the IBM jawbridge into the Java VM
#
#assistive_technologies=JawBridge
assistive_technologies=com.sun.java.accessibility.AccessBridge
```

For more information on enabling your JRE accessibility features and manually configuring Java™ Access Bridge for the Microsoft Windows Operating System Version 2.0.1, please refer to the Java™ Access Bridge for the Microsoft Windows Operating System Version 2.0.1 Setup Information.

Using IBM InfoSphere Guardium Help

The IBM InfoSphere Guardium S-TAP for IMS on z/OS Help system allows you to browse and search for information. This product uses IBM Eclipse help plug-in V3.1.2 to launch the help system and serve help pages.

Navigation information

To get help for a current window in IBM InfoSphere Guardium S-TAP for IMS on z/OS, click **Help** or press **F1** when you are in the Administration user interface.

Browse topics in the **Contents** frame on the left. Click topics to display them. Use the **Back** and **Forward** arrows in the contents pane to navigate within the history of viewed objects.

To synchronize the navigation frame with the currently displayed topic, click the **Show in Table of Contents** button (at the top of the contents pane). The **Show in Table of Contents** feature is helpful if you have followed several links to related topics in several files, and you want to see where the current topic fits into the navigation path.

To search the entire documentation set, type a query in the **Search** field. To narrow down the sections that are searched, click **Search scope** next to the search field. To return to the search results view, click the **Search Results** button at the bottom of the frame.

Chapter 2. Configuring InfoSphere Guardium S-TAP for IMS

This section describes the steps required to configure InfoSphere Guardium S-TAP for IMS.

Synopsis

- The Security section describes the resource authorizations required by the product.
- The pre-configuration tasks section describes planning steps and required information.
- The VSAM repository section describes the steps necessary for creating, the VSAM data set, as well as the related limitations, restrictions, and security considerations.
- The Log streams section describes the CFRM and log stream size requirements, how to define the log streams for batch and online jobs, as well as related security considerations, limitations, and restrictions.
- The section on Configuring the server provides the necessary information to customize the configuration file, customize the PROC, and start the server.
- The section on Configuring the agent provides the necessary information to customize the configuration file, customize the PROC, and start the agent.
- The section on Setting up the administration client enables you to create the administrator, and provides information on the related security considerations.
- The section on Setting up an IMS for auditing describes how to customize IMS catalogued procedure, configure IMS exits, as well as the related security considerations.
- The SAMPLIB member listing can be found in the Configuration Appendix section of this User's Guide.

Related concepts

"Collection profiles" on page 58
This section describes how collection profiles use DLI Calls, IMS Archive logs, and SMF data to determine the capture of audit events.

Security

InfoSphere Guardium S-TAP for IMS requires access to various IMS data sets and system components in order to perform its function. This section lists the security considerations and requirements for proper functioning of the product.

APF authorization

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

- Product data set SAUILOAD, which contains the IMS Online and Batch Activity Monitor executable code, must be APF authorized on all LPARS of the SYSPLEX.
- Product data set SAUIIMOD, which contains IMS specific executable load modules, must be APF authorized on all LPARS of the SYSPLEX where IMS batch jobs or IMS online regions to be monitored may execute.

- The IMS RESLIB (IMS.SDFSRESL) data set must be APF authorized on all LPARS of the SYSPLEX where IMS batch jobs or IMS online regions to be monitored may execute, as well as the LPARS where the AUI servers and agents will execute.

Refer to *z/OS V1R8.0 MVS System Commands* for more information on how to APF authorize libraries.

DBRC RECON data sets

InfoSphere Guardium S-TAP for IMS uses the IBM DBRC Application Programming Interface (API) in order to read data from the RECON data sets. These RECON data sets must be accessible from all the LPARS where the InfoSphere Guardium S-TAP agents and servers may execute.

For IMS V10, V11, and V12, the READ-ONLY attribute is used in the DBRC API call, allowing the InfoSphere Guardium S-TAP jobs and started tasks with a security access of READ, to process the RECON data sets correctly.

The DBRC API for IMS V9 does not allow the READ-ONLY attribute, therefore in this case, the InfoSphere Guardium S-TAP started tasks must be provided with a security access of CONTROL to the RECON data sets.

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

SMF and IMS archive log data sets

READ access to the SMF data sets and the IMS archived logs (SLDS data sets) is required for the user under whose authority the agent runs. If these data sets are protected by RACF or another security product, a profile must be defined granting 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 InfoSphere agent executes.

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

z/OS log streams

IMS batch jobs and online regions monitored by InfoSphere Guardium S-TAP for IMS write the audit data to z/OS log streams.

It is suggested that the z/OS log stream have a universal security access of UPDATE, because IMS online systems and DLI/DBB batch jobs will write to these log streams.

Related concepts

"z/OS Log stream customization" on page 54

Related reference

"Setting up z/OS log streams" on page 13
IBM InfoSphere 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 (AUIBssid task). Both XCF based and DASD based log streams are supported.

IMS DBDLIB and PSBLIB

InfoSphere Guardium S-TAP reads DBD and PSB data sets in order to determine segment and database PCB information.

Security of access of READ is required.

Pre-configuration tasks

The tasks in this section are required prior to configuring InfoSphere Guardium S-TAP.

Use the Planning list to determine necessary information before configuring. Then customize the edit macro and provide a valid job card, as described in the following sections.

Planning

Before configuring InfoSphere Guardium S-TAP for IMS, the administrator must determine the following:

- the user that will configure the product
- the user IDs that will be used to run the server and the agent started tasks
- there the server and the agent started tasks will run

Customizing the ISPF edit macro

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

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 CLIST to easily edit other the SAMPLIB members.

To set up the edit macro, copy AUIEMAC1 from the #HLQ.SAUISAMP to a CLIST library and then edit the macro by providing the appropriate values for each of the variables. After the edit macro has been properly modified, it may be used as a command to customize other SAMPLIB members in the following steps.

Note:

- Set up the edit macro and use it to edit the SAMPLIB members in the following steps unless otherwise specified.
- To run the macro, type the name of the edit macro in the command line in ISPF.

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

```
ISREDIT MACRO (NP)
ISPEXEC VGET (ZUSER)
ISREDIT CHANGE ALL '#AUIIMOD'   AUI.IBMTAPE.SAUIIMOD
ISREDIT CHANGE ALL '#AUILOAD'     AUI.IBMTAPE.SAUILOAD
ISREDIT CHANGE ALL '#AUISAMP'     AUI.IBMTAPE.SAUISAMP
ISREDIT CHANGE ALL '#AUIREPOS'    AUI.V0820.REPOS
```

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 InfoSphere Guardium S-TAP for IMS.
#AUIMOD	AUI.IBMTAPE. SAUIIMOD	Change the default value to point to the location of the SAUIIMOD data set for InfoSphere Guardium S-TAP for IMS.
#AUISAMP	AUI.IBMTAPE. AUISAMP	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/ customization EDITs.
#AUIREPOS	AUI.V0820.REPOS	Please specify the location of the VSAM repository to be used by the agent's primary and secondary address spaces. **Note:** The VSAM repository must be accessible from all LPARs in a given SYSPLEX.

Job cards for the sample JCL in the SAMPLIB

Some JCL members shipped 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 the VSAM repository

InfoSphere Guardium S-TAP uses a VSAM KSDS data set to store product configuration details and collection profile information across all LPARS of a SYSPLEX environment.

One VSAM repository must be used per SYSPLEX environment.

Creating the VSAM repository data set

The VSAM repository data set is created using the AUISJ001 member of the AUISAMP installation data set. This JCL will DELETE a previously defined VSAM KSDS data set, DEFINE the KSDS using the appropriate keywords and parameters, and initialize the data set with an initialization record.

Member AUISJ001 requires some customization before use:

- A JOB card must be supplied as required by your installation.
- A data set name must be coded where the “#AUIREPOS” variable is specified. Customization and use of the AUIEMAC1 edit macro will cause the data set name chosen for the #AUIREPOS variable during AUIEMAC1 customization to be used.

Execute the customized AUISJ001 JCL to create and initialize data set.

Size restrictions and security considerations

This section specifies the record lengths to use in order to make space calculations, as well as the relevant security considerations.

VSAM Limitations and restrictions

The VSAM repository file must be accessible by all LPARS in the SYSPLEX. A default size of five cylinders is supplied, but your installation may require more space.

Space calculations may be made using the following record lengths:

Restriction: Only one VSAM repository data set can be defined per SYSPLEX.

VSAM Repository space calculations

- 1300 bytes will be consumed by each user defined in the repository.
- 320 bytes will be consumed by each group defined in the repository.
- 2300 bytes will be consumed by each IMS defined in the repository.
- 1100 bytes will be consumed by each agent defined in the repository, plus an additional 490 bytes will be consumed for each SMF mask defined to the agent.

The number of bytes consumed by each collection profile defined in the repository may be calculated as follows:

- Each collection profile will consume 500 bytes.
- Each rule will consume 200 bytes.
- Each database/segment entry will consume 200 bytes.
- Each USERID or PSB will consume 200 bytes.

Note: The VSAM repository file must be updatable by all product started tasks that may execute on the SYSPLEX.

Setting up z/OS log streams

IBM InfoSphere 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 (AUIBssid task). Both XCF based and DASD based log streams are supported.

Each agent requires two unique log streams:

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

Log streams cannot be shared between agents, nor can they be shared between IMS Control regions and DLI/DBB batch jobs.

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 having performance benefits. For more information about the two types of log streams, refer to the IBM publication: *System Programmer's Guide to: z/OS System Logger*.

Log streams must be defined to your system before you attempt to define an agent using the administration user interface, because the agent definition process validates the existence of the log streams.

Related reference

"z/OS log streams" on page 10
IMS batch jobs and online regions monitored by InfoSphere Guardium S-TAP for IMS write the audit data to z/OS log streams.

Log stream security

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

Important:

- The USERID your IMS online control region executes under must have WRITE access to the log stream.
- If DLI/DBB batch jobs execute under a common USERID, that USERID must have WRITE permission to the log stream.
- The USERID under which the DLI Event Collector (AUIBssid task) executes must have READ/WRITE access to the log streams.
- If individual users are permitted to execute 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 may also be found within 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 may result in the loss of existing CFRM structure definitions. It is highly recommended that a systems programmer customize and execute this JCL.

Values which must be customized are:

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

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

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

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

Other values such as SIZE, INITSIZE and ALLOWAUTOALT should not be changed.

Note: AUILSTR1 must execute successfully before proceeding.

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 may also be found within the comments of the JCL.

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

Values which must be customized for IMS Batch processing include:

DEFINE STRUCTURE values:

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

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

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 by using the Administration user interface's Agent Editor.

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 by using the Administration user interface's Agent Editor.

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

The selection of the Staging data set classes
(STG_DATACLASS, STG_MGMT_CLASS and STG_STORCLASS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging dataset 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_DATACLASS, LS_MGMT_CLASS and LS_STORCLASS)

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

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

The HLQ and EHLQ are mutually exclusive and only one may be used. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.

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

DEFINE STRUCTURE values:

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

The LOGSUM, 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 by using the Administration user interface's Agent Editor.

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

The selection of the Staging data set classes
(STG_DATACLASS, STG_MGMT_CLASS and STG_STORCLASS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging dataset 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 may be removed if the STG_DATACLAS value is specified.

The selection of offload data set classes
(LS_DATACLASS, LS_MGMT_CLASS and LS_STORCLASS)

These parameters indicate the SMS classes to be used when the System logger allocates an offload dataset 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))

A value of 13500 (the number of 4K blocks) is the default/supplied value. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of this size.

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

The HLQ and EHLQ are mutually exclusive and only one may be used. 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.

DASD-based logs streams may only be accessed from one LPAR at a time, meaning that any IMS Online Control regions and DLI/DBB batch jobs to be audited, must execute on the same LPAR as the agent executes.

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 may be found within the comments of the JCL.

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

Values which must be customized for IMS Batch 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 by using the Administration user interface's Agent Editor.

The selection of the Staging data set classes
(STG_DATACLASS, STG_MGMT_CLASS and STG_STORCLASS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging dataset 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_DATACLASS, LS_MGMT_CLASS and LS_STORCLASS)

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

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

The HLQ and EHLQ are mutually exclusive and only one may be used. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.

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 by using the Administration user interface's Agent Editor.

The selection of the Staging data set classes
(STG_DATACLASS, STG_MGMT_CLASS and STG_STORCLASS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging dataset 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 ONLINE Log stream DASD data sets
(STG_SIZE)

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

The selection of offload data set classes
(LS_DATACLASS, LS_MGMT_CLASS and LS_STORCLASS)

These parameters indicate the SMS classes to be used when the System logger allocates an offload dataset 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 allocation/size of the offload data sets
(LS_SIZE(13500))

A value of 13500 (the number of 4K blocks) is the default/supplied value. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of this size.

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

The HLQ and EHLQ are mutually exclusive and only one may be used. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.

Configuring the server

This section provides the information required for configuring the server.

Server started task

The server started task reads the data set pointed to by the AUICFG DD in the provided SAUISAMP member AUISssid to load its configuration. The SAUISAMP member AUICFGS provides a sample configuration that can be used by the server started task. It is recommended that you make a copy of the AUICFGS and customize it for use by a given server. The AUICFGS data set is extensively documented and you can follow the instructions in this guide or in the AUICFGS data set to complete the next steps.

Note:

- This data set must contain properly formed XML. Extraneous characters such as sequence numbers will cause errors.
- The data set must be edited using the EBCDIC encoding (1047 CCSID).

Customizing the server configuration file

The configuration (SAMPLIB member AUICFGS) file provides the following options that may be customized.

Note:

- Options that do not have a default value must be specified before starting the server started task.
- The default values for all the configuration parameters may be used, except for the server-repository parameters.

client-listener-port
Must specify the IP port on which the server listens for connections from the InfoSphere Guardium S-TAP for IMS client.

Valid values are integers between 1025 and 65535. Please contact your system administrator to determine what TCP/IP port should be used.

By default, the port specified in the configuration file is 52522.

agent-listener-port

Must specify the IP port on which the server listens for connections from the InfoSphere Guardium S-TAP for IMS agent.

Valid values are integers between 1025 and 65535. Please contact your system administrator to determine what TCP/IP port should be used.

By default, the port specified in the configuration file is 52541.

log-level

Controls the amount of output log information generated by the server.

Valid values are:

- O – disable logging
- S – log severe error messages only
- E – log error and severe error messages
- W - log warning, error, and severe error messages
- I - log information, warning error, and severe error messages (recommended)

By default, the log-level specified in the configuration file is I.

bind-retry-max

Specifies the maximum number of attempts the server should make to bind to the specified client and agent listener ports, before exiting with an error.

There is typically no delay in binding. It is possible that one or both of the ports might be in use by another application. If a previous application was using one or both of the ports and failed, there may be a delay before the system releases the port(s) so that they can be used by the InfoSphere Guardium S-TAP for IMS server.

Valid values are integers greater than or equal to 0.

By default, the value specified in the configuration file is 30.

bind-retry-delay

Specifies the number of seconds the server should wait between attempts to bind to the client and agent listener ports.

The period of time (in seconds) that the server will continue attempts to bind is: `bind-retry-max * bind-retry-delay`.

Valid values are integers greater than 0.

By default, the value specified in the configuration file is 10.

repository-dsn

Specifies the VSAM repository to be used by the server.

The AUIEMAC1 edit macro can be used to change the repository to be used by the server, for example:

```
<repository-dsn>#AUIREPOS</repository-dsn>
```

This parameter must be uppercase.

This parameter is required.

trace-*

The trace-* parameters cause additional tracing information to be logged, in order to diagnose errors that may occur during product execution.

These parameters should not be enabled unless directed by product support, as there is a significant cost in performance when they are enabled.

Valid values for each are true or false.

community-string

Optional, and specifies an identifying string for the instance of the server. In order for agents to discover and connect to this server, those agents must be configured with the same community-string value.

There is no default value provided for this configuration element.

multicast-address

Optional, and specifies the UDP multicast address on which the server should make server announcements. In order for agents and clients to discover this server, they must be configured with the same multicast-address value.

Valid values are IP addresses in dotted-decimal notation, between 224.0.1.0 to 238.255.255.255, exclusive.

By default, the value specified in the configuration file is 236.1.2.8.

multicast-port

Optional, and specifies the UDP multicast port on which the server should make server announcements.

In order for agents and clients to discover this server, they must be configured with the same multicast-port value.

Valid values are integers between 1025 and 65535, inclusive. Please contact your system administrator to determine what multicast port can be used.

By default, the value specified in the configuration file is 52542.

multicast-interface

Optional, and specifies the local network interface address on which the server should make server announcements. If omitted, the server makes the announcements on all interfaces.

Valid values are IP addresses in dotted-decimal notation.

There is no default value provided for this configuration element.

multicast-ttl

Optional, and specifies the UDP multicast "time-to-live" value for the server announcements. This value specifies the maximum number of subnets over which the announcements will be routed. Consult your network configuration documentation for more information.

Valid values are integers greater than 0.

By default, the value specified in the configuration file is 5.

multicast-delay

Optional, and specifies the number of seconds the server should wait between making announcements of its presence on the network. Smaller values result in more network traffic, but better responsiveness to agents and clients attempting to discover this server.

Valid values are integers greater than 0.

Customizing the server PROC

The SAUISAMP member AUISssid provides a sample PROC that may be used for the server started task. The PROC can be customized as follows:

1. Edit SAUISAMP member AUISssid by running the ISPF edit macro. See the section on customizing the edit macro for more information.
2. Modify the CFG=AUI.V0820.SRVCFG(AUICFGS) to specify the location of the customized configuration data set for the server created in the previous section.
3. Rename the AUISssid member to any character name valid for started tasks in your environment. Please see the previous section for details on the server-repository element of the configuration file.
4. Copy the renamed member to the PROCLIB for the site. Please contact the system administrator to determine the location of the PROCLIB.

Starting the server

Use these commands to start and stop the server.

Note: APF Authorization must be completed before starting the server. Starting the server without completing APF Authorization results in a failure error.

The server can be started using the command /S SSID and stopped using the command /STOP SSID. The AUILOG DD contains the server log and can be inspected for any errors and or informational messages.

Server configuration security considerations

The User ID under which the server started task executes must have UPDATE authority to the VSAM repository.

Configuring the 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 (AUIAssid) and multiple secondary address spaces (AUIBssid – IMS batch/online collector, AUIFssid – smf collector, AUILssid – IMS log collector, AUIUssid – common storage utility) that are automatically started and stopped by the primary address space. All of the started tasks (for the primary agent address space and for the secondary address spaces) read the data set pointed to by the AUICFG DD in the provided SAUISAMP members AUIAssid, AUIBssid, AUIFssid, AUILssid and AUIUssid to load its configuration.

The SAUISAMP member AUICFGA provides a sample configuration that can be used by the agent's primary address space started task. This member may also be used by the secondary address spaces.

Follow the instructions on the AUICFGA data set in this User's Guide or in the data sets to complete the next steps.

Note:

- These data sets must contain properly formed XML and extraneous characters such as sequence numbers will cause errors.
- The data set must be edited using the EBCDIC encoding (1047 CCSID).
- It is recommended to make a copy of the AUICFGA and customize it for use by a given agent.

Customizing the agent configuration files

The configuration file provides the following options that may be customized by the user. The options that do not have a default value must be specified by the user before starting the agent started task.

Customizing the agent's primary address space configuration file

Note: The default values for all the configuration parameters may be used except for the server-address, server-repository and the server-repository-db parameters.

- Options that do not have a default value must be specified before starting the server started task.
- The default values for all the configuration parameters may be used except for the server-repository.

server-address

Must specify the host name or IP address (in dotted decimal notation, e.g., 1.2.3.4) of the InfoSphere Guardium S-TAP for IMS server to which the agent should connect.

There is no default value for this parameter.

server-port

Must specify the IP port number for the InfoSphere Guardium S-TAP for IMS server to which the agent should connect.

Valid values are integers between 1025 and 65535. Please contact your system administrator to determine what TCP/IP port should be used.

By default, the port specified in the configuration file is 52541.

log-level

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

Valid values are:

- O – disable logging
- S – log severe error messages only
- E – log error and severe error messages
- W - log warning, error, and severe error messages
- I - log information, warning error, and severe error messages (recommended)

By default, the log-level specified in the configuration file is **I**.

server-connect-retry-delay

Specifies the number of seconds the agent should wait between attempts to connect to the server.

The period of time (in seconds) that the agent will continue attempts to connect is: server-connect-retry-max * server-connect-retry-delay.

Valid values are integers greater than 0.

By default, the value specified in the configuration file is 10.

request-thread-timeout

Specifies the number of seconds a thread/task created to do work for a specific user should remain idle before exiting. Setting this value higher provides a better response to client requests, but consumes more resources (in the form of extra tasks that are not performing work).

This value should be set high enough so that a task does not exit during a typical end-user client session, i.e., greater than the expected time between end-user actions in the client.

Valid values are integers greater than 0.

By default, the value specified in the configuration file is 300.

job-poll-rate

Specifies the number of seconds the agent should wait before attempts to query the status of submitted jobs. Lower values provide better response time to end users, but require more resources on the server.

Valid values are integers greater than 0.

By default, the value specified in the configuration file is 5.

repository-dsn

Required parameter that specifies the data set name of the VSAM repository the agent should use.

The AUIEMAC1 edit macro can be used to change the repository to be used by the agent, for example:

```
<repository-dsn>#AUIREPOS</repository-dsn>
```

server-connect-retry-max

Specifies the maximum number of attempts the agent should make to connect to the server, before exiting with an error.

Typically, the server should be started and available before any agent is started, in which case the agent will immediately connect on the first attempt. This parameter allows for the case when the server is not immediately available.

Valid values are integers greater than or equal to 0.

By default, the value specified in the configuration file is 30.

smf-interval

Specifies the frequency (in minutes) at which the agent processes smf data.

It is recommended that this value be set corresponding to the frequency at which SMF output data sets are generated by the SMF log extraction process. For example, if the SMF data sets are generated every 4 hours, smf-interval should be set to 240 (4 hours).

By default, the value specified in the configuration file is 300 (minutes).

self-audit

Specified whether the IMS accesses via the address spaces of the product itself will be audited. By default, this is turned off.

Valid values are true and false.

By default, the value specified in the configuration file is *false*.

ims-log-interval

Specifies the frequency (in seconds) at which the agent process IMS data.

By default, the value specified in the configuration file is 300 seconds.

lpars-monitor-interval

Specifies the number of seconds between two subsequent retrievals of the list of online LPARs. This enables the LPARs that join the PLEX after the agent has started to be detected, and for common storage on such LPARs to be refreshed.

Valid values are between 1 and 300.

By default the value specified in the configuration file is 300 seconds.

multicast-address

Optional, and specifies the UDP multicast address on which the agent should listen for server announcements. In order for the agent to discover and connect to a server, that server must be configured with the same multicast-address value.

Server discovery is performed only if the server-address parameter is omitted.

Valid values are IP addresses in dotted-decimal notation, in the range from 224.0.1.0 to 238.255.255.255, inclusive.

By default, the value specified in the configuration is 236.1.2.8.

multicast-port

Optional, and specifies the UDP multicast port on which the agent should listen for server announcements. In order for the agent to discover and connect to a server, that server must be configured with the same multicast-address value.

Server discovery is performed only if the server-address parameter is omitted.

Valid values are integers between 49152 and 65535.

By default, the value specified in the configuration is 52542.

address-space-manager-config

Optional, however, it is highly recommended that the 'passphrase' element is modified for security.

The 'passphrase' element may be used to specify any string comprised of. If nothing is specified, a default value is used.

The 'listener-port' element may be modified if another application is already using the port.

The 'id' element may be modified to specify an integer between 100000 and 9999999.

If you are also using IMS Audit management Expert, this section should appear exactly the same in the configuration for all the agent related address spaces as in IMS Audit Management Expert v1.2.

If nothing is specified, the default values are used.

smf-proc / ims-batch-proc / ims-log-proc / cs-util-proc

These parameter elements should be used to specify the PROC names for the different agent address spaces. See section 2.9.1 and 2.9.2 for more details.

There is no default value provided for this configuration element.

loopback-address

Specifies the loopback hostname or IP address used for communication between the agent and sub-tasks. For most configurations, this value need not be changed. However, if localhost cannot be resolved on your system, please consult your network administrator for the correct loopback-address value.

trace-* Causes additional tracing information to be logged, in order to diagnose errors that may occur during product execution.

These parameters should not be enabled unless directed by product support, as there is a significant cost in performance when they are enabled.

Valid values for each are true or false.

By default, all of these elements in the configuration file have a value of false.

name-uid
The name-uid value is a user provided name used to reference the agent.

It may be 1 to 18 characters in length and must be a unique value within the repository.

This is a required parameter which has no default value.

appliance-server
The appliance-server parameter specifies the TCP/IP address of the Guardium appliance where all captured events are to be sent by the various data collectors.

This is a required parameter which has no default value.

appliance-port
The appliance-port parameter specifies the IP port number of the Guardium appliance to which the various data collectors should connect.

Valid values are between 0 and 99999 inclusive.

Default value: 16016.

appliance-ping-interval
The appliance-ping-interval indicates how often a PING should be sent to the Guardium appliance. This sends a regular signal to enable the Guardium appliance to recognize a connection is being maintained.

This value is express in seconds.

Default value: 5.

Customizing the agent's secondary address space configuration file

A sample for the agent's secondary address space configuration file is provided in the SAUISAMP member AUICFGA. For all the configuration elements, use this section as well as the AUICFGA member documentation.

Customizing the agent PROC

The SAUISAMP member AUIAssid provides a sample PROC that may be used for the agent started task. The PROC can be customized as follows:

1. Edit SAUISAMP members AUIAssid, AUIBssid, AUIFssid, AUILssid and AUIUssid by running the ISPF edit macro. See the Pre-configuration tasks Planning section of this guide for more details.

2. Modify the CFG=AUI.V0820.AGTCFG(AUICFGA) in AUIASSID to specify the location of the customized configuration data set for the agent created in the previous section.
3. Modify the CFG=AUI.V0820.AGTCFG(AUICFGA) in AUIBssid, AUIFssid, AUILssid and AUIUssid to specify the location of the customized configuration data set(s) for the secondary address spaces created in the previous section.
4. Rename the AUIASSID member to AUIA<SSID> where SSID is the value of the server-repository element in the configuration file. Please see the previous section for details on the server-repository element of the configuration file.
5. Rename the AUIBssid, AUIFssid, AUILssid and AUIUssid similarly, where the SSID is replaced with the SSID of the server repository being used. Please see the previous section for details on the server-repository element of the configuration file.
6. Copy the AUIA<SSID>, AUIB<SSID>, AUIF<SSID>, AUIL<SSID> and AUIU<SSID> members to the PROCLIB for the site. Please contact the system administrator to determine the location of the PROCLIB.

   Note: Each of these SSIDs should have APF authorization of the AUILOAD file before they are started.

Starting the agent

Use these commands to start and stop the server:

The agent can be started using the command /S AUIA<SSID> from the SDSF command line. The primary agent address space will then start up the AUIB<SSID>, AUIF<SSID> address spaces. One or more instances of AUIL<SSID> may also be started depending on the list of active collections.

The agent can be stopped by issuing the command /STOP AUIA<SSID> from the SDSF command line. The primary agent address space will then stop all the secondary address spaces that are online and then shut down. Depending on the load and the activity in the other secondary address spaces, the shut down process may take time. The user must monitor the AUILOG DD of the primary address space AUIA<SSID> for informational messages on the status of the secondary address spaces.

Agent security considerations

The User ID of the agent started tasks must have SYSADM authority for the audit data repository.

Additionally, the user ID of the agent started tasks (the primary and the secondary started tasks) should have the proper RACF profiles to read the control file contents (see the section on Setting up the control files) and to read and update the VSAM repository (see the section on Setting up the VSAM repository).

Important: Please contact your system administrator to ensure that **localhost** is being resolved to 127.0.0.1 (loopback address). The TCP/IP communication between the agent and the secondary address spaces relies on this resolution.

Setting up the administration client

Before the administration client can connect to the server, the user must create an administrator that can be used to login.

Either you must know the client-listener-port of the server that the administration client must connect to, or you must have the server configured for multicast so the client-listener-port can be discovered by the administration client.

Creating the administrator

Complete the following steps to create the administrator:

1. Edit SAUISAMP member AUISJUAP by running the ISPF edit macro. See the Pre-configuration tasks Planning section of this guide for more details.
2. Edit SAUISAMP member AUICFGU and specify a username and password for the administer account.
   a. Run the edit macro for this parameter to supply a valid value for your repository DSN name in this parameter: `<repository-dsn>#AUIREPOS</repository-dsn>`
3. Edit AUISJUAP and specify the configuration file by updating the AUICFG DD to point the SAUISAMP member AUICFGU.
4. Add the appropriate job card to AUISJUAP.
5. Submit AUISJUAP to create the administrator. The job steps must end with a return code of zero.

Administration client setup security considerations

Take these precautions to avoid potential security breaches:

After an administrator account has been created, the user must delete the password from the SAUISAMP member AUICFGU to avoid any potential security breaches. It is further recommended that the user setup RACF profiles to limit read access to the SAUISAMP member data sets and any other configuration files read by the server, agent and or any of the other product jobs.

Installing the administration client

Follow these steps to install the administration client. The client installation is a member of a data set from the z/OS installation.

Important: To install the administration client on your personal computer, you must have administration level access, which is granted by your PC user account being added to the Administrators group on the client host.

To install the administration client:

1. Locate the SAUIGUIW data set from the SMP/E installation.
2. Locate member AUIGUIW.
3. Use FTP to transfer member AUIGUIW (in binary) to your workstation, renaming the member with a local file name of AUIGUIW.zip.
4. Open AUIGUIW.zip. Unzip the installation files for the administration client to a folder.
5. Run the .exe file. (Follow the instructions in the install program if you want to change the location of the file.)

Installing administration client maintenance

This section describes the steps and authorization required to install maintenance for the administration client.

Installing client maintenance

Follow the steps in the topic *Installing the administration client*, substituting the member name AUIGUIWP with the member name AUIGUIW in all steps, 1-4.

Important: To correctly install maintenance for the administration client, you must have administration level access, which is granted by being added to the Administrators group on the client host.

Customizing IMS environments to capture DLI calls

For InfoSphere Guardium S-TAP for IMS to report on IMS database accesses, it needs to be sensitive to IMS DL/I calls. This section describes proper set up of the relationship between your IMS online and batch environments and InfoSphere Guardium S-TAP for IMS.

The InfoSphere Guardium for IMS programs used to communicate with your IMS environments are found in the SAUIIMOD data set created during product installation.

Customizing IMS catalogued procedures

For InfoSphere 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 InfoSphere Guardium S-TAP for IMS programs.

The InfoSphere Guardium S-TAP for IMS programs that must be accessed all reside in the SAUIIMOD installation data set. The preferred method of installing InfoSphere 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 InfoSphere 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.
- While InfoSphere Guardium S-TAP for IMS provides and uses the DFSFLGX0 and DFSISIV0 IMS exits to establish communication with IMS services, no customization of these exits is required.

Coexisting with other DFSGLFX0 and DFSISVI0 Exit routines

InfoSphere 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. InfoSphere 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.

InfoSphere Guardium S-TAP for IMS supports the protocols used by the IMS Tools Generic Exit product. You may define the InfoSphere Guardium S-TAP 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 pertinent 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 InfoSphere Guardium S-TAP for IMS Exit Cascading

For situations where the IBM IMS Tools Generic Exit is not available for use, InfoSphere Guardium S-TAP for IMS provides a method of supporting two instances of the DFSFLGX0 and DFSISVI0 exits. When loaded and executed, the InfoSphere Guardium S-TAP supplied program AUIFLGX0 (DFSFLGX0) and AUIISVI0 (DFSISIV0) determines from which DSN within the JOBLIB/STEPLIB concatenation it was loaded from. It then searches all other 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 InfoSphere 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-InfoSphere Guardium S-TAP 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 InfoSphere 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.

Security considerations for IMS processing

InfoSphere 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 InfoSphere Guardium S-TAP for IMS use.

SMF customization

For SMF customization, SMF events, SMF spill data sets, and SMF masks, as well as the IMS log and log stream must be customized. Detailed information on how to customize these areas is available in this User's Guide.

Related concepts

"SMF Customization process" on page 49
The SMF customization process requires three areas of customization, to SMF events, SMF spill data sets, and SMF masks.

Related reference

"IMS Logtypes and SMF record types collected by InfoSphere Guardium S-TAP" on page 71
The two tables in this section show the IMS logtypes collected by InfoSphere Guardium S-TAP.

Configuration appendix

This section provides additional material related InfoSphere Guardium S-TAP for IMS configuration.

Sample library members

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

Table 2. Sample library members

Member	Type	Description
AUIASSID	JCL	PROC to set up an agent address space (the primary address space).
AUIBSSID	JCL	PROC to set up the IMS batch collector address space (a secondary agent address space).
AUICFGA	XML	XML configuration file to be used by the agent address space (see SAMPLIB member AUIAssid).
AUICFGS	XML	XML configuration file to be used by the InfoSphere Guardium S-TAP server.
AUICFGU	XML	XML configuration file to be used by the UAP utility to create/update administrator account passwords.

Table 2. Sample library members (continued)

Member	Type	Description
AUICPMOD	JCL	JCL to copy utility program(s) from the SAUILOAD data set to the AUIMOD data set.
AUIFSSID	JCL	PROC to set up the SMF collector address space (a secondary agent address space).
AUIFUSPL	JCL	JCL to create the SMF incomplete event spill file for an agent.
AUILSSID	JCL	PROC to set up the IMS online log collector address space (a secondary agent address space).
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
AUISJ001	JCL	Creates VSAM file to contain common storage data.
AUISJUAP	JCL	Sample job to run the utility to create an administrative user for the product (can be used to login via the administration client).
AUISMFDF	JCL	Sample job to create GDG for the SMF Collection Routine.
AUISMFDP	JCL	Sample job to extract archived SMF data and create GDG data set for the SMF Collection Routine.
AUISSSID	JCL	PROC to set up the server started task.
AUIUSSID	JCL	PROC to set up the server address space.

Chapter 3. InfoSphere Guardium S-TAP administration

To enable InfoSphere Guardium S-TAP clients, servers, and agents to interact, you must configure them to communicate. Only one server instance is permitted on each SYSPLEX. This server instance is used to communicate with all agent instances executing within the SYSPLEX.

The InfoSphere Guardium S-TAP environment consists of the following:

- one agent
- one administration client

Server, client, and agent communications

The InfoSphere Guardium S-TAP for IMS server, client, and agent communicate with each other using TCP/IP connections.

Connections between server and agent can be established in two ways:

- Manual configuration
- Automatic discovery

Note: The InfoSphere Guardium S-TAP for IMS client must be manually configured.

Manual configuration

When using manual configuration, you use different methods to configure the client to server and agent to server connections.

Client-server configuration

This information describes client-server configuration.

You configure the server to run on a particular host machine. Additionally, you configure the server with a TCP/IP port number on which to listen for incoming connection requests from instances of the client. This value is specified by the *client-listener-port* element in the server configuration file (SAUISAMP member AUICFGS).

When you start the client, you must manually enter the host name or IP address on which the server is running, as well as the port number on which that server is configured to listen for client connections. Obtain these values from the person who configured the server.

Agent-server configuration

This information describes InfoSphere Guardium S-TAP for IMS agent to server configuration.

In addition to configuring the server for incoming client requests, you specify a different port on which to listen for incoming connection requests from instances of the agent. This value is specified with the *agent-listener-port* configuration element in the server configuration file.

Only one agent per SYSPLEX is required. When configuring an agent instance, specify the host name or IP address and the port number on which the server is running. These values are specified by the *server-address* and *server-port* configuration elements in the agent configuration file (SAUISAMP member AUICFGA). When the agent is started, it uses this configuration information to connect to the server.

Automatic discovery

The InfoSphere Guardium S-TAP for IMS server and agent can be configured to connect to each other automatically.

Automatic discovery reduces the manual configuration effort that is required and allows the agent to connect to a server even if the specific connection information is unknown.

Server notifications

The server sends notifications of the port numbers where it listens for incoming agent connections by using IP multicasting.

There are a wide variety of options related to the use of multicasting. You must consult your network administrator and configuration documentation to ensure that proper forwarding of multicast packets is enabled.

Agent-server connections

This information describes the configuration process to use server notifications for agent-server connections.

As described previously, you can specify the host name and port number of the server to which an agent connects. If you omit the server-address configuration option, the agent listens for server notifications on the network. When a notification for a server is received, the agent uses the information in the notification to connect to that server.

If you specify a value for the server-address configuration option, the agent attempts to connect to that address, and does not perform any automatic server discovery.

Automatic discovery allows the administrator to change which machine the server runs on without requiring changes in the agent configuration files.

Automatic discovery options

Additional server and agent configuration options are available to fine tune the automatic server discovery process, particularly in the case where a site is running more than one server.

Community string:

The function of the community string is similar to that of the description, in that it allows differentiation between multiple instances of the server.

Multicast options:

Several options that are related to multicasting are available in the server and agent configuration options.

Options

`multicast-address`

The *multicast-address* option specifies the global multicast address to which the server sends its notifications and on which the agent and client register interest. The default value is 236.1.2.8.

Note: Do not change the default value, unless there is a conflict with another application on your network. If such a conflict occurs, you can specify a different address, but you must ensure that you specify the same address in the server and agent configuration files and in the client options.

`multicast-port`

Similarly, the *multicast-port* option specifies the port to which the server sends its notifications. If a conflict occurs, you can specify a different port, ensuring that the same value is specified everywhere.

`multicast-interface`

The *multicast-interface* option is a server-only configuration option and specifies the local network interface address on which the server notifications are sent. If this parameter is omitted, the notifications are sent on all active interfaces.

`multicast-ttl`

The *multicast-ttl* option is also a server-only configuration option. It specifies how far away from the server machine the server's multicast notifications are propagated over the network. The default value is 5 subnets or routers.

Note: Do not specify a value greater than is necessary to reach all interested agents and clients, as it unnecessarily increases network traffic beyond this region.

`multicast-delay`

The *multicast-delay* option is a server-only configuration option and specifies how frequently in seconds the server sends notifications. The smaller this value is, the more responsive clients and agents are. That is, the shorter they have to wait for notifications. The smaller the value is, however, the more network traffic is generated by the server. The default value is 1 second.

InfoSphere Guardium S-TAP for IMS server

The InfoSphere Guardium S-TAP for IMS server provides central management and control of all InfoSphere Guardium S-TAP for IMS functions performed on behalf of user requests.

Note: Only one server instance per SYSPLEX is permitted, and that instance is required to manage the agents monitoring your IMS subsystems and supporting all InfoSphere Guardium S-TAP for IMS users.

Server environment

The InfoSphere Guardium S-TAP for IMS server must be running in order for users to perform any InfoSphere Guardium S-TAP for IMS functions.

Server security

The InfoSphere Guardium S-TAP for IMS server uses RACF security.

APF authorization

The InfoSphere Guardium S-TAP for IMS server and agent must run APF-authorized.

Server job output

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

Stopping the server

Use the following commands to stop the InfoSphere Guardium S-TAP for IMS server.

The server accepts standard z/OS /MODIFY and /STOP commands. From SDSF (or anywhere else that you can issue commands), you can issue one of these commands to the server:

`/MODIFY server-job-name,STOP`
This initiates a graceful server shutdown which causes the server to:

1. Stop accepting new client connections.
2. Send a message to all existing client connections that the server is trying to stop.
3. Wait for all existing client sessions to end.
4. End.

Note: Issuing the /STOP <job-name> command prevents you from issuing a /MODIFY <server-job-name>,FORCE or another STOP or MODIFY command.

`/STOP server-job-name`
This performs exactly the same function as the /MODIFY server-job-name,STOP command.

`/MODIFY server-job-name,FORCE`
This initiates a server hard stop which causes the server to:

1. Immediately drop all client connections.
2. Initiate a cancel on all running threads.
3. Exit as soon as the threads exit.

Note: Issuing this command is not recommended under normal circumstances.

InfoSphere Guardium S-TAP for IMS agent

The InfoSphere Guardium S-TAP for IMS agent provides access to database and system services, in support of the product's server and remote clients.

Agent environment

The agent must be running in order for InfoSphere Guardium S-TAP for IMS users to perform any functions related to the IMS subsystems monitored by that agent.

Agent security

APF authorization

The InfoSphere Guardium S-TAP for IMS server and agent must run APF-authorized.

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 and when errors occur.

In the event of exceptional conditions, additional messages might be written to the SYSOUT DD. If an abend occurs, dump information may be written to the CEEDUMP and (or) SYSUDUMP DDs. This information may 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.

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

`/MODIFY agent-job-name,STOP`

This initiates a graceful agent shutdown which causes the agent to:

1. Stop accepting new server connections.
2. Wait for all existing requests to finish.
3. Exit.

`/STOP agent-job-name`

This command performs exactly the same function as the /MODIFY agent-job-name,STOP command.

`/MODIFY agent-job-name,FORCE`

This initiates an agent hard stop which causes the agent to:

1. Immediately stop accepting new server requests.
2. Initiate hard cancels on all running threads.
3. Exit as soon as the threads exit.

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 are also started. These include the SMF data collector address space (SAUISMAP member AUIFssid) which collects events using SMF log data as input and sends the events to the appliance, and the DLI event data collector (SAUISAMP member AUIBssid) which reads event data from the z/OS log streams (Batch and Online) and send the events to the appliance. One IMS Archive Log event Data collector (SAUISAMP member AUILssid) 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 batch/online data collector

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

- /MODIFY <jobname>,START COLLECTOR IMS
- /MODIFY <jobname>,STOP COLLECTOR IMS

The STOP command may be used to stop the IMS Batch/Online collector:

- /STOP <jobname>

To ensure all events are read and purged from the Batch and Online DLI log streams, a DRAIN command may be used. To effect the DRAIN of the log streams, all collections for the agent must be deactivated.

- /MODIFY <jobname>,DRAIN

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 AUILssid address is started by the agent address space, or activation of a collection.

Stopping a specific AUILssid address space requires the use of the /STOP <jobname>.<token> command. The <token> value to be used can be found during AUILssid start-up in the AGENT JOBLOG. (For example, in "S AUILRS22.AAAAAAAC", AAAAAAAC is the token value) or when viewing the AUILssid task in TSO SDFS, the token is displayed as the STEPNAME.

Managing the audit repository

InfoSphere Guardium S-TAP for IMS saves configuration data to collect into a VSAM repository known as the audit repository.

By default, InfoSphere Guardium S-TAP is configured to not collect any audit data. To initiate collection of audit data, the administrator must define at least one audit collection profile and activate it using the corresponding audit data collection agent.

Tip: It is recommended that you make daily or weekly image copies of the repository.

Chapter 4. Administration tasks

The InfoSphere Guardium S-TAP for IMS administration user interface enables administrators to perform a variety of administrative tasks including managing users (add, edit, clone, delete), groups (add, edit, clone, delete), IMS subsystems (add, edit, delete), collection profiles (activate, deactivate), collections (add, edit, clone, delete), and agents (edit only).

The tabs on the interface are presented in order of task:

Users tab
Enables user account management, assignment of specific user permissions, and assignment of user membership to one or more groups.

Groups tab
Enables assignment of specific group permissions, and assignment of one or more users to a particular group.

IMSs tab
Enables selection of a particular agent, specification of IMS RECONs and Control libraries, and SMF and IMS log event filtering for each specific IMS definition.

Agents tab
Enables editing of SMF Masks, Stream Names, and allocation of agent-related Spill data sets as well as SMF and IMS log event filtering for all IMS systems controlled by the agent.

Collection profiles tab
Allows definition of audit rules based on database, segment, PSB name, or user ID. The selection of DLI calls to be audited as well as the collection of concatenated key and segments data may also be specified.

Collections tab
Allows the enabling or disabling of collection profiles and associates the collection profile with an IMS definition.

Starting the administration client

Start the InfoSphere Guardium S-TAP for IMS administration client from the Windows Start menu.

Click: **Start** > **Programs** > **InfoSphere Guardium S-TAP for IMS v8.2** > **Administrator v8.2** to start the administration client.

First, select a listed server from the **Settings** menu, or use the **Settings** > **Define Servers** menu option to manually define a server by typing the host name and port of a server that is not in the list. After selecting or defining a server, log in and connect to the desired InfoSphere Guardium S-TAP for IMS server.

Specifying a server

Before you can log in to InfoSphere Guardium S-TAP for IMS, you must first specify a server. You can either select a server from a list of available servers — or you can add a server.

To select a server from a list of available servers:

1. From the main menu, click **Settings**. The client lists previously specified servers in the server list (the most recently selected server is selected by default).
2. Select the server to which you want to connect using one of the following methods.
   - Click the InfoSphere Guardium S-TAP for IMS server to which you want to connect.
   - If the server you want to select is not listed, click **Define Servers** to add a server definition.

Initial log in

This information describes the initial log in procedure for logging into InfoSphere Guardium S-TAP for IMS using the administration user interface.

To log in to InfoSphere Guardium S-TAP for IMS for the first time:

Note: SAUISAMP job AUISJUAP must be customized and executed successfully before attempting to perform the initial log in.

1. From the main menu, click **Settings** and then select the InfoSphere Guardium S-TAP for IMS server to which you want to connect.

   Note: The server you specify must be running in order to successfully log in to InfoSphere Guardium S-TAP for IMS.
2. Log in using the default administrator user name and password:
   a. In the **Username** field, type the default administrator user name: `auiadmin`.
   b. In the **Password** field, type the password.
3. Click **Login**.

Once logged in, change the password for the default administrator user name and then delete it from the AUICFGU configuration file.

Adding a server definition

To add a server definition, you must provide the name of the server, the host and port settings.

To add a server definition:

1. From the main menu click **Settings** > **Define Servers**. The InfoSphere Guardium S-TAP for IMS Server Definitions window appears.
2. Click **Add**. The Server Editor window appears.
3. In the **Description** field, type the name of the server. For example: `AUISRVR1`
4. In the **Server Host** field, type the host specification of the server. For example: `123.ABCSOFTWARE.COM`
5. In the **Server Port** field, type the port specification of the server. For example: `12345`
6. Click **OK**.

Deleting a server definition

You can delete a particular server's definition so that the server is no longer available in the list of available servers.

To delete a server's definition and remove the server from the list of available servers:

1. From the main menu click **Settings** > **Define Servers**. The InfoSphere Guardium S-TAP for IMS Server Definitions window appears.
2. Click the server definition you want to remove.
3. Click **Delete**. The message `"Are you sure you want to delete the selected server definition?"` appears.
4. Click **Yes** to delete the selected server definition; otherwise click **No**.
5. Click **OK** to continue.

If you choose to delete a server definition, a check will first be made to see if InfoSphere Guardium S-TAP is connected to that server. If the server is not connected, the server definition is deleted. If the server is connected, a dialog appears to confirm that you want to disconnect from the server in order to delete the server definition.

Logging out from a server from the administration client

This information describes how to log out from the server from the administration client.

To log out from the server, click **File** > **Logout**. The log in window appears.

User administration

InfoSphere Guardium S-TAP for IMS user administration includes the tasks of managing user accounts, assigning permissions to users, and assigning users to groups.

From the administration interface, **Users** tab, administrators can create users, clone users, edit, and delete users. For each user, the **Users** tab displays information to identify the user and the user's assigned privileges (a checkmark indicates that the user has been assigned the corresponding privilege).

Note: Click **Refresh** from the **Users** tab to update the data display prior to adding, editing, cloning, or deleting users. Clicking **Refresh** queries the server for updates to enable you to view the latest data.

Adding a user

The New User Wizard enables privileged users to add a user to InfoSphere Guardium S-TAP for IMS.

Note: To add a new user to InfoSphere Guardium S-TAP for IMS, you must have the Create Users privilege. The Assign Permissions privilege and the Assign Users to Groups privilege are required to assign permissions to users and to add or remove groups from users, respectively.

To add a new user:

1. From the **Users** tab, click **Add** to open the New User Wizard. The first page of the New User Wizard appears. The outline of the steps needed to add the new user to InfoSphere Guardium S-TAP for IMS appears at the left side of the page.

   Note: Use the **Back** and **Next** buttons to navigate through the New User Wizard, or click on the various nodes at the left side of the panel to move through steps of the wizard.
2. Complete each step of the wizard as described in this guide. A summary overview is provided at the end of the wizard, including the new user account details, assigned privileges, and the groups to which the user is assigned.
3. Click **Finish** to add the new user to InfoSphere Guardium S-TAP for IMS, or **Cancel** to exit without saving. When added, the new user and its associated privileges appear in the list of users on the Users tab.

Specifying the user name and password (User Name)

Specify a username and password to uniquely identify the user.

To specify the username, an optional description, and the user password:

1. In the **Username** field, type the user name. The user name should not be less than 2 characters or exceed 40 characters. The name must not begin or end with a space.
2. In the **Password** field, type a password for the user. Note the following password restrictions enforced by the InfoSphere Guardium S-TAP for IMS administration client:
   - The password should not be less than 6 characters, nor more than 40 characters.
   - The password must not begin or end with a space.
   - The username and password are case-sensitive and must each contain at least two unique characters (two characters that are not in the other). The password should consist of a combination of letters and numbers.

     For example:
     - Correct: ABCuser1 and Pass123P with the password containing 40 or fewer characters.
     - Incorrect: ABCuser1 and ABCuserP.
3. In the **Description** field, type an optional user description (128 characters maximum).
4. In the **Expires in** field, specify the number of days the user account you are creating should remain active.

   Note:

   - The password you provide remains active for the specified number of days, at which time the user must specify a new password.
   - When selecting an integer value (1-999), the password is valid for today plus the number of days specified. Midnight is considered the start of the next day.
   - The password for a user expires at midnight based on the time zone in which the InfoSphere Guardium S-TAP for IMS server is running. If the client and server are running in different time zones, the expiration date displayed by the administration client is before or after the password actually expires on the server.

Assigning user permissions (Permissions)

Permissions enable or prevent users from performing specific activities within InfoSphere Guardium S-TAP for IMS.

Note: You must have the Assign Permissions privilege to assign permissions to users.

Assign or remove a privilege as follows:

- To assign a privilege, click the check box that corresponds to the privilege you want to assign to the user.
- To remove a privilege, click the check box to clear the selection.

New user permissions take effect as soon as they are defined and will be recognized by the client upon the user's next login. If a user's permissions are increased, the newly allotted privileges will not be allowed by the client until the next log in. If a user's permissions are decreased, the server will disallow the relevant actions when they are attempted. For this reason, permissions are checked in both the client and the server.

InfoSphere Guardium S-TAP for IMS privileges and permissions:

This topic describes the available privileges and permissions InfoSphere Guardium S-TAP for IMS provides.

`Connect to InfoSphere Guardium S-TAP for IMS`
Permission to connect to InfoSphere Guardium S-TAP for IMS using the administration user interface.

`Create Users`
Permission to add new users. If a user is assigned the Create Users permission, that user has the authority to edit, clone, or delete any users that they create.

`Create Groups`
Permission to add new groups. If a user is assigned the Create Groups permission, that user has the authority to edit, clone, or delete any groups that they create.

`Create Profiles`
Permission to add new profiles. If a user is assigned the Create Profiles permission, that user has the authority to edit, clone, or delete any profiles that they create.

`Edit Profiles`
Permission to modify existing profiles.

`Assign Permissions`
Permission to grant, or revoke, all types of user and group permissions When used with the Create Users permission, all permissions can be granted to users. When used with the Create Groups permission, all permissions can be granted to groups.

`Assign Connect`
Permission to grant or revoke the Connect to InfoSphere Guardium S-TAP privilege. This allows an administrator to quickly disable a user's ability to access InfoSphere Guardium S-TAP while keeping all user data intact.

`Assign Users to Groups`
Permission to add and remove users to, and from, groups.

Manage Agent Level Audit Options
Permission to add, delete, and modify SMF and IMS Archive log options at the agent level, which will cascade to all IMS definitions under the agent.

Manage IMS Definitions and Agent Configurations
Permission to add, delete, and update IMS definitions to be audited by an agent as well as agent configuration parameters.

Related tasks

"Assigning permissions to the group (Permissions)" on page 46
Permissions enable, or prevent, members of the group from performing specific activities within InfoSphere Guardium S-TAP for IMS.

Assigning the user to groups (Groups)

Assigning users to groups is an easy method of assigning a common set of privileges to more than one user.

Note: You must have the Assign Users to Groups privilege to add or remove users from groups.

Available groups to which the user can be assigned are shown in the **Available Groups** list. Groups that the user is currently a member of are shown in the **Assigned Groups** list.

- To assign a user to a group, in the **Available Groups** list, click the group you want to add the user to and then click **Add**. (To add the user to all available groups, click **Add All**.)
- To remove a user from a group, in the **Assigned Groups** list, click the group that you want to remove the user from and then click **Remove**. (To remove the user from *all* groups, click **Remove All**.)

User summary (Summary)

A summary overview of the new user account is the last step in the **New User Wizard.** The summary includes the new user account details, assigned privileges, the groups to which the user is assigned, and an expiration date of the user, if one is specified.

Editing a user

The User Editor enables you to modify user account information, permissions, and add or remove a user from groups.

To modify a user you must have the Create Users privilege. The Assign Permissions privilege and the Assign Users to Groups privilege are required to assign permissions to users and to add or remove users from groups, respectively.

To edit a user:

1. From the **Users** tab, click the user you want to edit.
2. Click **Edit**. The first page of the User Editor appears.
3. Complete each applicable step. You can click on a step from the hierarchy at the left of the panel to display the corresponding page of the editor.

   Note: If the **Password** and **Confirm Password** fields are left blank, the original password will be used.
4. Click **Finish** to save your modifications or **Cancel** to exit without saving.

Cloning a user

Cloning a user creates a copy of a selected (existing) user, as well as that user's assigned user permissions and group memberships, and enables you to modify the user information.

To clone a user you must have both the Create Users, Assign Permissions, and Assign Users to Groups privileges. The Assign Permissions privilege and the Assign Users to Groups privileges are required to assign permissions to users, and to add or remove users from groups, respectively. The Create Profiles permission is required to create a copy of each of the permissions that are assigned to the source user.

To clone a user:

1. From the **Users** tab, click the user you want to clone.
2. Click **Clone**. The first page of the User Editor appears. The current step in the process is highlighted at the left side of the page.
3. Complete each applicable step. You can click on a step from the hierarchy at the left of the panel to display the corresponding page of the User Editor.

   Note: You must specify a unique username and password for the cloned user.
4. Click **Finish** to save the cloned user or **Cancel** to exit without saving.

Deleting a user

Deleting a user removes all user information for an InfoSphere Guardium S-TAP for IMS user.

You must have the Create Users privilege to delete users. To delete a user:

1. From the **Users** tab, click the user you want to delete.
2. Click **Delete**. The message `"Are you sure you want to delete the selected user?"` appears.
3. Click **Yes** to confirm the deletion; otherwise click **No**. Upon confirmation of the deletion, the user is deleted.

Group administration

InfoSphere Guardium S-TAP for IMS group administration includes the tasks of managing groups, assigning permissions to groups, and assigning users to groups.

Assigning users to groups is a convenient way to assign a specific set of permissions to one or more users. From the administration interface **Groups** tab, administrators can create groups, edit groups, clone groups, and delete groups.

For each group, the **Groups** tab displays information to identify the group and the group's assigned permissions (a checkmark indicates that the group has been assigned the corresponding permission).

Note: Click **Refresh** from the **Groups** tab to update the data display prior to adding, editing, cloning, or deleting groups. Clicking **Refresh** queries the server for updates to enable you to view the latest data.

Default groups

Assigning privileges to users determines who will be allowed enable users to create or access database resources.

Use of InfoSphere Guardium S-TAP for IMS functionality is granted to users with the required privileges. InfoSphere Guardium S-TAP for IMS creates two default groups, **limited** and **admin**. These groups grant common sets of privileges to their members.

limited
Indicates the user has the ability to connect to InfoSphere Guardium S-TAP for IMS only. Members of this group will usually be auditors. They will have access to audited data as defined by their permissions.

admin
Indicates the user has full privileges. Members of this group are usually administrators for InfoSphere Guardium S-TAP for IMS, and have full administrative control of the product.

These default groups are created for your convenience and can be modified or deleted as desired.

Adding a group

Use the **New Group Wizard** to add a new group to InfoSphere Guardium S-TAP for IMS.

You must have the Create Groups privilege to add groups. The Assign Permissions privilege and the Assign Users to Groups privilege are required to assign permissions to groups and to add or remove users from groups, respectively.

To add a new group:

1. From the **Groups** tab, click **Add** to open the **New Group Wizard.** The **New Group Wizard** appears. The outline of the steps needed to add a group appears on the left side of the page.

   Note: Use the **Back** and **Next** buttons to navigate through the New Group Wizard, or may click on the various nodes at the left side of the page to move through the steps.
2. Complete each step of the wizard. A summary overview of the new group will be provided, including the new group details, assigned privileges, and the list of users assigned to the group.
3. Click **Finish** to add the new group, or **Cancel** to exit without saving. A newly created group, and its associated privileges, appears in the list of groups on the **Groups** tab.

Specifying the group name and description (Group name)

Specify a group name and optional description to identify the user group.

To specify the group name and an optional description:

1. In the **Group name** field, type the name of the group (40 characters maximum). The group name must not begin or end with a space.
2. In the **Description** field, type an optional description of the group (128 characters maximum).

Assigning permissions to the group (Permissions)

Permissions enable, or prevent, members of the group from performing specific activities within InfoSphere Guardium S-TAP for IMS.

Note: You must have the Assign Permissions privilege in order to assign permissions to a group.

Assign or un-assign group privileges as follows:

- To assign a privilege, click the check box that corresponds to the privilege you want to assign to the group.
- To un-assign a privilege, click the check box to clear the selection.

Related reference

"InfoSphere Guardium S-TAP for IMS privileges and permissions" on page 43
This topic describes the available privileges and permissions InfoSphere Guardium S-TAP for IMS provides.

Assigning users to a group (Members)

Assigning users to groups is an easy method of assigning a common set of privileges to more than one user.

You must have the Assign Users to Groups privilege to assign users to (or remove users from) groups.

Available users that can be added to the group are shown in the **Available Users** list. Current members of the group are shown in the **Group Members** list.

- To assign one or more users to the group, in the **Available Users** list, click the user (or users) you want to add and then click **Add**. (To add all available users to the group, click **Add All**.)
- To remove a user from the group, in the **Group Members** list, click the user (or users) that you want to remove and then click **Remove**. (To remove all of the users from the group, click **Remove All**.)

Group summary (Summary)

A summary overview of the new group is the last step in the **New Group Wizard.** The summary includes the new group details, assigned privileges, and the list of users assigned to the group.

Editing a group

The **Group Editor** enables you to modify the group details, permissions, and add or remove users from groups.

To edit a group you must have the Create Groups privilege. The Assign Permissions privilege and the Assign Users to Groups privilege are required to assign permissions to groups and to add or remove users from groups, respectively.

To edit a group:

1. From the **Groups** tab, click the group you want to modify.
2. Click **Edit**. The first page of the **Group Editor** appears.
3. Complete each applicable step. You can click on a step from the hierarchy at the left of the panel to display the corresponding page of the editor.
4. Click **Finish** to save your modifications or **Cancel** to exit without saving.

Cloning a group

Cloning a group creates a copy of a selected (existing) group with group permissions, user memberships, permissions, and enables you to modify the group permissions.

You must have the Create Groups privilege to clone groups. The Assign Permissions privilege and the Assign Users to Groups privilege are required to assign permissions to groups and to add or remove users from groups, respectively. The Create Profiles permission is required to create a copy of each of the permissions that are assigned to the source group.

To clone a group:

1. From the **Groups** tab, click the group you want to clone.
2. Click **Clone**. The first page of the **Group Editor** appears.
3. Complete each applicable step of the wizard. You can click on a step from the hierarchy at the left of the panel to display the corresponding page of the **Group Editor**.

   Note: You must specify a unique name for the cloned group.
4. Click **Finish** to save the cloned group or **Cancel** to exit without saving.

Deleting a group

Deleting a group removes all definitions for a particular group.

You must have the Create Groups privilege to delete groups.

To delete a group:

1. From the **Groups** tab, click the group you want to delete.
2. Click **Delete**. The message "Are you sure you want to delete the selected group" appears.
3. Click **Yes** to confirm the deletion; otherwise click **No**. Upon confirmation of the deletion, the group is deleted (any associated permissions are also deleted).

Agent administration

From the **Agents** tab, you can access the **Agent Editor** to modify the SMF auditing parameters, z/OS system log, and IMS Archive log auditing parameters for a selected agent. For each active or inactive InfoSphere Guardium S-TAP for IMS agent, the **Agents** tab displays information that identifies the particular agent, the status of its audit collectors (a check mark indicates that the corresponding collector is active).

Note: Click **Refresh** from the **Agents** tab to update the data display prior to modifying the agent configuration settings. Clicking **Refresh** queries the server for updates to enable you to view the latest data.

Adding an agent

Supply the following customization and configuration information before starting the agent task.

To add an agent:

1. Customize the agent task JCL (SAUISAMP member AUIAssid).
2. Provide configuration information (SAUISAMP member AUICFGA).
3. Start the agent task.

At agent start-up, the repository will be populated with an agent record stub, allowing the agent to be visible from the administration user interface, and permitting more detailed customization to occur.

Note: The agent must be configured before an IMS definition can be created.

Modifying an agent

The **Agent Editor** enables you to modify the SMF and IMS archive log audit parameters, and z/OS system log stream names.

You must have the Manage Agent Level Audit Options privilege to modify the IMS definitions and agent configuration settings.

Note: The administration client does not permit the modification of an InfoSphere Guardium S-TAP for IMS agent configuration for an agent that is offline or not available.

To modify the agent:

1. From the **Agents** tab, select the agent that you want to modify. Double-click the agent or click **Edit** to open the **Agent Editor**.
2. Complete each step from the hierarchy at the left of the editor. The summary panel displays a summary of the new agent configuration settings.
3. Click **Finish** to save your changes, or click **Cancel** (changes are not saved).

SMF Customization process

The SMF customization process requires three areas of customization, to SMF events, SMF spill data sets, and SMF masks.

SMF Events
Allows you to limit the events to be captured by the SMF Data Collector. The settings are propagated to every IMS definition controlled by the agent.

SMF Spill Data Set
Required to maintain SMF event persistence, where an event was found and the SMF accounting record (which is required to complete the SMF event) has yet to be produced by SMF. Only one SMF spill data set is required per agent.

SMF Masks
SMF data set mask are used to identify SMF log data sets to be processed using the z/OS catalog.

Access SMF Events, SMF Spill Data Set, and SMF Masks by navigating the drop-down hierarchy on the left of the Agent Editor panel, or by clicking on the available tab headings.

Related reference

"SMF customization" on page 31
For SMF customization, SMF events, SMF spill data sets, and SMF masks, as well as the IMS log and log stream must be customized. Detailed information on how to customize these areas is available in this User's Guide.

Modifying SMF events

This topic describes the options for modifying SMF events, as well as the rules for auditing.

Options to modify SMF events include the following:

- Audit All SMF events
- Audit data set OPEN for UPDATE
- Audit data set DELETE
- Audit data set OPEN for READ
- Audit data set CREATE
- Audit data set ALTER
- Audit Data set RACF violations

Note: Selecting **Audit All SMF events** results in all SMF events to be audited.

- A check mark beside the event type indicates that these events will be audited by all IMS systems defined to the agent, unless overridden at the IMS level.
- If unchecked, these events will not be audited by any IMS defined to the agent, and cannot be superseded at the IMS level.

Specifying an SMF spill data set

Follow these specifications for modifying and allocating an SMF spill data set.

An SMF spill data set must be defined as a sequential (DSORG=PS), Fixed Block (RECFM=FB) data set with a logical record length of 300bytes (LRECL=300). You may allocate this data set using TSO/ISPF or batch JCL and supply the data set name in the SMF Spill Data set input field. Alternatively, you may click **NEW...** to invoke the **Spill Data set allocator** utility to guide you through the allocation process.

The sizing of this dataset (SPACE=) is subject to the following:

- the frequency of the SMF data collector queries to the z/OS catalog for new SMF log data sets to process
- the number of LPARS in your SYSPLEX environment
- the SMF Event Expiration value supplied to the SAUISAMP AUICFGA member (parameter: **<smf-event-expiration-days>xx</smf-event-expiration-days>**)

Each incomplete SMF event (an SMF event for which a type x'30'' SMF accounting record has yet to be found) consumes 300 bytes, or one record. Incomplete events are stored in the SMF spill data set until:

- the associated SMF type x'30'' log record is encountered and the complete event is sent to the appliance
- a system IPL record SMF type x'00' log record is encountered, and the incomplete event is sent to the appliance with an indicator that the incomplete event was sent, due to an IPL being encountered
- the number of days since the SMF event was created by SMF has expired per the smf-event-expiration-days value. In this case, the incomplete event is forwarded to the appliance with an indicator providing the smf-event-expiration-days value, stating that the expiration date has occurred.

In all the above cases, after the SMF event is sent to the appliance, the SMF event is removed from the SMF spill data set.

Tip: Size the SMF spill data set to one cylinder per day that you wish to retain the incomplete SMF event as a primary quantity value, and 1.5 cylinders per day as the secondary quantity value. Using the RLSE parameter when pre-allocating the dataset as part of the SPACE= keyword is recommended.

SMF collection customization

SMF collection customization involves defining SMF collections data sets, establishing naming conventions for SMF data collection data sets, and customizing the copy the AUIFssid member to the PROCLIB for the site.

The agent must be able to process SMF data from each member LPAR of the SYSPLEX. To do this, extract the SMF records that InfoSphere Guardium S-TAP for IMS requires from the SMF dump data from each LPAR, and merge these into a single SMF log for InfoSphere Guardium S-TAP.

Note: Please contact the system administrator to determine the location of the PROCLIB in order to copy the AUIFssid member to the correct PROCLIB.

Defining SMF collection data sets

InfoSphere Guardium S-TAP for IMS keeps track of the most recently processed SMF data set. At the start of each processing cycle, the z/OS catalog is queried for data set names that meet the selection criteria (SMF data set mask). InfoSphere processes only previously unprocessed SMF data sets in data set name sequential order.

For a new installation, only SMF data sets that meet the selection criteria (SMF DSN mask) and are less than two days old are considered for processing. This is to avoid the potential of processing a large amount of historical data if the SMF DSN mask chosen returns SMF data sets created months ago or longer.

Important: Do not extend (DISP=MOD) onto a processed SMF log as the records added to the already processed log will not be processed by InfoSphere Guardium S-TAP for IMS.

Note: InfoSphere Guardium S-TAP for IMS can only report events that are being collected by SMF. Please review IMS log types and SMF record types collected by InfoSphere Guardium S-TAP for IMS for a list of SMF records used to report events. If any SMF record type in the table is not being collected at your site, InfoSphere Guardium S-TAP for IMS cannot report that event.

Naming conventions for SMF data collection data sets

The agent uses the SMF DSN mask in order to build data set names from the catalog. The mask must be specific enough to only return SMF logs. The naming convention for SMF log data sets must be such that the collating sequence must be in ascending order by date/time or a Generation Data Group (GDG). If the logs are GDG(s) then this will be the natural order. If the logs are not GDG(s) then the SMF log DSN must contain a date/time qualifier that will ensure the correct sequence.

For example:

```
hlq.SMFDUMP.Dyymmdd.Thhmmss.LOG
```

A date format of the form dmmddyy or dddmmyy will not provide the correct collating sequence. A date qualifier must be in the following form:

```
Dyymmdd
Dyyddd
Dyyyyddd
```

Note: GDG is the recommended implementation.
The AUISMFDF JCL in the SAUISAMP data set can be used to define the GDG base if that is the method that you chose.

Customizing the AUISMFDP JCL

This member must be customized prior to execution. Valid JOB statements, the DSN(s) of the input SMF data sets, the DSN of the output SMF data sets to be used by the AUIF<ssid> task, and output unit mnemonic must be provided. You may provide SMF DUMP data sets for more than one LPAR of your SYSPLEX as the SMFIN data set in a concatenation.

Note: The AUISMFDP job is not scheduled automatically by InfoSphere Guardium S-TAP for IMS. You must run the job manually or include it in your automated scheduling tool.

Agent Editor SMF mask rules and specifications:

Creating a mask for specified system, through the administration client's Agent Editor (SMF Masks) panel, allows you to specify the dataset name that the AUISMFDP job (from the SAUISAMP dataset) will create. This job contains the SMF data needed by InfoSphere Guardium S-TAP for IMS, in order to perform auditing on IMS artifacts accessible outside of normal IMS services.

The AUISMFDP output dataset may be a Generation Data Group (GDG) entry, formatted using a DATE/TIME, or another naming convention that causes the data sets to be presented in ascending order of creation. The only wildcard character that may be coded in the dataset name mask you specify is percentage sign (‘%').

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.

Masking character rules

The following are processing rules that pertain to the specification of the percentage sign.

Single percentage (%)
A single percentage sign indicates that only one alphanumeric or national character may occupy that position.

Multiple percentages (%%%)
Multiple percentage signs indicate that more than one character may substituted, with the number of substitution characters being equal to the number of percent signs specified.

Examples of recommended specifications

Specifying a GDG dataset in the **Mask for system name** field of the Agent Editor (SMF Masks) panel of the administration client. If the AUISMFDP job has been customized to produce a GDG dataset as the SORTOUT DD output data sets, you may specify one of the following options.

Specify the fully qualified GDG base name in the Mask for system name field, for example: `A.B.C.`
InfoSphere 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
```

Specify a data set name explicitly providing the Generation and Version values as a mask, for example: `A.B.C.G%%%%V%%`

InfoSphere Guardium S-TAP for IMS uses catalog services to determine the names of all cataloged datasets that match this mask, for example:

```
A.B.C.G0021V00
A.B.C.G0022V00
A.B.C.G0023V00
```

Specifying a DSN using a DATE/TIME naming convention

If the AUISMFDP job has been customized to produce a dataset name containing DATE and TIME values as qualifiers within the dataset name as the SORTOUT DD output datasets, you may specify the dataset name using a string of percent signs within the DATE and TIME qualifier names, for example: `HLQ.D%%%%%%.T%%%%%%.SMFDATA`

InfoSphere 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
```

IMS Log customization

This section describes IMS Log events and options for their modification.

IMS Log events

IMS Log events allow you to limit the events to be captured by the IMS Archive Log Data Collector. Option settings are propagated to every IMS definition controlled by the agent.

Modifying IMS Log events

Options to modify IMS log events include:

- Audit All IMS Log events
- Audit IMS Control Region starts/stops
- Audit User Sign/Signoff
- Audit DBD OPEN/CLOSE
- Audit DBD/PSB DBDUMP/START/STOP/LOCK/UNLOCK

Note: Selecting **Audit All IMS Log events** results in all IMS Log events being audited.

- A check mark beside the event type indicates that these events will be audited by all IMS systems defined to the agent, unless overridden at the IMS level.
- If unchecked, these events will not be audited by any IMS defined to the agent, and cannot be superseded at the IMS level.

Related concepts

"Collection profiles" on page 58
This section describes how collection profiles use DLI Calls, IMS Archive logs, and SMF data to determine the capture of audit events.

z/OS Log stream customization

Batch DLI Log stream name and Online DLI Log stream name represent the z/OS system log streams that serve as the logging media for audit data collected by InfoSphere Guardium S-TAP for IMS. The names of these data sets should reflect the log stream names used in the AUISAMP installation member AUILSTR2 for XCF based log streams, or if using DASD-ONLY log-streams, SAUISAMP member AUILSTR3.

Note: The log streams must be defined to your z/OS system before attempting to provide the log stream names to the agent using the Agent Editor.

Batch DLI Log stream name
Used to collects audit data generated when IMS DLI/DBB batch jobs are executed.

This name should match the name used as the "batch_logstream_name" variable, supplied to the **NAME** parameter of the DEFINE LOGSTREAM control statement of the Define Structure and Log stream for IMS Batch processing section of the control statements.

Online DLI Log stream name
Used to collect audit data generated by IMS Online transactions and BMPs.

This name should match the name used as the "online_logstream_name" variable supplied to the **NAME** parameter of the DEFINE LOGSTREAM control statement of the Define Structure and log stream for IMS Online processing section of the control statements.

Note: Both the **Batch log stream name** and **Online DLI Log stream name** fields are required. Each specified name must be unique, and cannot be shared between agent definitions.

Related reference

"z/OS log streams" on page 10
IMS batch jobs and online regions monitored by InfoSphere Guardium S-TAP for IMS write the audit data to z/OS log streams.

IMS administration

InfoSphere Guardium S-TAP IMS administration includes the tasks of managing and configuring new and existing IMS subsystems.

From the administration interface **IMSs** tab, administrators can create, edit, and delete IMS subsystems. For each IMS subsystem, the **IMSs** tab displays detailed information about the subsystem, including the IMS name, description, the monitoring agent, RECONS, and IMS data sets.

- In order to add or delete an IMS entry, you must have the Create Profile privilege, or belong to a group that has the Create Profile privilege.
- In order to edit an IMS entry, you must have the Edit Profile privilege, or belong to a group that has the Edit Profile privilege.

Note: Click **Refresh** from the **IMSs** tab to update the data display prior to adding, editing, or deleting IMS entries. Clicking **Refresh** queries the server for updates to enable you to view the latest data.

Creating an IMS entry

From the **IMSs** tab, click **Add** to open the New IMS Wizard.

The agent must be configured before an IMS entry can be created.

1. Complete each panel of the New IMS Wizard, clicking **Back** or **Next** to navigate.
2. Review the selected options in the IMS Summary panel. Click **Back** to make any necessary changes.
3. If the IMS Summary panel displays the correct information, click **Finish** to add the IMS entry and return the IMSs tab main panel, or **Cancel** to close the New IMS Wizard without adding the new IMS entry.

Considerations

The following considerations apply to IMS source definitions.

IMSPLEX Data Sharing Considerations

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

In an IMS data sharing environment where only a subset of databases are shared, an IMS definition must be created for each IMS subsystem that have nonshared databases to be audited. In this case, auditing information for shared databases will be collected and stored under the IMS definition with the name that is the lowest in a sorted collating sequence.

XRF Considerations

In an IMS XRF environment, only one IMS definition is required. InfoSphere Guardium S-TAP for IMS is not sensitive to which XRF partner is currently active, and will continue to produce audit data in the event of an XRF ACTIVE/BACKUP switch.

Adding an IMS Entry

To add an IMS Entry, click **Add** from the **IMSs** tab to open the New IMS Wizard.

IMS Entry Name
This is the name that InfoSphere Guardium S-TAP for IMS uses to reference the IMS environment. It must be a unique name using up to 8 characters and must not be currently defined to any other InfoSphere Guardium S-TAP for IMS agent in the SYSPLEX. This name does not have to reflect an IMS SSID or RSENAME.

Description
This is an optional field that must not exceed 128 characters.

Agent The IMS Agent can be selected from the list of supported IMS Agents. This value is used when deblocking control blocks found in the RESLIB, DBDLIB and PSBLIB data sets. In a data sharing environment where multiple IMS versions are participating, the version specified should reflect highest IMS version of the participating data sharing IMS subsystems.

RECONS

When prompted, enter the RECON data set names used by the DBRC region for this IMS environment. Specify an explicit DSN, or use a DSN mask to retrieve a list of data sets when the combo box is expanded. The RECON data sets are used to determine database names that may be considered candidates for auditing. At least two RECON data sets must be specified (RECON1 and RECON2). A data set specification for RECON3 is optional.

Note:

- A set of RECONS can only be defined to a single AUI IMS definition
- Databases must be defined to DBRC in order to be audited. The RECON data sets are also used to determine which IMS Archive Log data sets should be read when auditing IMS Online system starts and stops, IMS Users signing on and off, database opens and closes, and database and PSB starts and stops.

IMSPLEX

A five byte name used to specify the IMSPLEX name when DBRC RECON loss notification or DBRC parallel RECON access is in effect for the IMS being audited, and the DSPSCIX0 DBRC SCI Registration exit routine is not being used. If you are unsure of your sites or DBRC access requirements, please check with IMS systems programmer or other support personnel.

IMS Data Sets

When prompted, enter the RESLIB, DBDLIB and PSBLIB data set names used to determine IMS system, database, and PSB configuration information.

RESLIB: Enter the data set name(s) that contain the IMS Nucleus and action modules. *See the IBM IMS Installation manual under the topic IMS.SDFSRESL for details.* You may enter up to five data sets, each separated by a semi-colon (;). You may enter an explicit data set name or provide a DSN mask, and click **Browse** to retrieve a list of matching data set names. In an IMS data sharing environment that utilizes multiple IMS versions, the RESLIB of the IMS with the highest version of IMS should be specified.

DBDLIB: Enter the data set name(s) that contain the Database Description blocks(DBD) created by the DBDGEN utility. *Refer to the IBM IMS Installation manual under the topic IMS.DBDLIB for details.* The DBDLIB(s) are used to determine the database type and segment information when providing a list of databases and segments to be audited. You may enter up to five data sets, each separated by a semi-colon (;) You may enter an explicit data set name or provide a DSN mask, and click **Browse** to retrieve a list of matching data set names.

PSBLIB: Enter the data set name(s) that contain the Program Specification Blocks (PSB) created by the PSBGEN utility. *Refer to the IBM IMS installation manual under the topic IMS.PSBLIB for details.* The PSBLIB(s) are used to produce a list of PSB names that may be used as auditing criteria. You may enter up to five data sets, each separated by a semi-colon (;). You may enter an explicit data set name or provide a DSN mask, and click the Browse button to retrieve a list of matching data set names.

Auditing Levels

Allows for specific events to be omitted from the auditing process.

IMS Log Events: Events produced from the AUELxxxx address space.

SMF Events: Events produced from the AUEFxxxx address space.

Editing an IMS Entry

From the **IMSs** Tab, Select an IMS Entry name and click on the EDIT button to open the IMS Editor.

Note: There must be no active collections that reference the IMS entry you are editing.

IMS Entry Name

A required 8 byte field, which must be specified in EBCDIC characters. This is used to identify the IMS to the agent. The IMS Entry Name is set when the IMS definition is created and cannot be edited.

Description

This field is optional and can be edited. The description must not exceed 128 characters.

Agent The agent field cannot be edited.

RECONS

A list of RECON data set names is located in the selection column on the left of the IMS Editor panel. RECON data set names cannot be edited.

IMSPLEX

A five byte name used to specify the IMSPLEX name when DBRC RECON loss notification or DBRC parallel RECON access is in effect for the IMS being audited, and the DSPSCIX0 DBRC SCI Registration exit routine is not being used. If you are unsure of your sites or DBRC access requirements, please check with IMS systems programmer or other support personnel.

IMS Data Sets

A list of IMS data sets is located in the selection column on the left of the IMS Editor panel.

RESLIB: You may edit existing data set names, as well as add new data sets or delete existing data set names.

DBDLIB: You may edit existing data set names, as well as add new data sets or delete existing data set names.

PSBLIB: You may edit existing data set names, as well as add new data sets or delete existing data set names.

Auditing Levels

Allows for specific events to be omitted from the auditing process.

IMS Log Events: Events produced from the AUELxxxx address space.

SMF Events: Events produced from the AUEFxxxx address space.

Related concepts

"Collection profiles"
This section describes how collection profiles use DLI Calls, IMS Archive logs, and SMF data to determine the capture of audit events.

Deleting an IMS entry

Follow these steps to delete an IMS entry:

1. From the IMS tab, select an IMS entry name.

   Note: You may only delete an IMS entry while there are no collections active against it, and if no collections use the selected IMS as the collection source. See *Collection profile administration* for details.
2. Click **Delete.** The message "are you sure you want to delete the selected IMS entry" appears.
3. Click **Yes** to confirm the deletion, or **No** to cancel. Upon confirmation of the deletion, the IMS definition is deleted.

Collection profiles

This section describes how collection profiles use DLI Calls, IMS Archive logs, and SMF data to determine the capture of audit events.

Overview

Collection profiles are groups of IMS artifact types and security product-based user IDs, used to determine if events captured by IBM InfoSphere Guardium S-TAP for IMS are to be retained and sent to the Guardium appliance. These IMS artifacts include IMS databases, their segments, and PSBs. DLI call types (GET, UPDATE, REPLACE and DELETE) are also used to provide further filtering. IMS artifacts and user IDs can be specified using fully qualified names, or by using making characters. IMS artifacts and user IDs can be included or excluded in the collection profile.

Lists of IMS artifacts, USERIDS and DLI calls can be further separated into smaller groups in a collection profile. These groups are known as rules. You can specify one or more rules within a collection profile.

A collection profile and its rules are only in effect when activated. When activated, the collection profile is known as a collection. The activation of a collection profile causes the contents of the collection profile to be used to build a compiled filter. This compiled filter is an executable program, which uses algorithms to provide a highly efficient method of traversing the audit criteria of the collection, to determine if the event is to be audited and saved. This process is used when auditing DLI calls from IMS Online control regions and DLI/DBB batch jobs, data set access using SMF data, and other events found when reading IMS Archive Logs.

DLI Calls

- Compiled Filter is built and stored in E/CSA.
- Each active collection only has one copy of the compiled filter per LPAR.
- The compiled filter is active only while the collection is active.
- Individual DLI calls may be audited, others may be excluded.
- Segment data and concatenated key values may optionally be stored in the appliance.

- Before and after images of segment data resulting from REPLACE calls may optionally be stored in the appliance.
- As auditing DLI calls is the fundamental purpose of IBM InfoSphere Guardium S-TAP for IMS, this capability cannot be turned off or disabled.

IMS Archive Log

- Compiled filter is built and stored in private memory owned by the AUILssid task.
- Each AUILssid task monitors a separate IMS system and each maintains its own copy of the compiled filter.
- The compiled filter is built at AUILssid task cycle start, and is active for the duration of the cycle, regardless of any change in status of the collection.
- No events which are capable of being audited by the IMS Archive Log process contain segment name values. Therefore these values in the collection are ignored.
- If the IMS log record being examined does not contain one or more of the artifacts in the rule, that artifact is not used when making the audit decision. Only artifacts which exist in the IMS log record are used.

  Example:
  - IMS Online region START/STOP... No databases, segments, PSBs or user IDs are maintained in the IMS x'06' log record.
  - All IMS online region start/stop events are audited unless it was determined these events should not be audited at the agent or IMS definition levels.
- Auditing of IMS Archive Log events may be disabled at the agent level (all IMS systems monitored by the agent) by specifying `0` as the IMS-LOG-INTERVAL in the agent configuration file or by deselecting the **Audit All IMS Log events** box in the agent definition using the Administration user interface.
- Auditing of IMS archive Log events may also be disabled at the IMS level by de-selecting the **Audit All IMS Log events** box in the IMS definition using the Administration user interface. See the IMS administration: Editing an IMS Entry section in the Administration tasks of this UG.

SMF Data

- A single SMF task (AUIFssid) will audit all SMF activity for all IMS systems with an active collection controlled by the agent. A single pass of the SMF data is performed.
- The compiled filter is built at AUIFssid task cycle start, and is active for the duration of the cycle, regardless of any change in status of the collection.
- Segment and PSB names are not used as they do not exist in any SMF log data records.
- SMF events are data set based.
- Database names found in the collection are used to query DBRC to create a list of database data sets (DSGs, Overflows, AREAS and partitions) and any image copy data sets registered in DBRC for those database data sets.
- The RECON data set names of each audited IMS are also included in the list of data set names to be audited.
- The following IMS data sets are also retrieved from the RECON data sets and added to the list of data sets to be audited:
  - IMS Online Log data sets (OLDS)
  - IMS System Log data sets (SLDS)
  - IMS Recovery Log data sets (RLDS)

- Auditing of SMF events may be disabled at the agent level (all IMS systems monitored by the agent) by specifying `0` as the SMF-LOG-INTERVAL in the agent configuration file, or by deselecting the **Audit All SMF** events box in the agent definition using the Administration user interface.
- Auditing of SMF events may also be disabled at the IMS level by deselecting the **Audit All SMF** events box in the IMS definition using the Administration user interface.

CAUTION:
SMF event auditing uses data set rather than database names. Specifying mask values for database names, which result in the auditing of extraneous databases, can result in large lists of data sets.

A DEDB with 1024 areas will result in 1024 data set names, plus the image copy data sets for each of those AREAS, plus the data sets for any MADS data sets. This can result in 7168 data sets (plus image copies) being audited for one database.

Related concepts

"IMS Log customization" on page 53
This section describes IMS Log events and options for their modification.

"Editing an IMS Entry" on page 57
From the **IMSs** Tab, Select an IMS Entry name and click on the EDIT button to open the IMS Editor.

Related reference

Chapter 2, "Configuring InfoSphere Guardium S-TAP for IMS," on page 9
This section describes the steps required to configure InfoSphere Guardium S-TAP for IMS.

Collection profile administration

InfoSphere Guardium S-TAP for IMS collection profile administration allows you to create, delete, and modify collection profiles as well as activate and deactivate collections.

All functions described in this section are performed using the Administration user interface. The ID that is used to log into the Administration user interface requires Create Profiles permission to perform these functions.

- From the administration interface **Collection Profiles** tab, administrators can create new collection profiles, edit existing collection profiles, clone collection profiles, and delete collection profiles.
- For each collection profile, the **Collection Profiles** tab displays the name and description of the profile, and the number of active collections (the number of IMS systems to which the collection profile is applied).

Remember: Click **Refresh** from the **Collection Profiles** tab to update the data display prior to adding, editing, cloning, or deleting collection profiles. Clicking **Refresh** queries the server for updates to enable you to view the latest data.

Adding a collection profile

The **New Collection Profile Wizard** enables privileged users to add a collection profile to InfoSphere Guardium S-TAP for IMS.

Note: To add a new collection profile, you must be logged in to InfoSphere Guardium S-TAP for IMS and have the Create Profiles privilege.

Click **Add** to invoke the **New Collection Profile Wizard**, which allows you to specify:

- the required name of the profile (maximum 24 characters)
- an optional description (maximum 128 characters)
- the required IMS definition to be used as the source when listing databases, segments or PSB names

To add a new collection profile:

1. From the **Collection Profiles** tab, click **Add** to open the **New Collection Profile Wizard.** The first page of the **New Collection Profile Wizard** appears.

   Note: Use the **Back** and **Next** buttons to navigate through the New Collection Profile Wizard, or click on the various nodes at the left side of the panel to move through steps of the wizard.
2. Complete each step of the wizard as described in this guide. A summary overview is provided at the end of the wizard including the collection profile details, and the rule target filters applied to the collection profile.
3. Click **Finish** to add the new collection profile to InfoSphere Guardium S-TAP for IMS. The new collection profile, including its associated details, appears in the list of collection profiles in the **Collection Profile**s tab.

Once created, the collection profile can be applied to one or more IMS subsystems that are being monitored by InfoSphere Guardium S-TAP for IMS.

Specifying the profile name, description, and source (Profile Name):

When creating a collection profile, you must specify a unique name to identify the profile (specifying a description for the profile is optional).

To specify the name of the collection profile and an optional description:

1. In the **Profile Name** field, type a name to uniquely identify the collection profile (maximum of 24 characters).
2. In the **Description** field, type an optional description of the collection profile (maximum of 128 characters).
3. In the **Source** field, select a source IMS subsystem from the list provided. InfoSphere Guardium S-TAP for IMS can obtain the lists of objects (targets) to be audited for the collection profile using the source specified in this step.
4. Click **Next** to move to the next page in the Wizard.

The profile name you specify appears at the top of the folder hierarchy on the left side of the New Collection Profile Wizard, and a rule is automatically generated underneath it.

Defining a rule (Rule):

Rules determine what audit data is collected by InfoSphere Guardium S-TAP for IMS. Each InfoSphere Guardium S-TAP profile contains at least one rule. When you define a rule, you specify the targets to which the rule applies.

Entries in a collection profile are divided into rules. Each rule contains a related set of Databases, Segments, Events, PSBs and user IDs, which are used to determine if the events are to be audited. Multiple rules may be defined, and each is examined in the order of their appearance in the collection profile. The first rule encountered that returns a “true” condition is used to construct the audit event, which is then sent to the appliance. If no rule in the collection returns a “true” condition, the event is not audited.

1. The **Rule name** field is automatically populated in chronological order. Example: the first rule is named "Rule 1" and any additional rules you create will be named "Rule 2" and so on.
2. Click **Next** to move to the next step in the wizard to add Segments, Events, PSBs and USERIDs to the rule.

When creating a Collection profile, one rule is automatically added. If other rules are needed, they can be added by clicking the **New Rule** button on any screen where the button is present and not disabled.

Specifying audit targets for IMS databases and segments:

InfoSphere Guardium S-TAP for IMS enables you to specify IMS databases and segments as audit targets.

Databases and segments are the basis of each rule. A rule must contain at least one included database and segment entry in order to be eligible for activation as a collection. You may obtain a list of databases and segments from the RECON and DBDLIB data sets used when the IMS was defined by typing a complete database and segment name in the Target Filter data input field, or optionally a database and/or segment name containing a percent sign (%) or asterisk (*) as a wild-card character.

To add a database and segment from the returned list, highlight the desired database/segment pair within **Known Targets**, and click **Add**.

Database and segment pairs may also be excluded from processing, which is useful when a mask value has been specified, but specific databases and/or segments that meet that mask value should be excluded from auditing.

- Events from IMS DLI/DBB batch jobs and IMS Online Control regions use the database and segment values specified, to determine if an event is to be audited.
- SMF data and IMS Archive Log event auditing use the database values as these types of events are not sensitive to segments.

Including and excluding databases and segments:

From the Segments tab, you may retrieve a list of IMS databases and segments that are candidates for auditing for the IMS source you chose.

1. In the **Database** or **Segment** fields of the **Target Filter**, enter a fully qualified name or a mask value.
   a. In the **Target Filter**, **Database** and/or **Segment** field, type the filter. This is a text string followed by an option wildcard. A list of segments that match the filter and are registered in the RECON as associated with the source for the collection profile will be returned. For example,

      ```
      Databases=A*, Segments=B*
      ```

      returns a list of all IMS segments from the source IMS subsystem that begin with B and are present within databases that begin with A, and are registered in the RECON.
2. Click **Refresh** to refresh the **Known targets** list using the filter criteria. The retrieved databases and segments appear in the **Known Targets** area.

3. To include one or more database and segments from the **Known Targets** list in the rule, click the **Include** radio button, and click **Add**. The fully qualified database and segment appear in the **Included audited targets** list on the top right of the screen.
4. To exclude one or more database and segments from the **Known Targets** list in the rule, click the **Exclude** radio button, and click **Add**. The fully qualified database and segment appear in the **Excluded audited targets** list on the bottom right of the screen.

Mask characters supported when listing databases and segments include:

(%) The percentage sign represents a string of characters to a maximum length of 8 bytes.

For compatibility with some z/OS services, the asterisk **(*)** may be used in place of the percent sign.

(?) The question mark represents a single character value.

All other characters are treated as their value and are not considered masking characters.

Providing non-DBRC-registered database and segment names:

Fully qualified databases which are not registered in DBRC may be selected for auditing. Database and segments names may also be provided as mask values, allowing one database/segment entry to represent many databases and segments.

You may also include, or exclude databases and segments by providing a database and/or segment name containing a mask character, instead of specifying each database and segment individually. For example, a database value of `A` and a segment value of `%` would cause auditing of all segments within database `A`.

1. From the **Segments** tab, enter the database and segment name or mask value in the **Other Targets** data entry field at the bottom of the screen.
2. Set the **Include** or **Exclude** radio button to the desired value.
3. Click **Add Other**. The specified value appears in the appropriate audited targets list on the right of the screen.

Note: The only mask character supported when providing databases and segments in the **Other Targets** area is the percent sign **(%)**, which represents a string of characters to a maximum length of 8 bytes. All other characters are treated as their value and are not considered masking characters.

Specifying audit targets for events:

After Specifying audit targets for IMS segments, you must inform InfoSphere Guardium S-TAP for IMS which DL/I calls are to be audited, and whether retaining segment information with Insert and Replace calls is desired.

Note: This section only pertains to IMS DLI calls from DLI/DBB batch jobs and IMS Online Control regions. SMF and IMS Archive Log-generated events use agent and IMS specific criteria to determine which types of events are to be audited.

Note: Only Successful DLI calls are audited. DLI calls resulting in non-blank DLI status codes indicating a possible error are not audited.

- To specify that you desire all supported DL/I call types to be audited, and you wish to include the segment data used during insert and replace calls, select the **All Events** box in the row that includes the database and segment name. Selecting this box will automatically populate the remainder of the boxes for that row. Alternatively, you may click on the box representing the DLI call individually and action individually.
- To specify individual DLI calls, select each DL/I call type box in the row associated with the database and segment.
- To specify that the segment data used for Replace and Insert calls be retained by InfoSphere Guardium S-TAP for IMS, select the Capture Data box in the row associated with the database and segment.
- To deselect any checked boxes associated with a database and segment, you should click on any previously selected DL/I call or Capture Data box to the check mark and de-select the call or feature.

  Note: If you do not select any boxes for a database and segment, and the database was not specified as an IMS database target, no auditing will occur for the database or segment.

DLI calls can be audited include INSERT (ISRT), UPDATE (REPL), DELETE, (DLET) and GET (all forms of GET... GN, GHU, GNP, etc). You can optionally request that the segment concatenated key and segment data be captured and set to the appliance (capture data). You can also request that when a replace call is done, the segment data used as input to the REPLACE call (as well as the segment data returned from the GET HOLD call used to obtain positioning in the database) be sent to the appliance and linked for easy viewing as the Before Image.

Table 3. DLI Call/Action commands

Box	**DLI CALL/ACTION**
Insert	ISRT
Update	REPL
Delete	DLET
Read	GN, GU, GNP, etc.
Capture Data	Obtain concatenated key and segment data
Before Image	Obtain concatenated key and segment data and link Get Hold and Replace calls.

Configuring PSB filtering:

InfoSphere Guardium S-TAP for IMS enables you to specify PSBs as filters. From the PSB tab, you may retrieve a list of PSBs that are to be used as secondary criteria.

Specifying one or more PSBs for inclusion within a rule is optional. A list of PSBs associated with an IMS may be obtained from the PSBLIB data sets specified when defining the IMS system to the product. You can supply a fully qualified name or a mask value.

PSBs can also be specified for exclusion, which is useful when a mask value has been specified for inclusion, but specific PSBs that meet the mask value should be excluded from auditing.

The list of PSBs, if provided, is logically “ANDed” to the databases and segments specified in the rule.

- If the event meets at least one of the database/segment INCLUDE criterion, and meets any PSB INCLUDE criterion, the event is audited.
- If the event meets a database/segment INCLUDE criterion, and is found to match a PSB EXCLUDE criterion, the event is not audited.

1. To filter the **PSBs** list:
   a. In the **Target Filter**, **PSB** field, type the filter. This is a text string followed by an option wildcard. A list of PSBs that match the filter and are registered in the RECON as associated with the source for the collection profile returns. For example, **A*** returns a list of all PSBs from the source IMS subsystem that begin with A and are registered in the RECON.
   b. Click **Refresh** to refresh the **Known PSBs** list using the filter criteria. The name is shown for each object that matches the criteria you specified.
2. To add selected items to the **Included PSBs** list:
   a. In the **PSBs** list, click the PSBs you want to add to the **Included PSBs** list.
   b. Click **Add** to add the PSBs.
3. To add other (additional PSBs) in the Other PSBs area:
   a. In the **Other PSB** field, type the PSB name.
   b. To add the PSBs to the **Included PSBs** list, click **Add Other**.
4. Click **Next** to move to the next step in the wizard.
5. If needed, you can remove items from the **Included PSBs** list by clicking the PSBs, or PSB, you want to remove from the **Included PSBs** list and then clicking **Remove**. (To remove all PSBs from the list, click Remove All.)

Configuring USERID filtering:

InfoSphere Guardium S-TAP for IMS enables you to specify user IDs as filters.

Specifying one or more user IDs for inclusion within a rule is optional. You can provide a fully qualified user ID or a mask value to specify one or more user IDs. User IDs can also be specified for exclusion, which is useful when a mask value has been specified for inclusion, but specific user IDs that meet the mask value should be excluded from auditing.

The list of USERIDs, if provided, is logically “ANDed” to the databases and segments (and PSBs if applicable) specified in the rule. If the event meets at least one of the database/segment/PSB INCLUDE criterion, and meets any USERID INCLUDE criterion, the event will be audited.

1. To filter the **USERIDs** list:
   a. In the **USERIDs** field, type the user ID.
2. To add selected items to the **Included USERIDs** list:
   a. Click the **Include** radio button.
   b. Click **Add**.
3. To add selected items to the **Excluded USERIDs** list:
   a. Click the **Exclude** radio button.
   b. Click **Add**.
4. Click **Next** to move to the next step in the wizard.

5. If needed, you can remove items from the **Included USERIDs** or **Excluded USERIDs** list by clicking the user ID(s) you want to remove from the list, then clicking **Remove**. (To remove all user IDs from the list, click **Remove All**.)

Collection profile summary (Summary):

The last step of the **New Collection Profile Wizard** is the Summary. The Summary shows the entire profile you have created, including Databases/Segments, Events to be audited, PSBs and USERIDs specified for each rule in the Collection Profile.

When you have completed the collection profile, click **Finish**. The newly created collection profile appears in the list on the **Collection Profiles** tab.

Editing a collection profile

You can edit an existing collection profile by modifying the source profile description, or targets (databases, segments, events, PSBs, and USERIDs).

Important: To modify a collection profile you must have the Create Profile or Edit Profile privilege.

Note: You cannot edit a collection profile that has an active collection.

To edit a collection profile:

1. From the **Collection Profiles** tab, click the collection profile you want to edit.
2. Click **Edit**. The first page of the Collection Profile Editor appears.
3. Complete each applicable step. Click on a step from the hierarchy at the left of the panel to display the corresponding page of the editor.
4. Click **OK** to save your changes or **Cancel** to exit without saving.

Cloning a collection profile

Cloning a collection profile creates a copy of a selected (existing) collection profile, the collection profile's rule, and its associated targets. Cloning also enables you to modify the collection profile's information.

Important: You must have create profile privileges to clone a collection profile.

To clone a collection profile:

1. From the **Collection Profile** tab, click the collection profile you want to clone and click **Clone**. The first panel **Collection Profile Editor** appears. The name of the collection profile with each applicable step appears at the left side of the window.
2. To modify the profile name or description:
   a. In the **Profile Name** field, type a new name for the profile.
   b. In the **Description** field, type a new description for the profile.
   c. In the **Source** field, select a source IMS subsystem from the list provided. InfoSphere Guardium S-TAP for IMS can obtain the lists of objects (targets) to be audited for the collection profile using the source specified in this step.
3. To modify the IMS databases or segments, click the **Segments** node in the tree view and then add or remove databases or segments from the Audited targets list.
4. To modify the events, click the **Events** node in the tree view and then select or unselect individual events for specific IMS segments.

5. To modify the PSBs, click the **PSBs** node in the tree view and then add or remove PSBs from the Included or Excluded PSBs list.
6. To modify the user IDs, click the **USERIDs** node in the tree view and then add or remove USERIDs from the Included USERIDs list.
7. Click **OK** to save your modifications or click **Cancel** (modifications are not saved).

Deleting a collection profile

To delete a collection profile, the collection profile must not be part of an active collection. To activate or deactivate a collection, see the Collection administration section of this User's Guide.

1. From the **Collection Profile** tab, select the collection profile you want to delete by clicking the row containing the name of the target collection profile.
2. Click **Delete** at the bottom of the screen to delete the collection profile. The message **Are you sure you want to delete the selected collection profile?** appears.
3. Click **OK** to delete or **Cancel** to exit without deleting.

Collection administration

InfoSphere Guardium S-TAP for IMS collection administration allows you to create, activate, and deactivate collections.

A collection associates a specific collection profile with a specific IMS subsystem. From the administration interface **Collections** tab, administrators can activate and deactivate collections.

For each collection, the **Collections** tab displays the name of the collection profile, the IMS subsystem to which the collection profile is applied, and the date and timestamp since it was first applied.

Remember: Click **Refresh** from the **Collections** tab to update the data display before activating and deactivating a collection. Clicking **Refresh** queries the server for updates to enable you to view the latest list of active collections.

Clicking **Refresh** displays the Collection profile name, the IMS definition that the collection profile applies to, and the date and time that the collection was activated.

Note: The date and time is shown as a UTC/GMT date/time.

Activating a collection

Use the **Collection Editor** to activate a collection.

Activating a collection associates a collection profile with an IMS definition and causes the compiled filter to be built and used by IMS instances where at least one RECON data set name used by the IMS instance matches at least one RECON data set name used in the IMS definition.

Collection profiles defined using one agent can be activated on IMS definitions associated with any other agent.

- One collection profile may be associated with any number of IMS definitions at the same time. An IMS definition can only have one collection active at a time.

- Only one collection may be activated per request.

To be eligible for activation, each rule in the collection profile must have at least one database and segment entry with an event or DLI call type selected.

Note: You must have the Create Profiles privilege to create a collection.

To add a collection:

1. From the **Collections** tab, click **Activate**. The **Collection Editor** appears.
2. In the **Profile Name** field, select the existing collection profile you want to activate. The drop-down menu provides a list of Collection profiles that can be activated.
3. In the **Applies to** field, select the IMS system to which the selected collection profile is to be applied The drop-down menu provides a list of IMS definitions.
4. Click **OK** to activate the profile, or click **Cancel** to exit without activating the profile.

   Note: Only one collection can activate per IMS system.

Deactivating a collection

Use the **Collection Editor** to deactivate a collection.

Note: To modify the collection profile or IMS subsystem of a collection, it needs to be deactivated.

Important: You must have the Edit Profiles privilege to modify a collection.

To deactivate a collection:

1. From the **Collections** tab, select the collection you want to deactivate.
2. Click **Deactivate**. The collection is deactivated. The collection row is removed from the Collections panel.

Saving data to a file

Use the **File** > **Save As** menu option to save data, such as users, groups, IMS subsystems, and collection profiles, to an external file on your local machine.

To save data to a file:

1. Click the appropriate tab within the administration interface, from which you want to export the InfoSphere Guardium S-TAP for IMS object.
2. Select the data you want to save to a file.
3. Click **File** > **Save As**. The **Save** window appears.
4. Browse to the location where you want to save the file.
5. In the **File name** field, type a name for the file.
6. Click **Save** to save the file. The file is saved to the specified location in XML format. If you do not wish to save the file, click **Cancel** to cancel the operation.

   Note: For security reasons, the user password will not be included in the saved XML file.

Opening a data file

Use the **File** > **Open** menu option to open a previously saved data file.

To open a file:

1. Click the appropriate tab within the administration interface, where you want to import the InfoSphere Guardium S-TAP for IMS object.
2. Click **File** > **Open**. The **Open** window appears.
3. Browse to the location where the file is located.
4. Select the file you want to open.
5. Click **Open** to load the desired object within the InfoSphere Guardium S-TAP for IMS administration user interface.

   Note: For security reasons, the user password will not be included in the saved XML file. If the user is added back to the repository through the XML file, message AUIS2002E will occur upon login. The administrator will need to reset the password to allow the user to login, and the user password will need to be reset upon login.

Chapter 5. Reference information

This section provides IBM InfoSphere Guardium S-TAP for IMS on z/OS reference information.

IMS Logtypes and SMF record types collected by InfoSphere Guardium S-TAP

The two tables in this section show the IMS logtypes collected by InfoSphere Guardium S-TAP.

Table 4. IMS Logtypes collected by InfoSphere Guardium S-TAP

Logtype 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 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 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.
5923	DEDB ADS STATUS Log record	DEDB area data set status was changed.

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

Table 5. 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

Table 5. SMF record types and descriptions (continued)

SMF Record Number	TYPE
89	Usage Data

Important: InfoSphere Guardium S-TAP can only report events that are being collected by SMF. If any SMF record type in the above table is not being collected at your site, InfoSphere Guardium S-TAP cannot report that event.

Related reference

"SMF customization" on page 31
For SMF customization, SMF events, SMF spill data sets, and SMF masks, as well as the IMS log and log stream must be customized. Detailed information on how to customize these areas is available in this User's Guide.

Host and port reference worksheet

Use the following worksheet to help you properly configure InfoSphere Guardium S-TAP.

Table 6. Host and port reference worksheet

Purpose	Obtain Host Info From	Hosts	Obtain Port Info From	Ports	Configure
Server listens for clients			(Default)		1. The server configuration file <client-listener-port> configuration element 2. Server definitions for Administration UI
Server listens for agents	(Same as above)		(Default)		The server configuration file <agent-listener-port> configuration element
Agent calls server	(Same as above)		Must match the server configuration file <agent-listener-port> configuration element		The agent configuration file <server-port> configuration element

Administration interface shortcut keys

The following table shows the shortcut keys available within the InfoSphere Guardium S-TAP administration interface.

Table 7. Administration interface shortcut keys

Menu, menu command, or option	Keyboard shortcut
Add	Alt-A
Clone	Alt-L
Delete	Alt-D
Edit	Alt-E

Table 7. Administration interface shortcut keys (continued)

Menu, menu command, or option	Keyboard shortcut
Edit —> Copy	Ctrl-C
Edit —> Cut	Ctrl-X
Edit —> Paste	Ctrl-V
Edit menu	Alt-T
File —> Open	Ctrl-O
File —> Save As	Ctrl-S
File menu	Alt-F
Help —> Help Topics	F1
Help menu	Alt-H
Refresh	Alt-R
Settings > Define Servers	Ctrl-D
Settings menu	Alt-S

Administration client log files

The administration client writes logs to two locations.

Console log

The console log contains a list of events that are processed to provide an overview of events.

Log file (AuditExpertAdm.log)

The log file is a detailed log of these events and includes all of the messages passed back and forth from the client and server. This log is named *AuditExpertAdm.log*, and is located in the directory where the administration client is installed. The default location is: `C:\Program Files\IBM\IMS\DB2TOOLS\InfoSphereGuardiumSTAPforZv8.2\admin`

Restarting the agent after invalid SMF mask shutdown

If the InfoSphere Guardium S-TAP agent has been started for the first time (no previous collections) with an invalid SMF mask specified, the agent will shut down upon collection activation.

If the SMF mask entry is invalid, message AUIA304W appears. In the case that this failure occurs the first time the agent has been started, follow these steps to successfully restart the agent.

1. With only the InfoSphere Guardium S-TAP server started, log into the InfoSphere Guardium S-TAP administration user interface and the related collection, setting it to INACTIVE.

   Note: This does not require the agent job to be running.
2. Restart the InfoSphere Guardium S-TAP agent. The collection will not automatically activate.

3. In the administration user interface, go to the **Agents** tab and edit the SMF mask information to make it valid. (Correct misspelling, incorrect SMF data set name, etc.)
4. Re-activate the collection for the related collection profile. With a valid mask, the agent can begin collecting the SMF information.

Chapter 6. Troubleshooting

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

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

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

Error messages

All messages have a severity code printed as the last character of the message ID. The severity codes are described in this table:

Table 8. Error message severity codes

Severity Code	Description
I	Information message. No user action required.
F	Detailed information message: No user action required.
W	Warning message. Results may not be as expected.
E	Error message. Some may be user-correctable, read the User Response to determine the course of action.
S	Severe message: User action required.

Error messages and codes: AUIAxxxx

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

AUIA002I Terminating collector thread <id>.

Explanation: The thread collector with the specified *<id>* is terminating.

User response: None required.

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

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 up. In most cases, this may occur if an address space with that name is already online, or if there was a JCL error or there was an issue resolving the loopback address host name. If further assistance is required, contact IBM support.

AUIA004E Address Space <name> failed to stop successfully within the timeout period and was abandoned.

Explanation: The named address space did not stop within the time out period and was therefore abandoned by the master address space.

User response: Check the named address space logs to identify why it did not terminate. If further assistance is needed, contact IBM technical support.

AUIA005I Starting address Space <name>.

Explanation: The agent has automatically started the support address named.

User response: This is an informational message only.

AUIA006I Address Space <name> started successfully.

Explanation: The agent has successfully started the support address space named.

User response: None required.

AUIA007I Stopping address Space <name>.

Explanation: The agent has automatically stopped the support address space named.

User response: None required.

AUIA008I Address Space <*name*> stopped successfully.

Explanation: The named address space has successfully stopped.

User response: None required.

AUIA009E The address space <*name*> is not active.

Explanation: The named 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 may occur 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, please contact IBM support.

AUIA011W The database list was truncated because of potential storage shortage.

Explanation: An attempt to retrieve a list of databases failed because of memory shortage.

User response: Modify your filter to shorten the list of returned databases or increase the REGION size of the agent address space (AUIAxxxx).

AUIA012W The database and segment lists were truncated because of potential storage shortage.

Explanation: An attempt to retrieve a list of databases failed because of memory shortage.

User response: Modify your filter to shorten the list of returned databases or increase the REGION size of the agent address space (AUIAxxxx).

AUIA013W Reusing agent record for agent with name *'agent-name'*. Ignored active status.

Explanation: The repository already contained a record for agent with name agent-name and the agent is reusing the old record after verifying that another agent with the same name is not already online. This error is usually indicative of a failure of the previous agent during shutdown.

User response: Check the previous agent's logs for any errors.

AUIA014E An active record for the agent *'agent-name'* already exists in the repository.

Explanation: This error message occurs if you respond `N` to message AUIA100I. Replying `N` causes the agent to terminate and allows you the opportunity to investigate the root cause behind the incorrect status in the repository agent record. Usually, an incorrect status would mean that the previous agent did not shut down properly. Checking the previous agent's logs may help identify the root cause.

User response: For the agent to reuse the agent record in the repository, reply `Y` to message AUIA100I, and proceed.

AUIA015E IMS entry not found.

Explanation: The IMS entry cannot be located.

User response: Please provide a valid IMS entry and retry. You may need to refresh the administration user interface panel before continuing.

AUIA016E Specified Log Stream <*name*> does not exist.

Explanation: The Log Stream with the name specified during agent configuration does not exist.

User response: Verify that specified Log Stream exists. If it exists and this message occurs, please contact IBM support.

AUIA017E Specified Spill Dataset <*name*> does not exist.

Explanation: The Spill Dataset with the name specified during SMF Event collector configuration does not exist.

User response: Verify that specified Spill Dataset exists. If it exists and this message occurs, please contact IBM support.

AUIA018E Problem encountered for *<spill>*, *<problem area>*: **required** *<req>*, **received** *<res>*.

Explanation: This spill dataset *<spill>* could not be validated. The *<problem area>* with the parameters *<req>* and <res> gives additional details.

User response: Please fix the issue in the <problem area> using the required <req> value. Please contact IBM support for additional help.

AUIA019E z/OS call failure for *<spill>*, *<problem area>*: **RC=***<rc>*, **RSN=***<rsn>*.

Explanation: Attempt to validate the spill dataset caused an error with the z/OS services. A *<problem area>* with return *<rc>* and reason *<rsn>* codes are returned.

User response: Please contact IBM support.

AUIA020E IMS definition for *ims-name* **cannot be deleted because it is being used as a source for collection profile** *collection profile name*.

Explanation: An IMS definition can only be deleted if it is not being used to define a collection profile.

User response: Delete the associated collection profile before deleting the IMS definition.

AUIA021I MODIFY command *<command text>* **sent to Address Space** *<name>*.

Explanation: The MODIFY command *<command text>* sent to address space named.

User response: None 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, please 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: Named collector is disabled because of proc name for the collector address space has not been specified in the configuration.

User response: To enable this collector, please specify the proc name for collector address space. If the proc name is specified and the message occurs, please contact IBM support.

AUIA024I *<Collector name>* **collector is disabled: not configured.**

Explanation: Named collector is disabled because it has not been configured.

User response: To enable this collector, please configure it within the Administration user interface. If the specified collector is configured and the message occurs, please contact IBM support.

AUIA025E The agent *<name>* **for** *<host>* **has not been configured.**

Explanation: The agent *<name>* for system *<host>* has not been configured properly.

User response: This may occur during adding new IMS definition if the agent has not been configured before. Verify that the agent is configured. If the agent has been configured properly and the message occurs, please contact IBM support.

AUIA026E Problem encountered while validating *<log stream>*. **Function:***<func>*, **request:***<req>*, **RC=***<rc>*, **RSN=***<rsn>*.

Explanation: The Log Stream *<log stream>* could not be validated. A problem function *<func>* and request *<req>* with return *<rc>* and reason *<rsn>* codes are returned.

User response: This may occur during IMS Batch collector configuring if there are any problems with the Log Stream. If the Log Stream is correct and the message occurs, please contact IBM 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: Please contact IBM support.

AUIA028S An agent with the name *agent-name* **is already online.**

Explanation: An agent is already online and is using the name agent-name. The agent-name must be unique per sysplex.

User response: Please change the *agent-name* and restart the agent (or shutdown the other agent).

AUIA100I Reuse existing record for agent '*agent-name***'? Reply Y or N.**

Explanation: The repository record pertaining to the agent with name *agent-name* indicates that the agent is already online, although sysplex checks indicate that the agent is not online. Usually, an incorrect status would mean that the previous agent did not shut down properly. Checking the previous agent's logs may help identify the root cause.

User response: Reply `Y` if you want the agent to reuse the agent record in the repository and proceed. Reply `N` for the agent to terminate, which enables you to investigate the root cause behind the incorrect status in the repository agent record.

Error messages and codes: AUIBxxxx

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

AUIB300I CONNECTION TO z/OS SYSTEM *log_stream_type* **WAS SUCCESSFUL - LOG STREAM NAME:** *log_stream_name*

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: None required.

AUIB302I Drain request for *type* **logstream has completed. Logstream:** *name***.**

Explanation: A DRAIN request, which reads all data from the z/OS log stream, has completed.

System action: The AUIBssid tasks prepares to terminate.

User response: None 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 task (AUIBxxxx) will start the termination phase.

User response: None required.

Error messages and codes: AUICxxxx

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

AUIC3001E The group name is already in use.

Explanation: While editing or creating a group, a group name was specified that matches the name for an existing group.

User response: Please specify a unique group name.

AUIC3002E Please enter a group name.

Explanation: While editing or creating a group, no group name was specified.

User response: Please specify a unique group name.

AUIC3003E The name must not begin or end with a space.

Explanation: The username you have entered is invalid because it contains spaces.

User response: Provide a username that conforms to the rules documented in Chapter 4. of this User's Guide, in Administrative tasks, section: Specifying the user name and password.

AUIC3005E The IMS entry name is already in use.

Explanation: The specified IMS entry name needs to be unique.

User response: Specify a unique IMS entry name and repeat the operation.

AUIC3006E Please enter an IMS entry name.

Explanation: You must enter a valid IMS entry name in order to proceed in the New IMS Wizard.

User response: Enter an IMS entry name and try again.

AUIC3007E You must select a collection.

Explanation: Before you can edit a collection, you must first specify the collection you want to edit.

User response: Please select the collection you want to edit and try again.

AUIC3008E Please specify a source.

Explanation: The source for the selected Collection Profile is undefined. This may occur when the agent for the IMS definition which served as the source is no longer available.

User response: Select a source for the specified collection profile. Source(s) will be available only when the agent is properly configured and running, and when at least one IMS definition is defined.

AUIC3009W There are too many targets to load. Only the first 512 targets will be displayed. Please enter more restrictive values in the target filter, then click Refresh.

Explanation: The list of entries returned for the entered filter exceed the maximum threshold of 512 that is allowed to be displayed by the InfoSphere Guardium S-TAP client.

User response: Please enter a more refined filter value before clicking **Refresh** to limit the size of the returned list below the maximum threshold.

AUIC3010E You must select a user.

Explanation: A user must be selected before being edited.

User response: Please select a user and try again.

AUIC3011E You must select a group.

Explanation: Before you can edit a group, you must first select the group you want to edit.

User response: Please select the group you want to edit and try again.

AUIC3023E Authentication failed for an unknown reason.

User response: Check that the InfoSphere Guardium S-TAP for IMS on z/OS server is configured and operating properly. If the problem still exists, please contact your IBM support representative for further assistance.

AUIC3026E You must select a server from the Settings menu. If there is no entry for the server you wish to connect to, select Define Servers... from the Settings menu to create one.

Explanation: No InfoSphere Guardium S-TAP server is currently selected in the Settings menu.

User response: Select an existing server from the Settings menu, or define a new server using the **Define Servers...** option, then select the new server.

AUIC3027E No such host *host*.

Explanation: The administration client is unable to contact the specified host.

User response: Check that the server host for the selected server exists, and that it is running and responsive.

AUIC3028E Can not connect to {0} on port {1}. Check the host and port values in the settings menu. Check that the InfoSphere Guardium S-TAP on IMS for z/OS server is up and running. Check your computer's network connection. Check for a firewall blocking your connection to the server host.

Explanation: Unable to establish a connection to server {0} on port {1}.

User response: Ensure that the host and port values are correct, that the InfoSphere Guardium S-TAP on IMS for z/OS server has been started up and is responsive, and that the administration client is able to contact the InfoSphere Guardium S-TAP on IMS for z/OS server.

AUIC3029E Can not login for an unknown reason.

Explanation: The login failed due to an unknown reason.

User response: Please contact your IBM support representative for further assistance.

AUIC3030E Unexpected error from the server: [Error Message]

Explanation: This error could occur if the encryption key exchange and/or encryption encounter an issue.

User response: Restart the server/agent for an immediate workaround and contact IBM tech support for further analysis.

AUIC3031E No response from *server* within timeout period.

Explanation: No response has been received from the specified server within a reasonable period of time.

User response: Ensure that the connection to the InfoSphere Guardium S-TAP on IMS for z/OS server was not inadvertently dropped, and that the server is running and responsive. Then reconnect to the server and retry the same operation.

AUIC3032I This profile can not be modified. An active collection profile can not be modified. To modify this profile, delete or deactivate any collections associated with this profile.

Explanation: The profile you have attempted to modify is currently active.

User response: Delete or deactivate any collections associated with the profile you want to modify, then try again.

AUIC3033E Can not delete an active collection profile. Please delete or deactivate any collections associated with this profile.

Explanation: Collection profiles that are currently active can not be deleted. It is necessary to delete or deactivate collections associate with the profile you want to delete before you can delete it.

User response: Please delete or deactivate any collections associated with this profile and try again.

AUIC3034E Save of source failed with: [ERROR_MSG]

Explanation: The selected Source within the Collection Profile could not be saved.

User response: Please resolve the condition specified within the error message then retry the operation. If this fails, please contact your IBM customer support representative.

AUIC3037E You must select a profile.

Explanation: Before you can edit a collection profile, you must first specify the profile you want to edit.

User response: Please select the profile you want to edit and try again.

AUIC3038E The profile must have a name.

Explanation: To create a new collection profile, a name for the profile must be specified.

User response: Specify a name for the profile, then continue.

AUIC3039E The rule must have a name.

Explanation: The current rule name field appears to be empty.

User response: Please specify a valid rule name, not to exceed 128 characters.

AUIC3041E The name must not begin or end with a space.

Explanation: There is a space before or after the rule name.

User response: Delete any spaces before or after the rule name and retry.

AUIC3042E The name is already in use.

Explanation: The current entry name already exists.

User response: Please type in a unique entry name.

AUIC3047E Please select a user.

Explanation: An attempt was made to save a user to a file; however, no user was selected.

User response: Select a user and try again.

AUIC3048E User must have a name

Explanation: The user entry you are trying to import does not have a name associated with it.

User response: Please verify that the user entry you are trying to import has a valid name.

AUIC3049E Please select a group.

Explanation: An attempt was made to save a group to a file; however, no group was selected.

User response: Please specify a group and try again.

AUIC3050E Group must have a name.

Explanation: The group entry you are trying to import does not have a name associated with it.

User response: Please verify that the group entry you are trying to import has a valid name.

AUIC3051E You must select an authorization.

Explanation: You must first select an authorization before the authorization can be edited.

User response: Select the authorization you wish to edit and try again.

AUIC3052E Not a valid authorization. Be sure to select a user, a status, and a database.

Explanation: You must select a user, status, and database in order to add an authorization.

User response: Select a user, status, and database and try again.

AUIC3055E You must select an agent.

Explanation: An attempt was made to edit an agent; however, no agent was selected.

User response: Select an agent and try again.

AUIC3056E Updating the agent failed with: *{0}*

Explanation: The agent configuration could not be successfully updated.

User response: Correct the condition specified in the error message and try updating the agent configuration again.

AUIC3057E The password must contain at least 6 characters.

Explanation: To add a new user, you must specify a password that is at least 6 characters in length.

User response: Please specify a valid password for the new user and try again.

AUIC3058E The password *password* **is too similar to the username** *username***.**

Explanation: An error occurred while authenticating the specified user.

User response: Specify a password that is different from that of the specified username.

AUIC3060E Please enter a user name.

Explanation: A user name must be specified in order to add a new user.

User response: Please specify a name for the new user and try again.

AUIC3061E The user name is already in use.

Explanation: A user name was supplied that is already assigned to another user.

User response: Please specify a unique user name.

AUIC3062E Please enter an expiration value.

Explanation: The **Expires in** field is empty.

User response: Please enter a valid expiration value in the **Expires in** field before reattempting this operation.

AUIC3064E A description must be specified.

Explanation: The description field must be specified in the server definition.

User response: Please specify the description and then try to add/edit the server definition.

AUIC3065E A server host must be specified.

Explanation: The server name field must be specified in the server definition.

User response: Please specify the server name and then try to add/edit the server definition.

AUIC3066E A server port must be specified.

Explanation: The server port field must be specified in the server definition.

User response: Please specify a server port and then try to add/edit the server definition.

AUIC3067E The server port must be an integer in range from 1 to 65535.

Explanation: The server port specified is invalid.

System action: The system waits for the specification of a valid server port.

User response: Specify a valid server port integer between 1 and 65535.

AUIC3068E You must select a server first before editing it.

Explanation: A server was not selected.

User response: Select the server you want to edit, then click **Edit**.

AUIC3070E

Explanation:

User response:

AUIC3071E The password must contain a mixture of numbers, letters, and punctuation.

Explanation: For security purposes, InfoSphere Guardium S-TAP requires passwords to contain a mixture of numbers (without respect to case) and letters. Punctuation is also acceptable for use in passwords.

User response: Please enter a password that contains a combination of characters that meet the requirement and try again.

AUIC3073E Creation of the IMS failed for an unknown reason. Check the client and server logs for additional details.

Explanation: The IMS could not be created.

User response: Check the client and server logs to determine the cause of the failure.

AUIC3074E Update of the IMS failed for an unknown reason. Check the client and server logs for additional details.

Explanation: The IMS could not be updated.

User response: Check the client and server logs to determine the cause of the failure.

AUIC3075E Unable to delete the current user.

Explanation: The InfoSphere Guardium S-TAP user name you have attempted to delete is the user name you are currently logged in as.

User response: Have another user with the Create Users permission delete this user, or logout and login again as a different user with the Create Users permission to delete this user.

AUIC3076E Timed out waiting to create session on the InfoSphere Guardium S-TAP for IMS on z/OS server.

Explanation: An excess of time has elapsed.

User response: Please retry.

AUIC3077E Timed out waiting for authentication from the InfoSphere Guardium S-TAP for IMS on z/OS server.

Explanation: No authentication response was received from the InfoSphere Guardium S-TAP for IMS on z/OS server within the timeout period.

User response: Ensure that the connection to the InfoSphere Guardium S-TAP on IMS for z/OS server is running and responsive. Then try and re-authenticate with the server.

AUIC3079E The data set names must be unique.

Explanation: The RECONS are invalid because the data set names must be unique.

User response: Specify a unique data set name and retry.

AUIC3087E One or more unresolved wild-card strings have been encountered at the RECONS panel. Please resolve them before completing the IMS creation.

Explanation: The data set names in the RECONS panel should not contain unresolved wild-card filter masks.

User response: Please resolve any data sets in the RECONS panel containing wild-card characters by expanding the drop-down list and selecting one of the choices presented or by typing in the full data set name without wild-card characters.

AUIC3080E Empty data set name in the RECONS panel. Data set name fields should not be empty.

Explanation: One or more RECON data set name fields in the RECONS panel are empty.

User response: Please ensure that all the RECON data set fields are filled out.

AUIC3082E Entered DSN mask contains illegal characters.

Explanation: The DSN mask contains one or more non-permitted characters. Permitted characters include regular letters, numbers, asterisk key (*), or percentage key (%).

User response: Specify a DSN mask that contains the permitted character classes.

AUIC3083E The User name must contain at least 2 characters.

Explanation: The minimum length of a username is 2 characters.

User response: Provide a username that conforms to the rules documented in Chapter 4. of this User's Guide, in Administrative tasks, section: Specifying the user name and password.

AUIC3085E There is already a collection for this location and profile.

Explanation: The collection cannot be updated because a collection has already been set for this location and profile.

User response: Specify a new location and profile for the collection, or cancel to use the existing collection settings.

AUIC3089W Your password is set to expire in {0} days. Please remember to change your password before it expires in order to avoid any disruptions in using the client, where {0} is the number of days before the password expires.

Explanation: Your InfoSphere Guardium S-TAP password will expire at midnight (InfoSphere Guardium S-TAP server time) following the number of days specified.

User response: Please change your InfoSphere Guardium S-TAP password to avoid any future login disruptions.

AUIC3090W This collection profile does not contain any items to audit. Do you still want to continue?

Explanation: This collection profile does not have any rules that cause data to be audited.

User response: Click **Yes** to continue creation of this so-called empty collection profile. Click **No** to cancel its creation.

AUIC3091E You must select a server first before pinging it.

Explanation: No server has been selected.

User response: Select a server, then click **Ping**.

AUIC3092E You must select a server first before deleting it.

Explanation: You have not selected an InfoSphere Guardium S-TAP server definition to delete.

User response: Select the InfoSphere Guardium S-TAP server definition you want to delete, then click **Delete**.

AUIC3098E Invalid data set {0}: The number of characters in each segment must be between 1 and 8 characters.

Explanation: The specified data set name has one or more segments that are not between 1 and 8 characters.

User response: Please specify a data set where each segment contains more than 0 characters and less than 8 characters.

AUIC3099E A maximum of 5 data sets may be entered for each control library field.

Explanation: More than 5 data sets have been entered for one or more control library fields.

User response: Please limit the number of data sets to a maximum of 5 per control library field.

AUIC3100E Invalid data set {0}: The number of segments must not exceed 22.

Explanation: The specified data set name contains more than 22 segments.

User response: Please specify a data set name that contains 22 segments or less.

AUIC3101W {0} is not valid data set. It will be omitted.

Explanation: The data set entered is invalid and will not be accepted.

User response: Please enter a valid data set.

AUIC3102E Empty data set name in the Control Blocks panel. Data set name fields should not be empty.

Explanation: One or more control library data set name fields in the Control Blocks panel are empty.

User response: Please ensure that all the control library data set fields are filled out.

AUIC3105E At least one SMF mask field needs to be specified.

Explanation: The SMF masks fields appear to all be empty.

User response: Please make sure that one or more SMF masks have been populated.

AUIC3107E The server port must be a value ranging from 1 to 65535

Explanation: The server port value specified is not within the accepted range of values.

User response: Please change the port value to one between 1 and 65535.

AUIC3108W The administration client is currently connected to this AME server. Editing the server definition will cause the client to disconnect from it. Are you sure you want to edit the current server definition?

User response: Click Yes to edit the current server definition and disconnect. Click Cancel to remain connected to the server without editing the current server definition.

AUIC3109E The Archive Log Collector Spill Data Set field should not be empty.

Explanation: A fully qualified data set name is required in the Archive Log Collector Spill Data Set field for a previously allocated data set.

User response: Please specify a previously allocated data set name in the Archive Log Collector Spill Data Set field or allocate a new one by clicking the **New...** button and using the Spill Data Sets Allocator dialog.

AUIC3112W One or more wild-card characters appear within the entered item. Are you sure you want to continue to add this item to the selected list, with the caveat that the wild-card character will be entered in its literal form?

Explanation: You are attempting to add a string with one or more wild-card characters to the selected list.

User response: Click **Yes** to enter the current string in it literal form to the selected list. Click **No** to cancel the operation of adding the current string to the selected list.

AUIC3113E Primary quantity and Secondary quantity field values should be integers.

Explanation: The value(s) entered into the Primary quantity field and/or Secondary quantity field are not integers.

User response: Please make sure that the Primary quantity and Secondary quantity field values are integers, then retry the operation.

AUIC3114E Primary quantity and Secondary quantity field values should either both be empty or both be not empty.

Explanation: One of the Primary quantity or Secondary quantity fields is empty while the other is not.

User response: Please retry current operation where the Primary quantity and Secondary quantity field values are either both be empty, or both not empty.

AUIC3117E Block size field value should be integer

Explanation: The value entered into the Block size field is not an integer.

User response: Please make sure that the Block size field value is an integer, then retry the operation.

AUIC3119W Only the first 512 entries from the returned list are displayed. Please enter more restrictive values in the target filter, then click Refresh.

Explanation: The list of entries returned for the entered filter exceed the maximum threshold of 512 that is allowed to be displayed by the InfoSphere Guardium S-TAP client.

User response: Please enter a more refined filter value before clicking **Refresh** to limit the size of the returned list below the maximum threshold.

AUIC3124E Unknown host: [HOSTNAME]

Explanation: The given hostname cannot be reached.

User response: Please enter a different Server Host and repeat the operation.

AUIC3128E The profile name contains invalid characters.

Explanation: There are invalid characters in the Collection Profile name.

User response: Please ensure that the Collection Profile name contains only alphanumeric characters.

AUIC3300I Are you sure you want to delete the selected server definition?

Explanation: You have opted to delete the selected server definition.

User response: Click **Yes** to confirm the deletion of the selected server definition. Click **No** to cancel the deletion.

AUIC3301I Are you sure you want to delete the selected rule?

Explanation: You have opted to delete the selected rule.

User response: Click **Yes** to confirm the deletion of the selected rule. Click **No** to cancel the deletion.

AUIC3302I Are you sure you want to delete the selected collection?

Explanation: A confirmation is needed prior to deleting the selected collection.

User response: Click **Yes** to confirm the deletion. Click **No** to cancel the deletion and close the informational dialog.

AUIC3303I Are you sure you want to delete the selected group?

Explanation: You have opted to delete the selected group.

User response: Click **Yes** to confirm the deletion of the selected group. Click **No** to cancel the deletion.

AUIC3304I Are you sure you want to delete the selected user?

Explanation: You have opted to delete the selected user.

User response: Click **Yes** to confirm the deletion of the selected user. Click **No** to cancel the deletion.

AUIC3305I Are you sure you want to delete the selected collection profile?

Explanation: You have opted to delete the selected collection profile.

User response: Click **Yes** to confirm the deletion of the selected collection profile. Click **No** to cancel the deletion.

AUIC3306I Are you sure you want to delete the selected authorization?

Explanation: You have opted to delete the selected authorization.

User response: Click **Yes** to confirm the deletion of the selected authorization. Click **No** to cancel the deletion.

AUIC3307E At least one rule should be defined within a collection profile.

Explanation: The collection profile does not contain any rules.

User response: Please define at least one rule for the collection profile before trying to save it.

AUIC3308E The server definition already exists.

Explanation: The same server definition already exists and cannot be duplicated.

User response: Modify one or more of the server definition parameters and try saving again.

AUIC3309E A description must not begin or end with spaces.

Explanation: A description must not begin or end with spaces.

User response: Please specify a description that does not begin or end with spaces.

AUIC3310E A server host must not begin or end with a space.

Explanation: There is a space at the beginning or end of the server host you entered.

User response: Delete the space and retry.

AUIC3311E A server port must not begin or end with a space.

Explanation: There is a space at the beginning or end of the server port you entered.

User response: Delete the space and retry.

AUIC3312E The user has the "Connect to InfoSphere Guardium S-TAP for z/OS " permission and you are not allowed to set this permission.

Explanation: While cloning a new user, the "Connect to InfoSphere Guardium S-TAP for z/OS" permission needs to be assigned however the session user does not possess the necessary permission to do this.

User response: To assign the "Connect to InfoSphere Guardium S-TAP for z/OS" permission, the session user must possess the “Assign Connect" permission.

AUIC3313E The user has permissions set and you are not allowed to set permissions.

Explanation: The cloning of a user with existing InfoSphere Guardium S-TAP permissions failed because you do not have the required **Assign Permissions** privilege in order to assign InfoSphere Guardium S-TAP permissions to a new or existing user.

User response: Please send a request to your InfoSphere Guardium S-TAP administrator to have the **Assign Permissions** privilege assigned to you.

AUIC3315I Are you sure you want to close InfoSphere Guardium S-TAP?

Explanation: You have chosen to close or exit the administration client application.

User response: Click **Yes** to confirm that you want to close the administration client application. Click **No** to cancel the closing of the administration client application.

AUIC3316E Please supply an InfoSphere Guardium S-TAP password.

Explanation: Both a user name and password are required to log on to InfoSphere Guardium S-TAP.

User response: Please supply a valid password and try again.

AUIC3317E Please supply an InfoSphere Guardium S-TAP user name.

Explanation: Both a user name and password are required to log on to InfoSphere Guardium S-TAP. A valid user name has not been entered.

User response: Please supply a valid user name and try again.

AUIC3318I Do you want to save your server definition changes?

Explanation: Changes were made to the current server definition changes.

User response: Click **Yes** to confirm that you want to save the most recent server definition changes. Click **No** to cancel the most recent changes made.

AUIC3319E An illegal argument was used:

Explanation: One or more illegal arguments were detected while trying to login.

User response: Make sure your username and password are correct, then try logging in again.

AUIC3320E An unexpected error occurred: [Error Message]

Explanation: The administration client was unable to carry out the requested operation due to an unexpected programming condition in one of the InfoSphere Guardium S-TAP components or its dependent utilities.

User response: Please check the administration client, server, and/or agent logs for more specific error messages that may hint at the cause of the operation failure. If the cause of the failure is still unknown, please contact IBM technical support for further analysis.

AUIC3332I Some dialogs are still open. Logging out will cause these to close. Do you want to log out?

User response: Click **Yes** to log out and close the open dialogs, or **No** to cancel.

AUIC3323E The profile must have a source.

Explanation: You must select a source in order to proceed with collection profile filters definition.

User response: If the source list appears empty, please ensure that the agent is responsive and/or running, then select a source.

AUIC3324I The server running on the specified host and port was successfully contacted and is responsive.

Explanation: The specified server has responded to network packets sent to it, indicating that it is alive and responsive.

User response: Click **OK** on the informational dialog.

AUIC3325I The server running on the specified host and port is not responsive.

Explanation: The specified server has not responded to network packets sent to it, indicating that it is down and/or not responsive.

User response: Please check the server to see whether it is running, or enter a new server definition and try the ping operation once again.

AUIC3326E Values must be supplied for each field.

Explanation: One or more fields within the Repository JDBC Connection Editor dialog is empty.

User response: Please verify that all fields within the Repository JDBC Connection Editor dialog are filled and try again.

AUIC3327W Unable to edit inactive agent.

Explanation: It is not permitted to edit an agent configuration for an agent that is not active.

User response: Please activate the agent in question before attempting to modify its configuration settings through the administration client.

AUIC3328E The host name and port has incorrectly been set to the same host name and port as the IBM InfoSphere server you are connected to. Please change the values to match the host and port of the server instance where the IBM InfoSphere repository is located.

User response: Please change the values to match the host and port of the server instance where the IBM InfoSphere repository is located.

AUIC3330I Operation cancelled.

Explanation: The user has explicitly cancelled the operation to retrieve a response from the server.

User response: None required.

AUIC3331E Timed out waiting for server response.

Explanation: The administration client has timed out while waiting for the server to respond to its request.

User response: Please check to see that the appropriate IBM InfoSphere server and agent are responsive and operating correctly.

AUIC3501E Can not load IMS entries.

Explanation: Unable to load the IMS entries due to the error specified.

User response: Correct the condition specified in the error message then try refreshing the IMS entries again.

AUIC3502E You must select an IMS entry.

Explanation: Before you can edit an IMS entry, you must select the IMS entry you want to edit.

User response: Please select the IMS entry you want to edit and try again.

AUIC3503I Are you sure you want to delete the selected IMS entry?

Explanation: You have opted to delete the selected IMS entry.

User response: Click **Yes** to confirm the deletion of the selected IMS entry. Click **No** to cancel the deletion.

AUIC3504E Unable to delete IMS entry

Explanation: Unable to delete the IMS entry due to the error specified.

User response: Correct the condition specified in the error message then try to delete the same IMS entry again.

AUIC3508E IMS entry must have a name

Explanation: The IMS subsystem you are trying to import does not have a name associated with it.

User response: Please verify that the IMS subsystem you are trying to import has a valid name.

AUIC3512E Auditing is not possible without specifying at least one SMF mask for the agent associated with the audited IMS.

Explanation: The agent requires at least one SMF mask for auditing.

User response: Specify at least one SMF mask for the agent and retry.

AUIC3513E The operation to check the server status has failed has with the message: [Connection refused: connect] .

Explanation: The AUI server with the specified server host and port could not be contacted.

System action: The system could not verify that the specified server is valid.

User response: Please check that the specified server definition is indeed valid and that the server is running.

AUIC3514E Invalid user definition. The document root tag is not the expected user tag.

Explanation: The document root tag within the file to be loaded was not recognized. The root tag for objects that can be loaded within this panel is the `<user></user>` tag.

User response: Examine the .xml file to be loaded within the task panel and verify that the document root contains the user tag. Repeat the load operation once again. If the operation continues to fail, please contact IBM customer support.

AUIC3515E Invalid group definition. The document root tag is not the expected group tag.

Explanation: The document root tag within the file to be loaded was not recognized. The expected root tag for objects that can be loaded within this panel is the `<group></group>` tag.

User response: Examine the xml file to be loaded within the Groups task panel and verify that the document root contains the group tag. Repeat the load operation once again. If the operation continues to fail, please contact IBM customer support.

AUIC3516E Invalid collection profile definition. The document root tag is not the expected collection profile tag.

Explanation: The document root tag within the file to be loaded was not recognized. The expected root tag for objects that can be loaded within this panel is the `<profile></profile>` tag.

User response: Examine the xml file to be loaded within the Collection Profiles task panel and verify that the document root contains the profile tag. Repeat the load operation once again. If the operation continues to fail, please contact IBM customer support.

AUIC3517E Invalid IMS definition. The document root tag is not the expected IMS tab.

Explanation: The content of the xml file was not recognized. The expected root tag for objects that can be loaded within this panel is the `<ims></ims>` tag.

User response: Examine the xml file to be loaded within the Collection Profiles task panel and verify that the document root contains the profile tag. Repeat the load operation once again. If the operation continues to fail, please contact IBM customer support.

AUIC3519E The password and password confirmation are different.

Explanation: A request to confirm the value of the changed password has failed because the password and password confirmation field were entered differently.

User response: Please reenter the password correctly.

AUIC3520E The connection to server was lost.

Explanation: The administration client is unable to communicate with the InfoSphere Guardium S-TAP server.

User response: Please resolve any network connectivity issues, then try logging in again.

AUIC3525I There is already a server {0} with specified host and port. Do you still want to continue? [where {0} is the server definition description]

Explanation: A server definition already exists with the same host and port that you have specified.

User response: Click **Yes** to create a new server definition with the same host and port. Click **No** to discard the current server definition settings.

AUIC3527E A full server must be specified with a unique name.

User response: Please specify a server with a unique name and retry.

AUIC3528I *<value>* is already in the include list, remove it?

Explanation: You have attempted to add an item to the exclude list that is already in the include list.

User response: Click **Yes** to remove the item from the include list and add it to the exclude list, or **Cancel**.

AUIC3529I *<value>* is already in the exclude list, remove it?

Explanation: You have attempted to add an item to the include list that is already in the exclude list.

User response: Click **Yes** to remove the item from the exclude list and add it to the include list, or **Cancel**.

AUIC3530I File already exists. Do you want to overwrite?

Explanation: You have chosen to save the selected entry to a file with a filename that already exists.

User response: Click **Yes** to overwrite the existing file. Click **No** to cancel the saving of the selected entry.

AUIC3544W The administration client is currently connected to this server. Deleting the server definition will cause the client to disconnect from it. Are you sure you want to delete the current server definition?

Explanation: An attempt has been made to remove the server definition information for the InfoSphere Guardium S-TAP server to which the administration client is currently connected.

User response: Click **Yes** for the Administration client to terminate its connection to the server. Click **No** to terminate the operation.

AUIC3546I There are no targets that match the entered search criteria.

Explanation: No search results were returned because there were no targets that matched the search criteria.

User response: Try a new target search criteria.

AUIC3547I There are no differences between the targets results displayed from the previous and current search criteria.

Explanation: The results obtained from the current search filter and the previous search filter are identical.

User response: Try a new target search criteria.

AUIC3548I There are no PSBs that match the entered search criteria

Explanation: No search results were returned because there were no PSBs that matched the search criteria.

User response: Try a new PSB search criteria.

AUIC3549I There are no differences between the PSBs results displayed from the previous and current search criteria.

Explanation: The results obtained from the current search filter and the previous search filter are identical.

User response: Try a new PSB search criteria.

AUIC3550I There are no segments that match the entered search criteria

Explanation: No search results were returned because there were no segments that matched the search criteria.

User response: Try a new segment search criteria.

AUIC3551I There are no differences between the segments results displayed from the previous and current search criteria

Explanation: The results obtained from the current search filter and the previous search filter are identical.

User response: Try a new segment search criteria.

AUIC3552I There are no databases that match the entered search criteria.

Explanation: No search results were returned because there were no databases that matched the search criteria.

User response: Try a new database search criteria.

AUIC3553I There are no differences between the databases results displayed from the previous and current search criteria.

Explanation: The results obtained from the current search filter and the previous search filter are identical.

User response: Try a new database search criteria.

AUIC3554E Unable to activate a collection containing an empty collection profile.

Explanation: IBM InfoSphere does not permit the activation of a collection containing an empty collection profile.

User response: Please select a non-empty collection profile within the collection before activating it.

AUIC3557E Please supply an HFS Max Size.

Explanation: The mandatory **HFS Max Size** field value is empty.

User response: Please supply a valid HFS Max Size and retry.

AUIC3570W Are you sure you want to logout?

User response: Click **Yes** to continue or **No** to cancel.

AUIC3571W The IMS databases list was partially truncated due to memory constraints while trying to acquire the full list. Please refine your search criteria or increase the region size of the AUI task.

Explanation: The full IMS databases list exceeded memory capacity.

User response: Please refine your search criteria to yield a shorter results list, or increase the region size of the AUI task.

AUIC3572W The IMS segments list was partially truncated due to memory constraints while trying to acquire the full list. Please refine your search criteria or increase the region size of the AUI task.

Explanation: The full IMS segments list exceeded memory capacity.

User response: Please refine your search criteria to yield a shorter results list, or increase the region size of the AUI task.

AUIC3600E Please specify the Batch DLI log stream name.

Explanation: The Batch DLI log stream name field is empty.

User response: Specify the Batch DLI log stream dataset name.

AUIC3601E The Batch DLI log stream name must not exceed 128 characters.

Explanation: The Batch DLI log stream dataset name exceeds 128 characters.

User response: Please specify the Batch DLI log stream dataset, not to exceed 128 characters.

AUIC3602E Please specify the Online DLI log stream name.

Explanation: The Online DLI log stream name field is empty.

User response: Specify the Online DLI log stream dataset name.

AUIC3603E The Online DLI log stream name must not exceed 128 characters.

Explanation: The Online DLI log stream dataset name exceeds 128 characters.

User response: Please specify the Online DLI log stream dataset, not to exceed 128 characters.

AUIC3604E Please specify the MVS ID associated with the Batch log stream name.

Explanation: The MVS ID field associated with the Batch DLI log stream name is empty.

User response: Specify an MVS ID associated with the Batch DLI log stream name.

AUIC3605E The MVS ID associated with the Batch DLI log stream name must not exceed 128 characters.

Explanation: The MVS ID associated with the Batch DLI log stream exceeds 128 characters.

User response: Please specify an MVS ID associated with the Batch DLI log stream name, not to exceed 128 characters.

AUIC3606E Please specify the MVS ID associated with the Online log stream name.

Explanation: The MVS ID field associated with the Online DLI log stream name is empty.

User response: Specify an MVS ID associated with the Online DLI log stream name.

AUIC3607E The MVS ID associated with the Online DLI log stream must not exceed 128 characters.

Explanation: The MVS ID associated with the Online DLI log stream exceeds 128 characters.

User response: Please specify an MVS ID associated with the Online DLI log stream name, not to exceed 128 characters.

AUIC3608E The Batch DLI log stream and Online DLI log stream names must be different.

Explanation: The Batch DLI log stream and Online DLI log stream names specified are the same.

User response: Please specify a different name for the Batch DLI log stream and Online DLI log stream.

AUIC3609I This item has already been added to the selected list.

Explanation: The item you have selected to add has already been added.

User response: None required.

AUIC3610 The SMF Spill Data Set field should not be empty.

Explanation: A fully qualified data set name is required in the SMF Spill Data Set field for a previously allocated data set.

User response: Please specify a previously allocated data set name in the SMF Spill Data Set field or allocate a new one by clicking **New...** and using the Spill Data Sets Allocator dialog.

AUIC3611E The name must not begin or end with a space.

Explanation: The name contains one or more leading or trailing spaces.

User response: Ensure that the name does not contain any leading or trailing spaces.

AUIC3612E The name contains one or more unsupported characters.

Explanation: The name contains one or more non alphanumeric characters.

User response: Ensure that the name only contains alphanumeric characters.

AUIC3613E Unable to create a new IMS entry or update an existing one while the associated agent is inactive or unavailable.

Explanation: The associated agent for the IMS entry is either inactive or unavailable.

User response: Ensure that the agent associated with the IMS entry is active and available before attempting to create or update the IMS entry.

AUIC3614E Unable to activate a new collection while the server or the associated agent is inactive or unavailable.

Explanation: Either the server or the agent associated with the IMS entry for which the collection profile is being applied to is inactive or unavailable.

User response: Ensure that both the server and the agent associated with the IMS entry being applied to the collection profile is active and available.

AUIC3615E to deactivate the collection while the server or the associated agent is inactive or unavailable.

Explanation: Either the server or the agent associated with the IMS entry applied to the collection profile is inactive or unavailable.

User response: Ensure that both the server and the agent associated with the IMS entry that is applied to the collection profile is active and available.

AUIC3616E Unable to delete the IMS entry while the server or the associated agent is inactive or unavailable.

Explanation: Either the server or the agent associated with the IMS entry is either inactive or unavailable.

User response: Ensure that both the server and the agent associated with the IMS entry is active and available.

AUIC3617E The user name contains one or more unsupported characters.

Explanation: The user name contains one or more non alphanumeric characters.

User response: Ensure that the user name only contains alphanumeric characters.

AUIC3618E The password contains one or more unsupported characters.

Explanation: The password contains one or more non alphanumeric characters.

User response: Ensure that the password only contains alphanumeric characters.

AUIC3619E The group name contains one or more unsupported characters.

Explanation: The group name contains one or more non alphanumeric characters.

User response: Ensure that the group name only contains alphanumeric characters.

AUIC3620E The server host contains one or more unsupported characters.

Explanation: The server host contains one or more non-alphanumeric characters.

User response: Ensure that the server host only contains alphanumeric characters.

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>* **seconds.**

Explanation: The sub task that reads event data from SMF log data sets is scheduled to execute every <n> seconds.

User response: None required. If the scheduling for this collector needs to be changed, modify the **<smf-interval>n</smf-interval>** parameter of the agent configuration member (member AUICFGA of the SAUISAMP data set).

AUIF003E **Command** *<command>* **failed; interval value must be between** *<lower-bound>* **and** *<upper-bound>***.**

Explanation: This message indicates that <command> such as:

- */f AUIFSSID,SET INTERVAL <number>*

failed because of incorrect <*number*> value. Correct value must be between <*lower-bound*> and <*upper-bound*>.

User response: Please use interval value between <*lower-bound*> and <*upper-bound*>. If that does not resolve the issue, please contact IBM technical 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: None.

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: None required.

AUIF505I **SMF AUDITING IS DISABLED AT THE AGENT LEVEL**

Explanation: Auditing of SMF events has been disabled at the agent level by use of the Administration User Interface and the agent editor.

System action: The auditing of events sourced from SMF data sets is not performed.

User response: If this is a desired action, then no response is needed. If SMF events should be audited, then the agent configuration should be modified by using the Administration User Interface and the agent editor to select any or all SMF events you wish to be audited.

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 Administration User 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 Administration User Interface and the IMS Auditing Levels to select any or all SMF events you wish to be audited.

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**

Explanation:

TCP/IP Address
ip_address

PORT *port–number*

PING RATE
ping_rate

RETRY INTERVAL COUNT
retry_interval

RETRY COUNT
retry_count

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.

RETRY INTERVAL (*retry_interval*) indicates how often a re-connection to the appliance will be attempted with an inability to connect or a connection failure. The RETRY INTERVAL is shown in hour, minutes and second (HH:MM:SS) format.

RETRY COUNT (*retry count*) indicates how many attempts at a connection or re-connection will be performed before program termination occurs. This value is shown as a decimal number.

System action: The connection to the Guardium S-TAP appliance is attempted.

User response: None.

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.

AUIJ0010E **AGENT RECORD MISSING FROM REPOSITORY. AGENT NAME:** *agent_name*

Explanation: An attempt to read an agent record from the repository failed as the record was not found. This may occur if an agent record has been deleted through the use of the Administration user interface while functions are occurring that require information from the agent record.

System action: The request fails.

User response: Use the Administration user interface to verify that the agent definition has been removed/deleted.

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 may 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: None.

AUIJ012I NUMBER OF *event_type* **EVENTS SENT TO APPLIANCE:** *counter*

Explanation: This message is issued every 100,000 events sent to the appliance or approximately every 18 minutes. It 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*) may 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.

AUIJ013E *call_type* **TO GUARDUIM S-TAP APPLIANCE FAILED. RC:** *return_code* **RSN:** *reason_code* **- RC_GDM=** *gdm_rc* **- RC_PB=** *pc_rc* **- RC_LST=** *rc_lst* **- RS_LST=** *rs_lst*

Explanation: The requested call (*call_type*) to the Guardium S-TAP appliance has failed. RC can be either FFFFFFFF or 00000000. FFFFFFFF indicates an error.

System action: The process terminates.

User response: Determine the cause of the failure by checking the return code/ reason code.

- If RC_GDM is not zero, one of the RC_PB, RC_LST and RSN_LST will be set.
- If RC_LST and RSN_LST are zero but RC_GDM and/or RC_PB is not zero, contact IBM technical support (internal errors).
- If RC_LST and RSN_LST are not zero, consult the IBM InfoCenter for details: http://publib.boulder.ibm.com/infocenter/zos/v1r11/index.jsp?topic=/com.ibm.zos.r11.bpxa800/errno.htm.

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 Server and Agent software requirements documented in this User's Guide for a list of IMS releases support by this version of the product.

AUIJ016E UNABLE TO INITIALIZE APPLIANCE INTERFACE

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 AUICFGA or other member used in the AUICFG DD statement used to provide the agent with configuration information being incorrect. This error may also occur if the target of the TCP/IP address is unresponsive.

AUIJ0201E 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 product support with the content of this message.

AUIJ0202E VSAM ERROR ENCOUNTERED

Explanation:

FUNCTION:
vsam_function

R15: *return_code*

ACBOFLGS:
acboflag_value

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 product support with the content of this message.

AUIJ0203E VSAM ERROR ENCOUNTERED

Explanation:

FUNCTION:
vsam_function

RPL/RECORD TYPE
rpl/record_value

FDBWD:
rpl_fdbwd

OPTCD:
rpl_optcd

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 product support with the content of this message.

AUIJ250I AUDITING IMS EVENTS. COLLECTION PROFILE NAME: *collection_profile_name* **IMS NAME:** *ims_name*

Explanation: The auditing of IMS events is proceeded using the collection profile named (*collection_profile_name*) which is associated with the IMS definition (*ims_name*).

System action: Auditing continues.

User response: None.

AUIJ25IE 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 product support.

AUIJ303W *request_type* **REQUEST FOR LOG STREAM** *log_stream_name* **FAILED - 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: None required.

AUIJ304E *request_type* **REQUEST FOR LOG STREAM FAILED - RC =** *return_code* **RSN =** *reason_code*

Explanation: A request (*request_type*) made to the indicated log stream (*log_stream_name*) has failed. A retry of the request may have been attempted, but failed.

System action: Processing terminates.

User response: Investigate the cause of the error using the return and reason codes returned by the request.

AUIJ305E RECON DATASET ALREDY IN USE - DSN: *recon_dsn* **- AGENT:** *agent_name* **- IMS :** *ims_name*

Explanation: When attempting to define a new IMS or change the RECON data set name of an existing IMS definition, it was found that the RECON data set name (*recon_dsn*) was already in use by another IMS definition (*ims_name*) defined to agent (agent_name).

System action: The RECON data set name change or IMS definition is rejected.

User response: Determine why the RECON data set name was in use.

AUIJ330E REQUIRED DATA SET IS NOT CATALOGED. - 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 support for additional assistance.

AUIJ332E DATA SET IS NOT VALID WITHIN CONTEXT USED - DSN: *data_set_name* **-REASON:** *reason*

Explanation: The data set indicated (*data_set_name*) is not of a type valid for use where 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.

AUIJ351E COLLECTION PROFILE RECORD WAS NOT FOUND - KEY: *record_key*

Explanation: An attempt to find a RECON data set record in the repository has failed.

System action: The request terminates.

User response: The profile you attempted to delete could not be found.

AUIJ352E REQUESTED *record_type* **RECORD HAS BEEN UPDATED BY ANOTHER CLIENT - PLEASE RETRY YOUR REQUEST**

Explanation: An attempt to update a record in the repository has failed as another client has updated the record, since you last viewed it.

System action: The update is rejected.

User response: Click the refresh button to obtain a current view of the record in question, and perform your update.

AUIJ353E UNABLE TO DELETE COLLECTION PROFILE *collection_profile_name* **- ACTIVE AGAINST IMS:** *ims_name* **- AGENT:** *agent_name*

Explanation: An attempt to delete a collection profile has failed as the profile is flagged as being active to the IMS (*ims_name*) defined to agent (*agent_name*).

System action: The delete request fails.

User response: Deactivate the collection using the collection tab in the Administration user interface, then delete the collection profile.

AUIJ354E *data_set_type* **DATA SET ALREADY IN USE - DSN:** *data_set_name* **- AGENT:** *agent_name*

Explanation: The definition of a (*data_set_type*) data set (*data_set_name*) has been rejected as the data set name is already in use by another agent (*agent_name*).

System action: The use of that dataset name is prohibited and the request is rejected.

User response: Choose a new, unused data set name.

AUIJ355E IMS *ims_name* **ALREADY HAS AN ACTIVE PROFILE - PROFILE:** *collection_profile_name*

Explanation: An attempt to active a collection (*collection_profile_name*) on an IMS definition (*ims_name*) has failed as the IMS already has a collection active.

System action: The request is rejected as an IMS definition may only have one active collection.

User response: Deactivate the active collection and activate the desired collection.

AUIJ356E CANNOT EDIT AN *record_type (record_key)* **WITH AN ACTIVE PROFILE - PROFILE:** *collection_profile_name*

Explanation: An attempt to edit an IMS or agent definition has been rejected as the modification of an IMS or agent definition is prohibited while the entity has active collections.

System action: The edit request is rejected.

User response: To edit an IMS definition, deactivate the collection profile. For agents, you must deactivate all active collections against all IMS definitions.

AUIJ357E CANNOT DELETE AN *record_type (record_key)* **WITH AN ACTIVE PROFILE - PROFILE:** *collection_profile_name*

Explanation: An attempt to delete an IMS or agent definition has been rejected as the deletion of an IMS or agent definition is prohibited while the entity has active collections.

System action: The delete request is rejected.

User response: To delete an IMS definition, deactivate the collection profile. For agents, you must deactivate all active collections against all IMS definitions.

AUIJ358E COLLECTION HAS BEEN DEACTIVATED BY ANOTHER CLIENT - PROFILE: *collection_profile_name* **- IMS:** *ims_name*

Explanation: An attempt to deactivate a collection has failed, as the collection has already been deactivated by another client.

System action: The deactivation request is rejected.

User response: Click **Refresh** to obtain the current status of collections.

AUIJ360W LOAD FAILED FOR DBD *dbd_name* **-R1 =** *reason_code* **R15 =** *abend_code*

Explanation: When attempting to provide a list of segments in a database (*dbd_name*) the attempt to perform a z/OS LOAD on the DBD member failed.

System action: Information regarding the contents of this DBD is not returned, however, processing continues.

User response: The most probably cause of this error is an invalid DSN included in the IMS definition DBDLIB data set name list. Correct any errors in the IMS definition.

AUIJ361W INVALID DBD ENCOUNTERD IN DBDLIB -DBD MEMBER NAME: *dbd_name*

Explanation: When attempting to provide a list of segments in a database (*dbd_name*), it was determined that the contents of the DBD member (*dbd_name*) did not conform to expected values.

System action: Information regarding the contents of this DBD is not returned, however, processing continues.

User response: The most probably cause of this error is an invalid DSN included in the IMS definition DBDLIB data set name list. Correct any errors in the IMS definition.

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. If this message is returned with DBD_SEGMENT or PSB_SEGMENT as the *seg_type*, you may avoid this message by refining your search criteria.

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 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 product 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_cod*e) 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.

AUIJ450E DBRC API SERVICE FAILURE - FUNCTION: *function_code* **- RC:** *return_code* **RSN:** *reason_code*

Explanation: A request (*function_code*) to the DBRC API service has failed.

System action: Processing terminates.

User response: Determine the cause of the failure by using the *function_code*, *return* and *reason* codes. Information regarding the DBRC API may be found in manuals contained in the IBM IMS Book shelf for the applicable IMS release.

AUIJ500I STARTING *cycle_type* **CYCLE**

Explanation: The task is starting the processing cycle specified.

System action: Processing starts for the cycle specified.

User response: None 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: None required.

AUIJ502I PROCESSING SMF DATA SET : *smf_data_set_name*

Explanation: The SMF processing cycle has found a new, unprocessed data set which met the SMF mask value, and is beginning to process it.

System action: The data set is read looking for SMF events to report.

User response: None required.

AUIJ503I PROCESSING COMPLETE FOR SMF DATA SET: *smf_data_set_name*

Explanation: The SMF cycle has completed processing the data set.

System action: Any other unprocessed SMF data sets will be processed; if not, others are found. The cycle terminates.

User response: None 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: None required.

AUIJ505I SMF AUDITING IS DISABLED AT THE AGENT LEVEL

Explanation: No SMF events were selected to be audited by this agent.

System action: The task waits for the start of the next cycle.

User response: None required.

AUIJ506I SMF AUDITING IS DISABLED AT THE IMS LEVEL - IMS NAME: *ims_name*

Explanation: No SMF events were selected to be audited by the IMS indicated.

System action: Processing continues with any other IMS systems with active collections. If none exist, the processing cycle completes.

User response: None required.

AUIJ520E NAME/TOKEN SERVICE *service-name* **SERVICE FAILED (***name value***)**

Explanation: The name/token service failed.

System action: Processing terminates.

User response: Contact product support.

AUIJ521W CONTROL BLOCK AUIDCCOM NOT FOUND

Explanation: A critical E/CSA control block was not found.

System action: Processing terminates.

User response: Contact product support.

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.

AUIJ523W NO AUDITED IMS SYSTEMS FOUND

Explanation: : No active collections were found on the LPAR.

System action: No audited events will be found.

User response: If this is expected, then no action is required. View the list of active collections using the Administration User Interface (Collections Tab) to determine if any collections are active.

AUIJ600I NO NEW CATALOGED IMS LOG DATA SETS FOUND

Explanation: The IMS Archive Log processing cycle has determined that no new, unprocessed data sets have been found.

System action: The task waits for the start of the next cycle.

User response: None required.

AUIJ601I PROCESSING IMS LOG DATA SET : *ims_log_data set_name*

Explanation: The IMS Archive log processing cycle has found a new, unprocessed data set and is beginning to process it.

System action: The data set is read looking for IMS Log events to report.

User response: None required.

AUIJ602I PROCESSING COMPLETE FOR IMS LOG DATA SET : *ims_log_data set_name*

Explanation: The IMS Archive log cycle has completed processing the data set.

System action: Any other unprocessed IMS Log data sets will be processed. If not others are found. The cycle will terminate.

User response: None required.

AUIJ603I SCANNING RECON DATA SET FOR IMS LOGS TO PROCESS - RECON1: *recon1_dsn* **- RECON2:** *recon2_dsn* **- RECON3:** *recon3_dsn*

Explanation: The IMS Archive log cycle is reading the RECON data sets to determine if any new, unprocessed data sets exist which required processing.

System action: The RECON data sets are read using the DBRC-API.

User response: None required.

AUIJ604E IMS RECORD MISSING: IMS NAME: *ims_name*

Explanation: A critical error has occurred where the IMS definition record is no longer found in the repository and is needed for further processing.

System action: Processing terminates.

User response: None required.

AUIJ605I RECON DATA SET SCAN CCOMPLETE

Explanation: The RECON data sets have been read. This phase of processing is complete.

System action: Processing continues.

User response: None required.

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 may occur 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 product support.

AUIJ850E VSAM function ERROR - DDN: *dd_name* **- RC:** *return_code* **RSN:** *reason_code*

Explanation: A critical error has occurred when processing the VSAM repository

System action: Processing terminates.

User response: Contact product 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 product support.

Error messages and codes: AUIIxxxx

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

AUII017I IBM InfoSphere Guardium S-TAP for IMS on z/OS initialization complete

Explanation: InfoSphere Guardium S-TAP has successfully initialized in the DLI/DBB batch job or IMS control region environment.

User response: No action necessary.

AUII018E IBM InfoSphere Guardium S-TAP for IMS on z/OS initialization failed

Explanation: InfoSphere Guardium S-TAP 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 AUI messages to determine the reason for the initialization failure.

AUII019E IBM InfoSphere Guardium S-TAP for IMS on z/OS termination failed

Explanation: InfoSphere Guardium S-TAP 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 CODE manual and correct the error. If necessary, contact IBM 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 execute the product using a supported IMS release. Contact IBM 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 execute the product using a supported IMS release. Contact support for further assistance.

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 dataset is available in the STEPLIB/JOBLIB data set concatenation. Contact IBM product 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 product support.

AUII031E STAP FOR IMS INTERNAL LOGIC ERROR *(rc)*

Explanation: InfoSphere Guardium S-TAP initialization found a logic error.

System action: IMS processing continues without auditing.

User response: Contact IBM product 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 product 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 product 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 product support.

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 product 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 product support.

AUII120I NO COLLECTIONS ACTIVE FOR THIS IMS INSTANCE

Explanation: Initialization has completed successfully for the IBM InfoSphere Guardium S-TAP for IMS product but no collections were found that pertain to this batch job or IMS control region.

System action: Processing continues.

User response: None 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 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: If the desired action is to have the *imsexit* executed, then no action is required. If the *imsexit* should not be executed 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. InfoSphere Guardium S-TAP 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.

Error messages and codes: AUILxxxx

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

AUIL001S *module-name***: GETMAIN failed**

Explanation: The module *module-name* could not obtain virtual storage

User response: Increase Region size.

AUIL002I Archive log reader interval set to *<n>* **seconds.**

Explanation: This information message indicates that the Archive log reader is scheduled to process archive logs every *<n>* seconds.

User response: None 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 AUILSSID,SET INTERVAL number failed because of incorrect *number* value. Correct values must be between <*lower-bound*> and <*upper-bound*>.

User response: Please use an interval value between <*lower-bound*> and <*upper-bound*>. If that does not resolve the issue, please contact IBM technical support.

AUIL005S *module-name*: **NOT RUNNING APF AUTHORIZED**

Explanation: The module *module-name* requires APF authorization to execute.

User response: Ensure all load libraries for InfoSphere Guardium S-TAP are APF authorized.

AUIL008S *module-name*: **xxxxxxxx DSN NOT A PDS**

Explanation: The designated library must be a PDS.

User response: Check that the supplied DSN is a PDS.

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: None 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: None 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: None 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: None required.

AUIL604E **IMS RECORD MISSING: IMS NAME:** *ims_name*

Explanation: When attempting to determine certain properties of the IMS named (*ims_name*) it was determined that the IMS record required was not in the product repository.

System action: Processing terminates with a return code of 8.

User response: Contact IBM support.

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: None required.

Error messages and codes: AUIRxxxx

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

AUIR001E **Incompatible repository version** *current version* **(expected:** *required version***).**

Explanation: The version of repository specified in configuration file is not supported by AUI agent/server.

User response: Check configuration file to verify that the specified repository is correct. If the repository is specified correctly and the message occurs, please contact IBM support.

AUIR002E **The provided** *parameter 'value'* **is too long; should be less than** *maximum length* **characters.**

Explanation: The value of the specified *parameter* is too long and exceeds the maximum length *maximum length*.

User response: Specify a shorter value that does not exceed the specified limit for the parameter.

AUIR003E **Specified** *amount* **user groups, but maximum number is** *limit***.**

Explanation: Too many groups were specified.

User response: Limit the number of groups to *limit*.

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*.

AUIR005E **A collection for the profile *profile* and the source *ims* is already active.**

Explanation: The specified profile and source are already targeted by another active collection.

User response: You already have an active collection targeting the specified profile and source. If this message occurs and you do not have an active collection targeting the specified profile and source, please contact IBM support.

Error messages and codes: AUISxxxx

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

AUIS100E **Agent not found.**

Explanation: The agent was not found.

User response: Check the server log for additional information. Contact your administrator or IBM Support, if needed. for assistance.

AUIS101S **The agent at *'machine name'* has unexpectedly disconnected.**

Explanation: The agent at machine *machine-name* has unexpectedly disconnected and the requests associated requiring the given agent can no longer be processed.

User response: Check the agent log to identify why the agent disconnected.

AUIS103E **Location *location-name* does not exist on *machine-name*.**

Explanation: The location that is identified in the message does not exist.

User response: Verify that the subsystem or data sharing group *location-name* exists on *machine-name*.

AUIS104S **The agent for location *location-name* has unexpectedly disconnected.**

Explanation: The agent for the location that is identified in the message has unexpectedly disconnected.

User response: Review the agent job output to determine why it disconnected unexpectedly.

AUIS200E **The configuration file *file-name* is invalid; the root element *element* is not <server-config>.**

Explanation: The contents of the specified configuration file are invalid.

User response: Correct the file contents to specify server-config as the root XML element.

AUIS201E **An error occurred while opening the configuration file *file-name*. *message-text***

Explanation: An error occurred while opening the configuration file that is identified in the message.

User response: Review the message text for more information about the error that occurred. Specify a valid configuration file which is not in use by any other process.

AUIS202E **The length of the *parameter*configuration parameter exceeds *number*.**

Explanation: The length of the configuration parameter that is identified in the message exceeds the maximum allowable length.

User response: Specify a value for the configuration parameter which does not exceed the maximum allowable length.

AUIS203S **A server that uses *repository-name* as the repository is already online.**

Explanation: The repository identified by *repository-name* must not be shared between multiple servers.

User response: Ensure no other server on the sysplex uses the same repository identified by *repository-name*.

AUIS300I **Received an acknowledgment with sequence = *number* and ID = *number* from an agent session with ID = *number*.**

Explanation: IBM InfoSphere Guardium S-TAP for IMS on z/OS received an acknowledgment from an agent session with the ID that is identified in the message.

User response: None required.

AUIS301I Received a data message from an agent session with ID = ***number*****.**

Explanation: IBM InfoSphere Guardium S-TAP for IMS on z/OS received a data message from the agent session with ID that is identified in the message.

User response: None required.

AUIS302I Received a negative acknowledgement with sequence = ***sequence-id*** **from an agent session with ID =** ***session-id*****.**

Explanation: IBM InfoSphere Guardium S-TAP for IMS on z/OS received a negative acknowledgement from an agent session that is identified in the message.

User response: None required.

AUIS303I Received a response with ID = ***id*****, type =** ***type*****, and final indicator =** ***indicator*** **from an agent session with ID =** ***session-id*****.**

Explanation: IBM InfoSphere Guardium S-TAP for IMS on z/OS received a response from an agent session that is identified in the message.

User response: None required.

AUIS304E Invalid data was received from an agent: ***data***

Explanation: Invalid data that is identified in the message was received from an agent.

User response: Contact IBM Customer Support.

AUIS305I Received request with sequence = ***sequence-id*** **and type =** ***type*** **from client session** ***session-id*****.**

Explanation: IBM InfoSphere Guardium S-TAP for IMS on z/OS received a request from the client session that is identified in the message.

User response: None required.

AUIS306I Received a report with type = ***type*** **from an agent session with ID =** ***session-id*****.**

Explanation: IBM InfoSphere Guardium S-TAP for IMS on z/OS received a report from an agent that is identified in the message.

User response: None required.

AUIS307E An invalid report type ***report-id*** **was received.**

Explanation: An invalid report type that is identified in the message was received.

User response: Contact IBM Customer Support.

AUIS400I IBM InfoSphere Guardium S-TAP for IMS on z/OS server started.

Explanation: The server started successfully.

User response: None required.

AUIS401I IBM InfoSphere Guardium S-TAP for IMS on z/OS server is terminating. Please end your session.

Explanation: IBM InfoSphere Guardium S-TAP for IMS on z/OS server is terminating.

User response: End your session.

AUIS402I IBM InfoSphere Guardium S-TAP for IMS on z/OS server is terminating normally.

Explanation: InfoSphere Guardium S-TAP server is terminating normally.

User response: None required.

AUIS403E IBM InfoSphere Guardium S-TAP for IMS on z/OS server is terminating due to prior errors.

Explanation: The InfoSphere Guardium S-TAP server is terminating due to prior errors.

User response: See preceding messages to determine why the server is terminating.

AUIS404E The task is not running APF-authorized.

Explanation: The task is not running APF-authorized.

User response: IBM InfoSphere Guardium S-TAP for IMS on z/OS load library, and the load libraries for all of the IMS subsystems accessed, must be APF-authorized. See "Configuring InfoSphere Guardium S-TAP for IMS" for more information about the required configuration steps.

AUIS405I Sending report with type = ***type*** **to client with session id =** ***session-id*****.**

Explanation: InfoSphere Guardium S-TAP is sending the report that is identified in the message.

User response: None required.

AUIS406I Administrator has requested that this session be closed. Please end your session.

Explanation: The administrator has requested that this session be ended.

User response: End your session.

AUIS410E (CT *request-id*) Task does not exist.

Explanation: (CT *request-id*) Task does not exist.

User response: Contact IBM Customer Support.

AUIS411I (CT *request-id*) Task started.

Explanation: (CT *request-id*) Task started.

User response: None required.

AUIS412E (CT *request-id*) Error: *message-text*

Explanation: Message text identifies the error and the request ID.

User response: Use the specified message text to diagnose the error.

AUIS413I (CT *request-id*) Task ended.

Explanation: (CT *request-id*) Task ended.

User response: None required.

AUIS500I (CT *request-id*) Started processing request with sequence = *sequence-id* **and type =** *type***.**

Explanation: InfoSphere Guardium S-TAP started processing the request that is identified in the message.

User response: None required.

AUIS501I (CT *request-id*) Completed processing request with sequence = *sequence-id* **and type =** *type***.**

Explanation: InfoSphere Guardium S-TAP completed processing the request that is identified in the message.

User response: None required.

AUIS502E An invalid request type *request-id* **was received.**

Explanation: An invalid request type that is identified in the message was received.

User response: Contact IBM Customer Support.

AUIS600I (AT *request-id*) Task started.

Explanation: Task started.

User response: None required.

AUIS601E (AT *request-id*) Error: *message-text***.**

Explanation: Message text identifies the error and the request ID.

User response: Use the specified message text to diagnose the error.

AUIS602I (AT *request-id*) Task ended.

Explanation: Task ended.

User response: None required.

AUIS603I (AT *request-id*) Sent request. agent-info {id= *agent-id***} ; request-info {type=***request-type***,sequence=***sequence-id***}**

Explanation: Request sent.

User response: None required.

AUIS604I (AT *request-id*) Received ack. agent-info {id=*agent-id***}; ack-info {sequence=***sequence-id* **,id=***request-id***}**

Explanation: Acknowledgement received.

User response: None required.

AUIS605I (AT *request-id*) Received nack. agent-info {id=*agent-id***}; nack-info {sequence=***sequence-id***}**

Explanation: Negative acknowledgement received.

User response: None required.

AUIS606I (AT *request-id*) Received response. agent-info {id=*agent-id***} ; response-info {id=***request-id***, final =***indicator***}**

Explanation: Response received.

User response: None required.

AUIS607I (AT [*number*]) Agent disconnected unexpectedly. agent-info id = *number***.**

Explanation: The agent at machine machine-name has unexpectedly disconnected and the requests associated requiring the given agent can no longer be processed.

User response: Check the agent log to identify why the agent disconnected.

AUIS608I Task was cancelled.

Explanation: Task was cancelled.

User response: None required.

AUIS700I (ACP) Received *command* **command.**

Explanation: InfoSphere Guardium S-TAP received the command that is identified in the message.

User response: None required.

AUIS701I (ACP) *command* **-- Begin output.**

Explanation: This is the beginning of the output from the command that is identified in the message.

User response: None required.

AUIS702I (ACP) *command* **-- End output.**

Explanation: This is the end of the output from the command that is identified in the message.

User response: None required.

AUIS703E (ACP) *command* **not recognized.**

Explanation: The command that is identified in the message is not recognized.

User response: Specify a command that is supported by the server. See "InfoSphere Guardium S-TAP Administration" for supported administrative commands.

AUIS704E (ACP) *command* **-- Unique specification ID not specified.**

Explanation: The command is not properly formatted.

User response: See "InfoSphere Guardium S-TAP Administration" for supported administrative commands.

AUIS705E (ACP) *command* **-- Session ID required.**

Explanation: The command is not properly formatted.

User response: See "InfoSphere Guardium S-TAP Administration" for supported administrative commands.

AUIS706I Successfully processed 'modify' command *<cmd>***.**

Explanation: A described modify command has been successfully processed.

User response: None. This is an informational message.

AUIS800E Specified *<amount>* **user groups, but maximum number is** *<limit>***.**

Explanation: Too many groups were specified.

User response: You need to limit amount of groups to *<limit>*.

AUIS801E Group not found.

Explanation: The group was not found.

User response: Make sure you specified the group name correctly. If this does not solve the problem, contact your administrator for assistance.

AUIS802E User not found.

Explanation: InfoSphere Guardium S-TAP was not able to find the user.

User response: Check the server log for additional information. Contact your administrator or IBM Support if needed.

AUIS803E Collection profile not found.

Explanation: The Collection profile was not found.

User response: Check the server log for additional information. Contact your administrator or IBM Support if needed.

AUIS900E User [*user***] not authorized to [***action***].**

Explanation: The user is not authorized to perform the specified action.

User response: Contact your administrator to obtain authorization.

AUIS1100E The provided *<parameter> '<value>'* **is too long; should be less than** *<maximum length>* **characters.**

Explanation: The length of provided parameter exceeds the maximum length.

User response: Specify shorter value for parameter that does not exceed the specified limit.

AUIS1101E The attribute *<attribute>* **of XML element** *<element>* **has wrong value** *'<value>'***.**

Explanation: The attribute *<attribute>* of XML element *<element>* has wrong value *<value>*.

User response: If the error occurred while reading the agent or server configuration file, correct the file contents. Otherwise, contact your administrator.

AUIS1207E Invalid user name/password.

Explanation: An invalid user name or password was entered.

User response: Verify the user name and password and retry the operation.

AUIS1208E Permission Denied.

Explanation: Permission to the InfoSphere Guardium S-TAP server has been denied.

User response: Contact your administrator.

AUIS1240E Connection refused. Client/Server incompatibility detected.

Explanation: Client connection process refused because of client version is not supported by server.

User response: Please use compatible client and server versions. If your versions are correct and you receive this error, contact your administrator or IBM Customer Support.

AUIS1241E Insertion of collection profile failed.

Explanation: The attempt to insert the selected collection profile has failed.

User response: Check the server log for additional information. Contact your administrator or IBM Support if needed.

AUIS1242E The password has expired.

Explanation: The password has expired.

User response: Please specify a new password for the user.

AUIS1243E Empty *Rule [n]* **is not allowed to be part of a collection profile.**

Explanation: An empty rule cannot be part of a collection profile.

User response: Specify target(s) and event(s) for the rule to audit. If the rule is not empty and this message occurs, please contact IBM support.

AUIS1244E Collection profile should contain at least on rule.

Explanation: Collection profile should contain at least on rule.

User response: Add one or more rules to the collection profile.

AUIS1250W This password expires in *n* **days.**

Explanation: The password will expire in the specified number of days.

User response: Please specify a new password for the user.

AUIS1251W This password expires tomorrow.

Explanation: This password expires tomorrow.

User response: Please set a new password for the user.

AUIS1252W This password expires today.

Explanation: This password expires today.

User response: Please specify a new password for the user.

AUIS1260E Allocation parameter invalid: *field* **is empty.**

Explanation: Allocation could not be performed because the specified field is empty.

User response: Please enter a valid entry in the field and retry.

AUIS1261E Allocation parameter invalid: '<*name*>'**max length =** <*max*> **exceeded.**

Explanation: Allocation parameter <*name*> is invalid: max length <*max*> exceeded.

User response: Change the parameter to correspond to the requirements.

AUIS1262E Allocation parameter invalid: '<*parameter name*>' **is negative.**

Explanation: Allocation parameter is not valid: <*parameter name*> must be not negative.

User response: Change the parameter to correspond to the requirements.

AUIS1263E Allocation parameter invalid: '<*parameter name*>' **is not positive.**

Explanation: Allocation parameter is not valid: <*parameter name*> must be positive.

User response: Change the parameter to correspond to the requirements.

AUIS1264E Allocation parameter invalid: *data set name***.**

Explanation: At attempt to allocate a data set using the provided name failed. The name of the data set is invalid per MVS naming requirements.

User response: Please correct the data set name and try again.

AUIS1265E The block size specified must be a multiple of <*multiplier*> **and less then** <*limit*>**.**

Explanation: The block size parameter must be a multiple of <*multiplier*> and less then <*limit*>.

User response: Change the block size parameter to correspond to the requirements.

AUIS2000I IBM InfoSphere Guardium S-TAP for IMS on z/OS Update Administrator Password started.

Explanation: The password update process is starting normally.

User response: None required.

AUIS2001I IBM InfoSphere Guardium S-TAP for IMS on z/OS Update Administrator Password terminating normally.

Explanation: The password was updated successfully and the update process is terminating normally.

User response: No action required.

AUIS2002E IBM InfoSphere Guardium S-TAP for IMS on z/OS Update Administrator Password is terminating due to prior errors.

Explanation: An error occurred while updating the password because of prior errors. The update process is terminating.

User response: Check for previous error messages indicating the reason why the addition of the procedure failed.

AUIS2003I IBM InfoSphere Guardium S-TAP for IMS on z/OS Administrator password for user *user* successfully updated.

Explanation: The password for the specified user was updated successfully.

User response: No action required.

AUIS2004E Addition of new IBM InfoSphere Guardium S-TAP for IMS on z/OS user *user* failed.

Explanation: An error occurred while adding the specified user.

User response: Check for previous error messages indicating the reason why the addition of the new user failed.

AUIS2005E Required configuration parameter *AUI-new-user-password* omitted from configuration file.

Explanation: An error occurred because the required configuration parameter *AUI-new-user-password* was not included in configuration file.

User response: Add the required parameter to the configuration file.

AUIS2006E The supplied password '*password*' must contain at least 6 characters.

Explanation: An error occurred while authenticating the specified user.

User response: Specify a password that contains at least six characters.

AUIS2007E The configuration file *file* is invalid; the root element *element* is not <uap-config>.

Explanation: The specified configuration file is not valid because the specified root element is not <uap-config>.

User response: Change the root element to <uap-config> in the specified configuration file.

AUIS2008E The password '*<password>*' must contain a mixture of numbers, letters, and punctuation.

Explanation: For security purposes, UAP utility requires passwords to contain a mixture of numbers (without respect to case) and letters. Punctuation is also acceptable for use in passwords.

User response: Please enter a password that contains a combination of characters that meet the requirement and try again.

AUIS2009E The password '*<password>*' is too similar to the user name '*<user>*'.

Explanation: For security purposes, UAP utility requires passwords that is different from that of the specified user name.

User response: Specify a password that is different from that of the specified user name.

AUIS2010E An error occurred, return code = *rc*, during hashing of the password '*password*'.

Explanation: An error occurred while hashing the specified password.

User response: Check for previous error messages indicating the reason why the addition of the new user failed. If the information is insufficient to resolve the problem, contain IBM technical support.

AUIS2011I Addition of new IBM InfoSphere Guardium S-TAP for IMS on z/OS administrator user *user* succeeded.

Explanation: The specified user was added successfully.

User response: No action required.

AUIS2012I Addition of new IBM InfoSphere Guardium S-TAP for IMS on z/OS group <*group*> succeeded.

Explanation: The specified group was added successfully.

User response: None required.

AUIS2013E Addition of new IBM InfoSphere Guardium S-TAP for IMS on z/OS group '<*group*>' failed.

Explanation: An error occurred while adding the specified group.

User response: Check for previous error messages indicating the reason why the addition of the new group failed.

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: InfoSphere Guardium S-TAP 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.

AUIT002I Cancelled request with ID = *id* and type = *type.*

Explanation: IBM InfoSphere Guardium S-TAP for IMS on z/OS cancelled the request identified in the message.

User response: None required.

AUIT003E Unable to cancel request with ID = *id* and type = *type*.

Explanation: IBM InfoSphere Guardium S-TAP for IMS on z/OS was unable to cancel the request identified in the message.

User response: The job name or ID was not known, and the job could not be cancelled. Review the message log to determine the name and ID of the job that was submitted, and use native JES facilities to review and cancel the status of the job.

If you are not trying to cancel a z/OS job request, contact IBM customer support.

AUIT004E A cancel request was received for a non-existent request (ID = *id*).

Explanation: You attempted to cancel a non-existent request.

User response: Contact IBM customer support.

AUIT005I Cancelling request with ID = *id* and type = *type*.

Explanation: IBM InfoSphere Guardium S-TAP for IMS on z/OS is cancelling the request identified in the message.

User response: None required.

AUIT006S The product is not properly configured to authenticate users.

Explanation: IBM InfoSphere Guardium S-TAP for IMS on z/OS 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 "InfoSphere Guardium S-TAP for z/OS agent" for more information about how to complete the required configuration.

AUIT007I Completed processing request with ID = *id* and type = *type*.

Explanation: InfoSphere Guardium S-TAP completed processing the request identified in the message.

User response: None required.

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.

AUIT009I No server address was configured; listening for server advertisements.

Explanation: No specific server address was configured, so the InfoSphere Guardium S-TAP client is listening for server advertisements.

User response: None required.

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.

AUIT011E The maximum number of connection attempts has been reached.

Explanation: InfoSphere Guardium S-TAP has repeatedly attempted to connect to the server and the maximum number of connection attempts has been reached.

User response: The agent is not able to connect to the server specified in the configuration file. Review the configuration file to ensure that the correct server host name (or IP address) is specified by the *server-address* configuration parameter. Ensure that the server has been started and is properly running. Ensure that the *server-port* value in the agent configuration file matches the *agent-listener-port* value in the server configuration file.

AUIT012I Performing discovery of available locations.

Explanation: The InfoSphere Guardium S-TAP agent is looking for available locations.

User response: None required.

AUIT013I InfoSphere Guardium S-TAP agent is terminating.

Explanation: The InfoSphere Guardium S-TAP agent is terminating.

User response: None required.

AUIT014I Connected to server *hostname* **on port** *port number***.**

Explanation: The InfoSphere Guardium S-TAP agent has connected to the identified server and port number.

User response: None required.

AUIT015I Attempting connection to server *hostname* **on port** *port number***.**

Explanation: The InfoSphere Guardium S-TAP agent is attempting to connect to the identified server and port number.

User response: None required.

AUIT016I Discovered data sharing group *group name***.**

Explanation: The InfoSphere Guardium S-TAP agent has discovered the identified data sharing group.

User response: None required.

AUIT017I Discovered subsystem *subsystem-id***.**

Explanation: The InfoSphere Guardium S-TAP agent has discovered the identified subsystem.

User response: None required.

AUIT018I The agent is ready to process requests.

Explanation: The agent is ready to process requests.

User response: None required.

AUIT019I InfoSphere Guardium S-TAP agent started.

Explanation: InfoSphere Guardium S-TAP agent started.

User response: None required.

AUIT020I Starting the socket selector thread (thread *thread id***).**

Explanation: The InfoSphere Guardium S-TAP agent is starting the identified socket selector thread.

User response: None required.

AUIT021I Processing request with ID = *id* **and type =** *type***.**

Explanation: The InfoSphere Guardium S-TAP agent is processing a request with the identified ID and type.

User response: None required.

AUIT022I Reading request with ID = *id* **and type =** *type***.**

Explanation: The InfoSphere Guardium S-TAP agent is reading a request with the identified ID and type.

User response: None required.

AUIT023I Received shutdown request.

Explanation: The InfoSphere Guardium S-TAP agent has received a shutdown request.

User response: None required.

AUIT024I Request thread timed out waiting for work.

Explanation: The InfoSphere Guardium S-TAP agent request thread has timed out waiting for work.

User response: None required.

AUIT025I The socket selector thread is terminating.

Explanation: The InfoSphere Guardium S-TAP agent socket selector thread is terminating.

User response: None required.

AUIT026E Location *location name* is not known to the agent.

Explanation: The location name specified on a received request does not match any IMS subsystem ID or data sharing group attachment name known to the agent.

User response: Ensure that a valid location is specified in the client. If a valid location is specified, ensure that the IMS subsystem is operational.

AUIT027S An invalid request type *request-id* was received.

Explanation: The InfoSphere Guardium S-TAP agent received an invalid request type.

User response: Contact IBM customer support.

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 InfoSphere Guardium S-TAP for IMS on z/OS agent" for more information about the required configuration. Check the agent job log for additional messages which may be generated.

AUIT029E Location *location name* has not been configured for use with InfoSphere Guardium S-TAP.

Explanation: The specified location name is recognized by the agent, but an error occurred while accessing the product control file for the location's configuration information.

User response: Use sample job AUISJ001 to establish the required configuration parameters.

AUIT031I Starting the command listener thread (thread *thread-id*).

Explanation: The InfoSphere Guardium S-TAP agent is starting the command listener thread.

User response: None required.

AUIT032I Received stop command: *command-text*.

Explanation: The InfoSphere Guardium S-TAP agent received a STOP command.

User response: None required.

AUIT033I Received modify command: *command-text*.

Explanation: The InfoSphere Guardium S-TAP agent received a MODIFY command.

User response: None required.

AUIT034S InfoSphere Guardium S-TAP agent is terminating due to hard stop request.

Explanation: InfoSphere Guardium S-TAP agent is terminating due to a user /MODIFY FORCE command.

User response: None required.

AUIT035E An error occurred while opening *file-name*: *message-text*

Explanation: An error occurred while opening the specified file and there is also error information in the message.

User response: Use the specified message text to diagnose why the specified file could not be opened.

AUIT036E An error occurred while writing *file-name*: *message-text*

Explanation: An error occurred while writing to the specified file and there is also error information in the message.

User response: Use the specified message text to diagnose why the specified file could not be written.

AUIT037I Associating with advertised server *server name* (description *'description'*)

Explanation: 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 "InfoSphere

Guardium S-TAP for z/OS agent" for more information about how to complete the required configuration. is associating with the identified server.

User response: None required.

AUIT038W An XML error occurred while parsing a server advertisement.

Explanation: An XML error occurred while parsing a server advertisement.

User response: Contact IBM customer support.

AUIT039W The request was cancelled.

Explanation: The request was cancelled due to a user or administrator request.

User response: None required.

AUIT040E An I/O abend S*abend-code***-***reason-code* **occurred on** *filename***.**

Explanation: An abend occurred while trying to write to the identified file.

User response: Review the abend and reason codes to determine the error that occurred while writing the file.

AUIT041I Authenticating user *user-id***.**

Explanation: Authenticating a user with user ID *user-id*.

User response: None required.

AUIT044E The connection to the server has been lost.

Explanation: InfoSphere Guardium S-TAP is unable to communicate with the InfoSphere Guardium S-TAP server.

User response: Please resolve any network connectivity issues, then try logging in again.

AUIT045E Subsystem *ssid* **is not known to the agent**

Explanation: The specified subsystem is not known to the agent.

User response: Verify that the SSID represents a valid subsystem.

AUIT1027E Data set *data set* **already exists.**

Explanation: The specified data set already exists. The data set must be unique.

User response: Enter a unique data set name and retry.

Error messages and codes: AUIVxxxx

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

AUIV013I Listening on port *port-number***.**

Explanation: Identifies the port number that the server is listening to.

User response: None required.

AUIV014I The network connection has been disconnected.

Explanation: The network connection has been disconnected.

User response: None required.

AUIV015I Session *session-id* **ended normally.**

Explanation: The session that is identified in the message ended normally.

User response: None required.

AUIV016I Session *session-id* **established.**

Explanation: The session that is identified in the message has been established.

User response: None required.

AUIV017E The maximum number of listen attempts has been reached.

Explanation: The server cannot open the client or agent port in order to listen for incoming requests.

User response: The server cannot open the client or agent port in order to listen for incoming requests. Ensure that the desired ports are specified in the server configuration file. Ensure that the specified ports are not in use by any other application.

AUIV018E Session *session-id* **has ended abnormally.**

Explanation: The session that is identified in the message has ended abnormally.

User response: Contact IBM Customer Support.

AUIV019E (ACP) *command* **not recognized.**

Explanation: The command that is identified in the message is not recognized.

User response: Specify a command that is supported by the server. See "InfoSphere Guardium S-TAP Administration" for supported administrative commands.

AUIV020I **Successfully processed 'modify' command <*cmd*>.**

Explanation: A described modify command has been successfully processed.

User response: None. This is an informational message.

Error messages and codes: AUIXxxxx

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

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 or server configuration file, correct the file contents. Otherwise, contact IBM Customer 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 or server configuration file, correct the file contents. Otherwise, contact IBM Customer 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 or server configuration file, correct the file contents. Otherwise, contact IBM Customer 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 or server configuration file, correct the file contents. Otherwise, contact IBM Customer 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 or server configuration file, correct the file contents. Otherwise, contact IBM Customer Support.

AUIX019E **An XML schema violation was detected; required element *element* child *child-element* is not present.**

Explanation: An XML schema violation was detected; required element *element* child *child-element* is not present.

User response: If the error occurred while reading the agent or server configuration file, correct the file contents. Otherwise, contact IBM Customer Support.

AUIX020E **Memory allocation failed (*number* bytes).**

Explanation: Memory allocation failed (*number* bytes).

User response: Contact IBM Customer 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 or server configuration file, correct the file contents. Otherwise, contact IBM Customer 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 or server configuration file, correct the file contents. Otherwise, contact IBM Customer 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 or server configuration file, correct the file contents. Otherwise, contact IBM Customer 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 or server configuration file, correct the file contents. Otherwise, contact IBM Customer 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 or server configuration file, correct the file contents. Otherwise, contact IBM Customer 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: If the error occurred while reading the agent or server configuration file, correct the file contents. Otherwise, contact IBM Customer 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 Customer Support.

AUIX028E The command line option *option* is invalid.

Explanation: The command line option *option* is invalid.

User response: Correct the command line option and retry the operation. See "The InfoSphere Guardium S-TAP for z/OS client/server environment" for valid options.

AUIX029E The command line option *option* value *value* is invalid.

Explanation: The command line option *option* value *value* is invalid.

User response: Correct the command line option and retry the operation. See "The InfoSphere Guardium S-TAP client/server environment" for valid options.

AUIX030E The required command line option *option* was not specified.

Explanation: The required command line option *option* was not specified.

User response: Specify the required command line option and retry the operation. See "The InfoSphere Guardium S-TAP client/server environment" for valid options.

AUIX031E A value is required for the command line option *option*.

Explanation: A value is required for the command line option *option*.

User response: Specify a value for the command line option and retry the operation. See "The IBM InfoSphere client/server environment" for valid options.

AUIX032E Too many values were specified for the command line option *option*.

Explanation: Too many values were specified for the command line option *option*.

User response: Specify only one value for the command line option and retry the operation. See "The InfoSphere Guardium S-TAP for z/OS client/server environment" for valid options.

AUIX033E The command line option *option* does not accept any values.

Explanation: The command line option *option* does not accept any values.

User response: Correct the command line option and retry the operation. See "The InfoSphere Guardium S-TAP client/server environment" 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 Customer Support.

AUIX035E The operation completed successfully.

Explanation: The operation completed successfully.

User response: None 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 Customer 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 Customer Support.

AUIX038E Permission is denied (*socket-return-code***).**

Explanation: Permission is denied (*socket-return-code*).

User response: Contact IBM Customer Support.

AUIX039E The network is down (*socket-return-code***).**

Explanation: The network is down (*socket-return-code*).

User response: Contact IBM Customer Support.

AUIX040E No buffer space is available (*socket-return-code***).**

Explanation: No buffer space is available (*socket-return-code*).

User response: Contact IBM Customer 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 Customer Support.

AUIX042E The protocol is not supported (*socket-return-code***).**

Explanation: The protocol is not supported (*socket-return-code*).

User response: Contact IBM Customer 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 Customer 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 Customer 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 Customer Support.

AUIX046E The destination network is unreachable (*socket-return-code***).**

Explanation: The destination network is unreachable (*socket-return-code*).

User response: Ensure that the correct host name or IP address was specified.

AUIX047E The socket handle is invalid (*socket-return-code***).**

Explanation: The socket handle is invalid (*socket-return-code*).

User response: Contact IBM Customer 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 Customer Support.

AUIX049E The function call was interrupted (*socket-return-code*

Explanation: The function call was interrupted (*socket-return-code*).

User response: Contact IBM Customer 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 Customer Support.

AUIX051E The connection was aborted (*socket-return-code***).**

Explanation: The connection was aborted (*socket-return-code*).

User response: Contact IBM Customer 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: Ensure 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 other application's 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 Customer 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 Customer Support.

AUIX056E An invalid parameter was specified (*socket-return-code*).

Explanation: An invalid parameter was specified (*socket-return-code*).

User response: Contact IBM Customer Support.

AUIX057E The socket is not connected (*socket-return-code*).

Explanation: The socket is not connected (*socket-return-code*).

User response: Contact IBM Customer Support.

AUIX058E The operation is not supported (*socket-return-code*).

Explanation: The operation is not supported (*socket-return-code*).

User response: Contact IBM Customer Support.

AUIX059E The socket has been closed (*socket-return-code*).

Explanation: The socket has been closed (*socket-return-code*).

User response: Contact IBM Customer Support.

AUIX060E The socket is already connected (*socket-return-code*).

Explanation: The socket is already connected (*socket-return-code*).

User response: Contact IBM Customer Support.

AUIX061S An unknown error occurred (*socket-return-code*).

Explanation: An unknown error occurred (*socket-return-code*).

User response: Contact IBM Customer Support.

AUIX062E A socket error occurred on *socket-operation*: *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 or server configuration file, correct the file contents. Otherwise, contact IBM Customer 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 or server configuration file, correct the file contents. Otherwise, contact IBM Customer 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 or server configuration file, correct the file contents. Otherwise, contact IBM Customer 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: If the error occurred while reading the agent or server configuration file, correct the file contents. Otherwise, contact IBM Customer Support.

AUIX071E An error occurred while invoking the subsystem interface (RC = *return-code*).

Explanation: The specified return code was returned by the z/OS subsystem interface when trying to query job status or results.

User response: See "MVS Using the Subsystem Interface" for more information about the return code.

AUIX072E An error occurred while invoking the SYSOUT API (SSOBRETN = *return-code*, SSS2REAS = *reason-code*).

Explanation: The specified return code was returned by the z/OS subsystem interface when trying to query job status or results.

User response: See "MVS Using the Subsystem Interface" for more information about the return code.

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: If the error occurred while reading the agent or server configuration file, correct the file contents. Otherwise, contact IBM Customer Support.

AUIX078E An error occurred while opening the DB2 load libraries: RC = *return-code*.

Explanation: An error occurred while opening the DB2 load libraries: RC = *return-code*.

User response: Ensure that the correct list of load libraries for the IMS subsystem is configured in the product control file, using sample job AUISJ001. See "DFSMS Macro Instructions for Data Sets" for more information about the return code.

AUIX079E An error occurred while attaching the DB2 attachment facility subtask: RC = *return-code*.

Explanation: An error occurred while attaching the DB2 attachment facility subtask: RC = *return-code*.

User response: Contact IBM customer service.

AUIX080S The DB2 attachment facility subtask ended unexpectedly: RC = *return-code*.

Explanation: The DB2 attachment facility subtask ended unexpectedly: RC = *return-code*.

User response: Contact IBM Customer Support.

AUIX082E The input DB2 command is too long.

Explanation: The input DB2 command is too long.

User response: Contact IBM Customer 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 "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 "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 "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 Customer Support.

AUIX089E The specified user ID *user-id* and password are invalid.

Explanation: The specified user ID *user-id* and password are invalid.

User response: Correct the user ID and password and retry the operation.

AUIX090E The specified password for user ID *user-id* has expired.

Explanation: The specified password for user ID *user-id* has expired.

User response: Use native facilities to change your password, then retry the operation.

AUIX091E Access for the specified user ID *user-id* has been revoked.

Explanation: Access for the specified user ID *user-id* has been revoked.

User response: See your security administrator to get your user ID reinstated.

AUIX092E An error occurred while performing authentication: SAF RC = *saf-return-code*, RC = *return-code*, RSN = *reason-code*.

Explanation: An error occurred while performing authentication: SAF RC = *saf-return-code*, RC = *return-code*, RSN = *reason-code*.

User response: Contact IBM Customer Support.

AUIX093S An unexpected error occurred (*file-name*, *line-number*).

Explanation: An unexpected error occurred (*file-name*, *line-number*).

User response: Contact IBM Customer 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 Customer 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 Customer 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 Customer 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 Customer 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: None 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 "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: None required.

AUIX117E Excessive data was encountered in the ASN.1 data stream.

Explanation: Excessive data was encountered in the ASN.1 data stream.

User response: Contact IBM Customer Support.

AUIX118E Insufficient data was encountered in the ASN.1 data stream.

Explanation: Insufficient data was encountered in the ASN.1 data stream.

User response: Contact IBM Customer Support.

AUIX119E An unsupported ASN.1 feature was encountered.

Explanation: An unsupported ASN.1 feature was encountered.

User response: Contact IBM Customer Support.

AUIX120E Invalid DES-encrypted data was encountered.

Explanation: Invalid DES-encrypted data was encountered.

User response: Contact IBM Customer Support.

AUIX121E Invalid DES-encrypted data was encountered (pad = ***pad-value*****).**

Explanation: A temporary error occurred while exchanging the encryption key with the server.

User response: Disconnect and connect back to the server. If the error persists, please contact IBM technical support.

AUIX122I Build date ***component*** **=** ***date*****.**

Explanation: Build date *component = date*.

User response: None required.

AUIX123W The action was cancelled.

Explanation: The action was cancelled.

User response: None 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 InfoSphere Guardium S-TAP load library, and the load libraries for all of the IMS subsystems accessed, must be APF-authorized. See "InfoSphere Guardium S-TAP agent" for more information about the required configuration steps.

AUIX125E An error occurred while retrieving product configuration data: RC = ***return-code*****.**

Explanation: An error occurred while retrieving product configuration data: RC = *return-code*.

User response: Ensure that a product control file has been created and loaded using sample jobs AUISJ000 and AUISJ001, and that it is allocated to the IMSPARMS DD.

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.

AUIX128E An error occurred while submitting the job: RC = *return-code***.**

Explanation: An error occurred while submitting the job: RC = *return-code*.

User response: Contact IBM Customer Support.

AUIX129I Job *job-id* **was submitted.**

Explanation: The specified job was submitted.

User response: None required.

AUIX130E An ICSF cryptographic error occurred: API = *<api-call>***, RC =** *<rc>***, REASON =** *<reason>***.**

Explanation: An ICSF cryptographic error occurred at <api-call>.

User response: Contact your administrator or IBM Support.

AUIX131E A BSAFE cryptographic error occurred: API = *<api-call>***, RC =** *<rc>***.**

Explanation: An BSAFE cryptographic error occurred at *<api-call>*.

User response: Contact your administrator or IBM Support.

AUIX132E A shared memory error occurred on "*service name***":** *error message***.**

Explanation: This error may only occur in the primary agent address space and when the error occurs, the primary agent address space will shut down with a CC of 12. The error will only occur during startup and indicates that attempts to create a shared memory segment failed because of an already existing shared memory segment that never belonged to and/or currently does not belong to the primary agent address space.

This message may occur in the secondary address space if the <id> elements in the <address-space-manager-config> parameters of the AUICFGA config member used by the agent primary address space and the secondary address spaces(s) do not match.

User response: Edit SAUISAMP member AUICFGA (or the customized AUICFGA) and specify a different <id> element in the <address-space-manager-config> section.

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 may be present in the message when applicable.

User response: Please contact IBM technical 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 may be present in the message when applicable.

User response: None required.

AUIY003E Active module not found.

Explanation: This message indicates a CSI abend has occurred. Additional diagnostic information may be present in the message when applicable.

User response: None 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 may be present in the message when applicable.

User response: None required.

AUIY005E PSW = *string string*

Explanation: This message indicates a CSI abend has occurred. Additional diagnostic information may be present in the message when applicable.

User response: None required.

AUIY006E Callable service invocation failed with return code = *n* **and reason code = XXXXXXXX**

Explanation: A service requested by the server address space has failed.

User response: View the JES log of the server address space to determine the data set name and reason for the error. Contact IBM support if needed.

AUIY007I Invoking callable service *callable service***.**

Explanation: The specified callable service has been invoked successfully.

User response: None required.

AUIY008I **Returned from callable service** *service-name*

Explanation: Returned from a callable service that is identified in the message.

User response: None 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.

AUIY010S **Attempts to update the CSA failed because of a VSAM mismatch; expected CSVS dataset** *'dataset'***.**

Explanation: Attempts to update the CSA failed because of a VSAM mismatch

User response: Contact your administrator or IBM Support.

Error messages and codes: AUIZxxxx

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

AUIZ001E **Data set** *[dataset]* **is not catalogued.**

Explanation: The data set specified in the message text has not been catalogued.

User response: Allocate the data set.

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. Please 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 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: None 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:

```
address-space-manager-config section, element <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:

```
address-space-manager-config section, element <id>
```

AUIZ006S **Shared memory segment passphrase** *'actual value'* **invalid; expected** *'expected-value'*

Explanation: A passphrase mismatch has occurred, indicating that the shared memory segment may be owned by another installation of InfoSphere Guardium S-TAP.

User response: Change the passphrase for the address space manager and restart the agent:

```
address-space-manager-config section, element <passphrase>
```

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 AUICFGA and members of the primary address space and secondary address spaces.

AUIZ008W **IBM InfoSphere Guardium S-TAP for IMS on z/OS agent failed to shut down properly last time.**

Explanation: The agent did not shut down properly and the shared memory segments were not properly cleaned.

User response: Optional: check the old logs to verify any issues during shutdown.

AUIZ009S Attempts to attach to shared memory segment *segment key* failed.

Explanation: This error message always occurs in conjunction with error message AUIX132E.

User response: Please see error message AUIX132E for resolution.

AUIZ010W Configuration value for *'<parameter>'* is set below the allowed minimum of *<limit>*.

Explanation: Configuration parameter is not valid: *<parameter>* should be not below the *<limit>*.

User response: Please change the parameter to correspond to the requirements.

AUIZ011W Configuration value for *'<parameter>'* is set above the allowed maximum of *<limit>*.

Explanation: Configuration parameter is not valid: *<parameter>* should be not above the *<limit>*.

User response: Please 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: None 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: Please contact IBM technical support.

AUIZ014E Invalid data set *'dataset'*: Data set name must not exceed 44 characters.

Explanation: MVS data sets cannot exceed 44 characters.

User response: Please rectify the current data set(s) that exceed 44 characters, then retry.

AUIZ015E 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: Please specify a data set where each segment contains more than 0 characters and 8 or fewer characters.

AUIZ016E Invalid data set *'name'*: The first character in each segment must be alphabetic (A-Z) or national (#, @, $).

Explanation: The dataset name provided does not is not a valid name and does not satisfy the MVS dataset naming requirements.

User response: Please correct the dataset name and try again.

AUIZ017E Invalid data set *'<dataset>'*: 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: Please specify a data set where non-first characters in the segments is alphabetic (A-Z), numeric, national (#, @, $), or hyphen.

AUIZ018E Invalid data set *'<dataset>'*: 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: Please specify a data set where non-first characters in the SMF segments is alphabetic (A-Z), numeric, national (#, @, $), hyphen, asterisk (*) or percent (%).

AUIZ019E Data set '*data set*' is not APF-authorized.

Explanation: The data set *data set* requires APF authorization.

User response: Specified dataset must be APF-authorized. See "Configuring InfoSphere Guardium S-TAP for IMS" for more information about the required configuration steps.

AUIZ020E 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: Please specify a data set where first character in SMF segments must be alphabetic (A-Z) or national (#, @, $), asterisk (*) or percent (%).

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi, Kanagawa 242-8502
Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A complete and current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml.

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

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

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

Other company, product, and service names may be trademarks or service marks of others.

Index

Product Number: 5655-STM

Printed in USA

SC19-3344-00