

Version 10 Release 1.3

*IBM Security Guardium S-TAP for Db2 on
z/OS
User's Guide*



Note:

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

May 2020 Edition

This edition applies to Version 10 Release 1.3 of IBM® Security Guardium® S-TAP® for DB2® on z/OS® (product number 5655-STQ) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright Rocket Software Inc., 2006, 2020.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

© Copyright International Business Machines Corporation 2006, 2020.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this information.....	V
Chapter 1. IBM Security Guardium S-TAP for Db2 on z/OS overview.....	1
What's new in IBM Security Guardium S-TAP for Db2 on z/OS V10.1.3?.....	1
The IBM Security Guardium S-TAP for Db2 on z/OS installation environment.....	1
Installation and operation requirements.....	3
Compatibility with IBM Db2 Query Monitor for z/OS and other products.....	3
Required user ID authorizations.....	4
Globalization.....	4
Service updates and support information.....	5
Product documentation and updates.....	5
Accessibility features.....	6
Chapter 2. Configuring IBM Security Guardium S-TAP for Db2 on z/OS.....	7
Upgrading from previous versions of InfoSphere Guardium S-TAP for DB2.....	7
Configuring IBM Security Guardium S-TAP for Db2 on z/OS.....	8
APF authorizing the LOAD library data set.....	8
Enabling the dynamic LPA facility service CSVDYLPA.....	9
Service class considerations.....	9
Customizing JCL members.....	9
Creating the IBM Guardium S-TAP for Db2 control file.....	9
Configuring the IBM Guardium S-TAP for Db2 control file.....	10
Configuring the collector agent.....	11
Configuring the collector agent for additional Db2 subsystems.....	13
Support Services Address Space overview.....	14
Enabling CICS Login User ID reporting.....	15
Chapter 3. Data collection.....	17
Data collection process.....	17
Collection policy.....	17
Collected event types.....	18
Filtering.....	19
Event types and filtering.....	20
Filtering by database name.....	21
Filter wildcard support.....	22
Policy pushdown.....	22
Streaming audit data to multiple systems.....	23
Starting and stopping the collector agent.....	23
Including or excluding failed accesses and negative SQL code.....	24
Quarantining SQL activity.....	24
SQL Blocking.....	24
Controlling host variable collection.....	25
Collecting Command activity by using the Audit SQL Collector.....	26
Collecting SET CURRENT SQLID events by using the Audit SQL Collector.....	26
Chapter 4. Reference information.....	27
Sample library members.....	27
MODIFY command.....	28
S-TAP logging.....	31
Collector agent parameters.....	31

Keeping connections active when HOT_FAILOVER is enabled.....	45
Collector agent sample parameter file.....	45
ADHEMAC1 edit macro variables.....	46
Chapter 5. Messages and codes for	49
Error messages.....	49
Error messages and codes: ADHAxxx.....	49
Error messages and codes: ADHGxxx.....	50
Error messages and codes: ADHIxxxx.....	54
Error messages and codes: ADHKxxxx.....	55
Error messages and codes: ADHPxxxx.....	56
Error messages and codes: ADHQxxxx.....	64
Chapter 6. ADHP102E.....	83
Chapter 7. ADHP102E.....	85
Notices.....	87
Trademarks.....	88
Terms and conditions for product documentation.....	88
Privacy policy considerations.....	89
Index.....	91

About this information

IBM Security Guardium S-TAP for Db2 on z/OS (also referred to as IBM Guardium S-TAP for Db2) collects and correlates data access information from Db2 to produce a comprehensive view of business activity for auditors.

These topics provide instructions for installing, configuring, and using IBM Guardium S-TAP for Db2.

These topics are designed to help database administrators, system programmers, appliance programmers, and system operators perform these tasks:

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

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

Chapter 1. IBM Security Guardium S-TAP for Db2 on z/OS overview

IBM Security Guardium S-TAP for Db2 on z/OS (also referred to as IBM Guardium S-TAP for Db2) collects and correlates data access information from Db2 to produce a comprehensive view of business activity for auditors. IBM Guardium S-TAP for Db2 enables you to determine which users updated or read a particular table, on a specific z/OS Db2 system, within a specific time period.

Use IBM Guardium S-TAP for Db2 to collect and correlate the following types of data to the Guardium system:

- Modifications to an object (SQL UPDATE, INSERT, DELETE)
- Reads of an object (SQL SELECT)
- Explicit GRANT and REVOKE operations to capture events where users might be attempting to modify authorization levels
- Assignment or modification of an authorization ID
- Authorization attempts that are denied because of inadequate authorization
- CREATE, ALTER, and DROP operations against an object (such as a table)
- Utility access to an object (IBM utilities only)
- Db2 commands entered, including which users are issuing specific commands

IBM Guardium S-TAP for Db2 uses Db2 data sharing to obtain audit information from all members of the data sharing group.

What's new in IBM Security Guardium S-TAP for Db2 on z/OS V10.1.3?

Version 10.1.3 of IBM Guardium S-TAP for Db2 provides speed and monitoring enhancements.

Enhancements to this version of the product include:

- New Simulation mode enables you to test policies without sending data to the appliance. Data is collected on z/OS.
- Support for the collection of BIND/REBIND events
- Support for the collection of CICS Unit of Work ID
- Improved memory management
- Support for blocking policies pushed-down from the appliance
- Improved filtering of events
- **MODIFY** command now collects more diagnostic information
- Ability to exclude host variables
- Support for initiating an appliance **MUST GATHER** command from z/OS
- Support for S-TAP logging
- Support for Internet Protocol version 6 (IPV6) introduced with PH16991

The IBM Security Guardium S-TAP for Db2 on z/OS installation environment

The IBM Guardium S-TAP for Db2 SQL Collector Agent collects data from an audited Db2 subsystem in accordance with the filtering policies you set with the Guardium system.

The IBM Guardium S-TAP for Db2 collector agent runs as a started task and is responsible for the collection of audit data in an IBM Guardium S-TAP for Db2 environment. As shown in the following

diagram, SQL collector data is filtered and sent to the Guardium system, enabling you to view reports on your workstation.

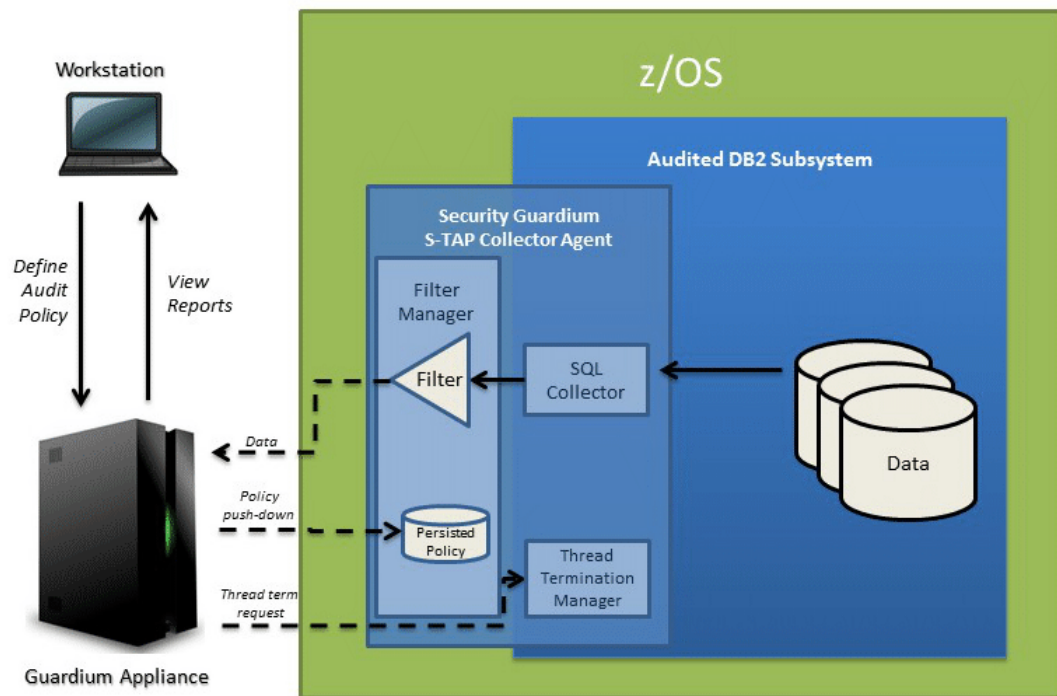


Figure 1. An overview of the IBM Guardium S-TAP for Db2 environment

Guardium Appliance System

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

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

Guardium Appliance System and S-TAP Collector Agent communication

The Guardium system and the IBM Guardium S-TAP for Db2 agent communicate by using a TCP/IP connection. The filtering policies that you create instruct the agent about the data to collect, such as which jobs and data sets to monitor for data accesses.

The IBM Guardium S-TAP for Db2 agent is responsible for:

- Collecting Db2 audit data based on the policy settings.
- Enabling activities to be blocked.
- Streaming collected event activity to the Guardium system.

For more information about how Guardium system policies are interpreted and enabled by the S-TAP, see [“Policy pushdown” on page 22](#).

With the Guardium system installed, configured, and running in your environment, you can test your connection from the z/OS platform to the Guardium system by configuring and running the IBM Guardium S-TAP for Db2 sample library member, ADHTCPD. Consult your network security team to review the results and confirm that connection from the z/OS platform to the Guardium system is available.

Installation and operation requirements

Verify that you have the hardware and software that is required to install and operate IBM Guardium S-TAP for Db2.

FEC common code FMID H25F132 is required, and must be present on the system for the successful installation of this product.

IBM Db2 Data Access Common Collector for z/OS V1.1 (CQC) common code FMID HCQC110 is required, and must be present on the system for the successful installation of this product.

Hardware requirements

Any hardware that is capable of running Db2 for z/OS (V11 or later, until end of service).

Collector agent requirements

- Db2 Version 11 or later, until end of service.
- z/OS Version 2 Release 2 or later, until end of service.
- The IBM Guardium S-TAP for Db2 collector agent must be run on an operating system version that is equivalent to the operating system version on which the product SMP/E installation is performed.
- Resource Recovery Services (RRS) must be configured and enabled for IBM Guardium S-TAP for Db2 to use the RRSF attachment facility to connect to Db2.

Compatibility with IBM Db2 Query Monitor for z/OS

IBM Guardium S-TAP for Db2 does not require Db2 Query Monitor to be installed or activated on a Db2 subsystem that IBM Guardium S-TAP for Db2 audits. If you are running Db2 Query Monitor on your system, be aware that IBM Guardium S-TAP for Db2 can audit a Db2 subsystem that is running Db2 Query Monitor Version 3.2 or later. Certain IBM Guardium S-TAP for Db2 PTFs require Db2 Query Monitor PTFs through SMP/E IFREQ.

To implement Db2 Query Monitor, your site must have the appropriate operating system, environment, hardware, software, and network requirements. For information about installing and operating Db2 Query Monitor, refer to the [IBM Db2 Query Monitor for z/OS Knowledge Center](#).

Compatible releases and maintenance levels

The following product abbreviations are used:

- InfoSphere® Guardium S-TAP for Db2: STP
- IBM Security Guardium S-TAP for Db2 on z/OS: STP
- Db2 Query Monitor: CQM

Table 1. Compatible releases and maintenance levels					
	CQM 3.2	CQM 3.3	STP 9.1	STP 10.0	STP V10.1.3
CQM 3.2	---	LPAR	Db2	Db2	Db2
CQM 3.3	LPAR	---	Db2	Db2	Db2

Table 1. Compatible releases and maintenance levels (continued)					
	CQM 3.2	CQM 3.3	STP 9.1	STP 10.0	STP V10.1.3
STP 9.1	Db2	Db2	---	LPAR	LPAR
STP 10.0	Db2	Db2	LPAR	---	LPAR
STP 10.1.3	Db2	Db2	LPAR	LPAR	---

Where:

LPAR

The two products releases can coexist on the same LPAR (provided they use a different MASTER name), but cannot be active on the same Db2 subsystem.

Db2

The two products releases can coexist on the same LPAR and can both be active on the same Db2 subsystem/shared collector.

Required user ID authorizations

To operate IBM Guardium S-TAP for Db2, the S-TAP collector agent started task must run under the authority of a Time Sharing Option (TSO) user ID with these authorizations.

The collector agent user ID requires Db2 privileges. Grant the collector agent user ID SYSCTRL authority, and the authority to issue the **SELECT** statements on these tables:

- SYSIBM.SYSTABLES
- SYSIBM.SYSTABLESPACE
- SYSIBM.SYSINDEXES

OMVS segment

The collector agent uses UNIX System Services (USS) callable services as the network interface to the appliance. The USS callable services require that an OMVS segment is defined in the RACF® profile for the user ID under which the collector agent job runs. The OMVS segment that is defined for the user ID must contain the following minimum requirements:

- A numeric user ID that is assigned to the user
- A valid path to an existing home directory
- A program name, for example: /bin/sh or /bin/echo for non-shell
- A numeric group ID that is assigned to the user's DEFAULT group

To verify that the ID has an OMVS segment in its RACF profile, use the following command:

```
LU user ID OMVS
```

To add an OMVS segment to the RACF profile of an ID, refer to this sample command:

```
ALTUSER user ID
OMVS(UID(nnn)HOME('/u/ user ID)
PROGRAM('/bin/sh')
```

Globalization

Db2 Universal Database for z/OS is increasingly being used as a part of large client-server systems. In these environments, character representations vary on clients and servers across many different platforms and across different geographies. IBM Guardium S-TAP for Db2 for Db2 Universal Database for z/OS supports these environments by enabling the use of the Unicode encoding scheme for internal processing of metadata and audit data.

IBM Guardium S-TAP for Db2 supports double-byte characters.

Service updates and support information

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

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

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

Product documentation and updates

Db2® Tools information is available at multiple places on the web. You can receive updates to Db2 Tools information automatically by registering with the IBM My Notifications service.

Information on the web

The Db2 Tools Product Documentation web page provides current product documentation that you can view, print, and download. To locate publications with the most up-to-date information, refer to the following web page:

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

You can also access documentation for many Db2 Tools from IBM Knowledge Center:

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

Search for a specific Db2 Tools product or browse the **Information Management > Db2 family**.

IBM Redbooks® publications that cover Db2 Tools are available from the following web page:

<http://www.redbooks.ibm.com>

The Data Management Tools Solutions website shows how IBM solutions can help IT organizations maximize their investment in Db2 databases while staying ahead of today's top data management challenges:

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

Receiving documentation updates automatically

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

To register with the My Notifications service:

1. Go to <http://www.ibm.com/support/mysupport>
2. Enter your IBM ID and password, or create one by clicking **register now**.
3. When the My Notifications page is displayed, click **Subscribe** to select those products that you want to receive information updates about. The Db2 Tools option is located under **Software > Information Management**.
4. Click **Continue** to specify the types of updates that you want to receive.
5. Click **Submit** to save your profile.

How to send your comments

Your feedback helps IBM to provide quality information. Send any comments that you have about this book or other Db2 Tools documentation to comments@us.ibm.com. Include the name and version number of the product and the title and number of the book. If you are commenting on specific text, provide the location of the text (for example, a chapter, topic, or section title).

Accessibility features

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

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

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

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

Chapter 2. Configuring IBM Security Guardium S-TAP for Db2 on z/OS

After you install IBM Guardium S-TAP for Db2, you must customize some files for your system. All configuration steps are required in both stand-alone and data sharing environments.

Before you begin

Review the collector agent security and system requirements before proceeding with the following steps. A list of sample library members is provided in this User's Guide.

About this task

The following table describes the configuration steps and the corresponding SADHSAMP sample library member that is required for customization.

Table 2. Configuration steps

Step	Description of configuration step	SADHSAMP sample library member to use
1	APF authorizing the LOAD library data set	(Not applicable)
2	Customizing JCL members using the ADHEMAC1 macro	ADHEMAC1
3	Binding DBRMs using the JCL bind job	ADHBIND
4	Granting required authorizations to USERID and ADHPLAN by using the JCL authorization member	ADHGRANT
5	Creating the IBM Guardium S-TAP for Db2 control file	ADHSJ000
6	Configuring the IBM Guardium S-TAP for Db2 control file	ADHSJ001
7	Configuring the collector agent	ADHCFGP and ADHCSSID
8	Authorizing ADHPLCY for policy pushdown	Define ADHPLCY to RACF or an equivalent security system

Upgrading from IBM Guardium S-TAP for Db2 V9.0, V9.1, or V10.0

You can upgrade to IBM Guardium S-TAP for Db2 V10.1.3 from IBM Guardium S-TAP for Db2 V9.0, V9.1, or V10.0 by completing these steps.

Procedure

1. Complete the SMP/E installation of IBM Guardium S-TAP for Db2 V10.1.3.
2. APF-authorize the V10.1.3 SADHLOAD data set.
3. Customize and run the Db2 bind job in SADHSAMP(ADHBIND).
4. Customize and run the Db2 grant job in SADHSAMP(ADHGRANT).
5. Export and save your collection profiles.
(V8.1 collection profiles, or policies, were administered either with the InfoSphere Guardium S-TAP for Db2 administration client, or the IBM Guardium system.)
6. Stop the previous version's collector agent and server address spaces.

7. Update the collector started task JCLs (ADHCssid) to:

- Remove the previous version of the product SADHLOAD data sets.
- Include the new V10.1.3 product SADHLOAD data sets in the STEPLIB DD concatenation members.

Note: ADHSssid and ADHAssid started tasks are not used in IBM Guardium S-TAP for Db2 V10.1.3.

8. Update the V10.1.3 collector configuration member (typically SADHSAMP(ADHCFGP)).

9. Install a collection policy on the IBM Guardium system.

- If policy pushdown was used for V8.1 collection administration, follow the Guardium Policy Builder instructions for migrating policies for V8.1 to V10.1.3.
- If the InfoSphere Guardium S-TAP for Db2 administration client was used for V8.1 collection administration, use the XML exported in Step 4 as a reference for the Guardium Policy Builder to define collection policies for V10.1.3.

10. Start the collector address space by typing /S ADHCssid at the z/OS command prompt.

What to do next

Now you can install policies on the z/OS host by using the IBM Guardium system interface. No additional configuration steps are required.

Configuring IBM Security Guardium S-TAP for Db2 on z/OS

After installation, configure IBM Guardium S-TAP for Db2 by completing the steps that are described in this section.

APF authorizing the LOAD library data set

The system programmer must APF authorize the product LOAD library for data collection to work correctly. The system programmer must modify the IEAAPFxx or PROGxx PARMLIB members to define the IBM Guardium S-TAP for Db2 data set, as specified by ADHEMAC1 macro value #SADHLOAD, as an APF authorized library.

About this task

The IBM Guardium S-TAP for Db2 agent requires that all data sets accessed in the STEPLIB of the collector job be APF authorized, including:

- the LOAD library data set
- adhh1q.SADHLOAD
- the FEC data set fechlq.SFECLOAD (where *adhh1q* and *fechlq* are the data set high level qualifier where S-TAP and FEC products are installed)
- the CQC data set cqchlq.SCQCLOAD (where *adhh1q* and *cqchlq* are the data set high level qualifier where S-TAP and CQC products are installed)

Other data sets that require APF authorization are:

- CEE.SCEERUN
- CEE.SCEERUN2
- Db2 EXIT data set (i.e. DSN.VAR1.SDNEXIT)
- Db2 LOAD library data set (i.e. DSN.VAR1.SDSNLOAD)
- SYS1.LINKLIB

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

Enabling the dynamic LPA facility service CSVDYLPA

The user ID that was used to start the Collector Agent PROC must be enabled to use the dynamic LPA facility CSVDYLPA to enable the collector agent to collect data.

About this task

Determine whether the dynamic LPA facility CSVDYLPA is SAF protected. If the dynamic LPA facility CSVDYLPA is not SAF protected, this step is not required.

Procedure

Provide the user ID with ADD/UPDATE/DELETE authority.

For more information about how to enable the CSVDYLPA resource, see section 5.6.3 of the *z/OS V1R7.0 MVS Planning: Operations Guide* (SA22-7601-06), section *Controlling/Adding A Module to LPA after IPL*.

Service class considerations

The collector agent started task must be set at a dispatching priority that is the same as, or higher than, that of Db2.

Related tasks

[Configuring the collector agent](#)

To configure the collector agent, complete the steps provided in each of the subsequent sections. The address space dispatching priority for IBM Guardium S-TAP for Db2 must be the same as, or higher than, that of Db2.

Customizing JCL members

Use the edit macro ADHEMAC1 to customize the variables in the JCL to be run. Running ADHEMAC1 allows you to modify members without requiring you to remember plan names, creators, and other variables from one editing session to the next editing session.

Procedure

1. Copy member ADHEMAC1 from the adhhilvl.SADHSAMP to your site's CLIST library, and then edit the ADHEMAC1 macro with the appropriate variables.
2. After you copy the edit macro to your CLIST library, use it to edit each sample library member individually. You might need to update the macro between edits depending on the member being edited and the context of the variable to be modified in the sample library.
3. To run the macro, type the **ADHEMAC1** command to automatically update the appropriate variables in the member that you are editing.

Related reference

[ADHEMAC1 edit macro variables](#)

This table shows the ADHEMAC1 edit macro variables, including their default value and instructions for use. An example is also provided.

Creating the IBM Guardium S-TAP for Db2 control file

IBM Guardium S-TAP for Db2 configuration information is stored in a VSAM data set, which is the product control file.

About this task

Using the sample JCL that is included with the product, complete these steps to create the IBM Guardium S-TAP for Db2 control file:

Procedure

1. Edit SADHSAMP member ADHSJ000.

2. Add the appropriate job card to ADHSJ000.
3. In the DELETE instruction, change the data set name.
4. In the DEFINE CLUSTER instruction, change the following text within parentheses:
 - Data set NAME
 - VOLUMES
 - DATA NAME
 - INDEX NAME
5. In the REPRO instruction, change the name of the OUTDATASET.
6. Run ADHSJ000 to create the control file. The job steps must end with a return code of zero.

Configuring the IBM Guardium S-TAP for Db2 control file

IBM Guardium S-TAP for Db2 requires information that identifies target Db2 subsystems, product options, and data set attributes. The product configuration is saved in the VSAM product control file data set that you created previously.

About this task

Update the product control file by using the sample JCL that is included with IBM Guardium S-TAP for Db2. Sample library member ADHSJ001 contains the JCL to update the control file. The following steps list the tasks required to configure the product control file data set.

Important: The Db2 plan names that are specified in the product configuration options must match the product plan names assigned to the product's Db2 plans bind plan job.

Procedure

1. Edit SADHSAMP member ADHSJ001.
2. Add the appropriate job card to ADHSJ001.
3. Change ADH.V0A00.CONTROL to the name of the VSAM control data set that you created using member ADHSJ000.
4. Change #SADHLOAD to the name of the product LOADLIB used for IBM Guardium S-TAP for Db2.
5. Modify the SYSIN DD statements as instructed in the sample member. For more information, see [“Required statements for each subsystem”](#) on page 10.

Important: In a data-sharing environment, specify subsystem names (not group names) in ADHSJ001.

6. Run ADHSJ001.

Ensure that the update job steps of the product control file end with a return code of zero. If a non-zero return code occurs, review the job output for errors, correct the problem, and resubmit the JCL.

Required statements for each subsystem

The following statements are required for each Db2 subsystem that is added to the control file.

Table 3. Required statements for each subsystem	
Statement	Setting
SET DB2 SSID	#SSID
UPDATE DB2 ZPARMS	#SZPARM
UPDATE DB2 BOOTSTRAP 1	#SBSDS01
UPDATE DB2 LOADLIB 1	#SDSNEXIT
UPDATE DB2 LOADLIB 2	#SDSNLOAD
SET PRODUCT CFG	NULL

Table 3. Required statements for each subsystem (continued)	
Statement	Setting
SET PRODUCT VER	NULL
UPDATE ADH PLAN 1	ADHPLAN1
UPDATE ADH CORR ID 1	ADH ID 1
UPDATE ADH CORR ID 2	ADH ID 2

Configuring the collector agent

To configure the collector agent, complete the steps provided in each of the subsequent sections. The address space dispatching priority for IBM Guardium S-TAP for Db2 must be the same as, or higher than, that of Db2.

Related reference

[Service class considerations](#)

The collector agent started task must be set at a dispatching priority that is the same as, or higher than, that of Db2.

Configuring the JCL for ADHBIND

SADHSAMP(ADHBIND) is a job that binds the packages and plan used by the collector agent.

Procedure

1. Customize and submit the JCL according to the instructions in the member.
2. Submit the ADHBIND JCL to bind the collector agent packages and plan on each Db2 subsystem on which you want to use IBM Guardium S-TAP for Db2.

Configuring the JCL for ADHGRANT

SADHSAMP(ADHGRANT) is a job that grants authorizations to the user ID and plan that are used by the collector agent.

Procedure

1. Customize and submit the JCL according to the instructions in the member.
2. Submit the ADHGRANT JCL to grant authorizations to the user ID and plan that are used by the collector agent for each Db2 subsystem on which you want to use IBM Guardium S-TAP for Db2.

Note: The ADHGRANT job contains examples of the GRANTS that meet the minimal authorization requirements for the collector agent. Alternative authorizations and, subsequently, GRANTS, can be used to meet the minimal authorization requirements for the collector agent.

Configuring the ADHCFGP data set

The ADH#MAIN program uses parameters to define the IBM Guardium S-TAP for Db2 subsystem name, the monitored Db2 subsystem, the Guardium system host name or network address TCP/IP port, and other parameters that control how the IBM Guardium S-TAP for Db2 collector agent is implemented.

About this task

These parameters are defined in an 80-byte sequential or partitioned data set that you must allocate to the ADHPARMS DD. A sample is available in the SADHSAMP library member ADHCFGP.

Note: The AUDIT parameter is required. It instructs the collector agent to audit a specific Db2 subsystem. It supports only one Db2 subsystem.

To use the sample ADHCFGP member:

Procedure

1. Copy ADHCFGP to the appropriate location (PARMLIB) on your system.
2. Verify that the parameters are valid for your environment. If necessary, edit the parameter file for your IBM Guardium S-TAP for Db2 objects.
3. Edit the ADHPARMS DD in the started task JCL to point to the ADHCFGP data set that you have customized.

Example

An example of the ADHCFGP member contents is as follows:

```
BROWSE    ADH.SMPE.SAMPLIB(ADHCFGP) - 01 L
Command ==>
SUBSYS(#SSID)
AUDIT(#SSID)
MASTER_PROcname (ADHMST31)
APPLIANCE_SERVER(#APPSRVR)
```

Defining the collector agent started task JCL

The collector agent runs as a started task. The sample library member ADHCSSID contains the sample JCL to set up the IBM Guardium S-TAP for Db2 collector agent started task.

Before you begin

To run the collector agent as a started task, the JCL must be in a cataloged procedure library. Modify the sample started task JCL in SADHSAMP library member ADHCSSID for your site, according to the instructions in the member.

About this task

The started task requires:

- READ access to the ADHCFGP data set in the RACF DATASET class
- UPDATE access to the DB2PARMS data set in the RACF DATASET class
- The ability to connect to the Db2 subsystem that is monitored by the collector agent
- The ability to read data from the following Db2 subsystem catalog tables:
 - SYSTABLES
 - SYSINDEXES
 - SYSDBRM
 - SYSPACKAGE
 - SYSPACKSTMT
 - SYSSTMT

Procedure

1. Using the sample library member ADHCSSID as a template, customize the member according to the directions contained in the sample JCL. Any valid member name can be used for the started task name, but the suggested started task name is ADHCSSID, where SSID is the identifier of the Db2 subsystem that is to be monitored.
2. Copy the customized JCL to an appropriate SYSPROC data set. The JCL must include definitions for the following data descriptions:

ADHPARMS

ADHPARMS must name the IBM Guardium S-TAP for Db2 collector agent configuration file.

DB2PARMS

DB2PARMS must name the IBM Guardium S-TAP for Db2 product control file (example: ADH.V0A00.CONTROL).

ADHPLCY

ADHPLCY enables policy persistence. For more information, see the Policy Persistence information provided in [“Policy pushdown” on page 22](#).

If ADHPLCY is defined, it must point to a data set that is allocated with a record format of fixed blocked (RECFM=FB) and a record length (LRECL) greater than or equal to 256.

The ADHPLCY data set should be allocated with a minimum of 50 primary tracks and 10 secondary tracks. The ADHPLCY data set can be sequential, PDS, or PDS/E. If you use PDS or PDS/E, the space requirements might need to be increased in relation to the number of members that are contained within the data set.

ADHLOG

ADHLOG is the SYSOUT data set to which IBM Guardium S-TAP for Db2 collector agent log messages will be written.

STEPLIB

STEPLIB must include the IBM Guardium S-TAP for Db2 SADHLOAD data set.

Note: Every data set allocated to STEPLIB must be APF-authorized.

SYSPRINT

SYSPRINT is the SYSOUT data set to which log messages will be written.

Related reference

Sample library members

Use the following sample library members that are included with IBM Guardium S-TAP for Db2 for installation and configuration.

Configuring the collector agent for additional Db2 subsystems

The collector agent must be configured for each Db2 subsystem that is to be audited.

Before you begin

You must have the following user ID authorities:

- READ access to ADHCFGx parameter data sets, Db2 catalogs, and VSAM control data sets
- Access to the DSNR resource class in Db2
- OMVS segment definition
- GRANT authority for SYSCTRL Db2 to communicate with the agent started task user IDs on all Db2 subsystems to be audited
- READ authority for the Db2 catalog tables
- Authority to use the [dynamic LPA facility CSVDYLPA](#)

To define additional Db2 subsystems for auditing, follow these steps:

Procedure

1. For additional stand-alone Db2 subsystems, use the SADHSAMP member ADHBIND to bind IBM Guardium S-TAP for Db2 plans on each Db2 subsystem that is to be audited.
 - For data sharing group members, use ADHBIND to bind one member of the data sharing group. The bind will apply to all additional group members.
 - When configuring the product control file for each member of the data sharing group, the PLAN value that is used in the ADHBIND job can also be used for the ADHPLAN1 value in the SJ001 JCL job.
 - For the first member of the data sharing group, PACKAGES and PLANS that are used in the ADHBIND job will work for all members of the data sharing group.
2. For each data sharing group or additional stand-alone Db2 subsystem, grant EXECUTE permission for the agent started task ID to the ADH PLAN 1, as specified in the PCF file for the Db2 subsystem. Refer to the JCL SADHSAMP member ADHGRANT for additional details on granting EXECUTE permission to the ADH PLAN.

3. Update the control file with the new SSID, or create a new S-TAP control file for each SSID by using the SADHSAMP member ADHSJ001.
4. Configure a new S-TAP agent configuration file.
5. Add the agent started task name to the z/OS started task table.
6. Start the new S-TAP agent.

Note:

- Dispatching priority must be the same as, or higher than, Db2.

After you start the agent, review the agent log and MVS™ log for any error messages. When an active collection policy is received, the agent starts collecting audit data.

Support Services Address Space overview

IBM Guardium S-TAP for Db2 uses a Support Services Address Space, also referred to as a Master Address Space. Learn about how the Master Address Space works, as well as the implications for using and stopping it.

A Support Services Address Space, also referred to as a Master Address Space, starts for each z/OS image after the first instance of IBM Guardium S-TAP for Db2, InfoSphere Optim™ Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS starts with a MASTER_PROCNAME value that is not yet in use on that z/OS image.

The Master Address Space is a Service Address Space for all instances of IBM Guardium S-TAP for Db2, InfoSphere Optim Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS that specify the same **MASTER_PROCNAME** parameter value that is running on the z/OS image. The Master Address Space acts as a placeholder for shared collector resources, and is similar to other Master Address Spaces that are used throughout MVS. For sample, MVS and Db2 both have Master Address Spaces.

The Master Address Space:

- Never shuts down
- Does not run any code except for its initialization routines
- Owns resources that are needed by the shared collector
- Does not require a formal shutdown and should not be canceled or forced to shut down during the operation of IBM Guardium S-TAP for Db2, InfoSphere Optim Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS.
- Forcing the Master Address Space to stop causes the abnormal termination of all IBM Guardium S-TAP for Db2, InfoSphere Optim Query Workload Replay for Db2, and IBM Db2 Query Monitor for z/OS subsystems on the LPAR.

Important: During installation, do not stop or start the Master Address Space unless required by product maintenance or instructed to do so by IBM Software Support.

Usage considerations for the Master Address Space

The following considerations apply to the use of the Support Services Address Space when you are using IBM Guardium S-TAP for Db2 to monitor the same Db2 subsystem, or multiple Db2 subsystems, on the same LPAR.

Monitoring the same Db2 subsystem

If you use multiple collector products (such as IBM Guardium S-TAP for Db2, InfoSphere Optim Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS) to monitor the same Db2 subsystem, each product must specify the same value for the **MASTER_PROCNAME** parameter.

Monitoring multiple Db2 subsystems that reside on the same LPAR

If you use multiple collector products (such as IBM Guardium S-TAP for Db2, InfoSphere Optim Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS) or multiple instances of the same product to monitor different Db2 subsystems that reside on the same LPAR, each product can have a different value for the **MASTER_PROCNAME** parameter.

Note: This rule applies to instances when you are running different maintenance levels of the same product on the same LPAR (for example, if you are testing new maintenance levels prior to upgrading your production system).

Stopping the Master Address Space

Do not stop the Master Address Space unless you are directed to do so by IBM Software Support or by a +HOLD(ACTION) in a PTF.

To ensure product stability, the Master Address Space should only be stopped by using the sample job that is provided in SADHSAMP, member ADHMSTR. This job verifies that no IBM Guardium S-TAP for Db2, InfoSphere Optim Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS subsystems are using the Master Address Space before it is stopped.

Enabling CICS Login User ID reporting

You can capture the CICS® Login User ID for SQL Statements that are run in Db2 for CICS. The capture of CICS transactions is limited to CICS versions TS 4.2 or later, until end of support.

About this task

Update the CICS Connection definition to capture the CICS Login User ID:

Procedure

1. Set the **ATTACHSEC** parameter to **ATTACHSEC (IDENTIFY)** for the user ID to be passed from the Terminal-Owning Region (TOR) to the Application-Owning Region (AOR).
This makes the user ID available for collection.
2. Ensure that the **CICS_USERID** collector agent parameter is set to Y to enable reporting of the CICS login user ID. For more information, see [Collector agent parameters](#).

Results

The CICS Login User ID is reported in Guardium interface **DB2 Client Info** field for SQL Statements that are run in Db2 for CICS transactions.

Chapter 3. Data collection

IBM Guardium S-TAP for Db2 collects data from an audited Db2 subsystem, in accordance with the collection policies that you create through the IBM Guardium system. Use a collection policy to specify filtering criteria that captures relevant data and filters out irrelevant data. The filtering criteria that you specify determines which data is streamed to your IBM Guardium system.

You can define and manage data collection and filtering in the **Guardium Policy Builder** of the IBM Guardium system interface.

Data collection process

During the collection process, IBM Guardium S-TAP for Db2 collects event data and verifies the data against the collection criteria that is defined in the collection policy.

Collection includes the following:

- All reads and all changes (with collector agent based collection)
- Host variables up to a maximum of 256 bytes per variable
- Dynamic SQL text up to 2 million bytes per statement
- Static SQL text up to 4000 bytes

Data collected from Db2 is filtered during the collection process, and non-relevant events are discarded. Specify filtering criteria by defining a collection policy so that only relevant events are captured. This limits the amount of unnecessary data that is collected and stored by IBM Guardium S-TAP for Db2.

Collection policy

The collection policy is defined by the Guardium policy. It is used to determine which events (SQL, Command, Utilities, etc.) are streamed from the z/OS collector agent to the Guardium appliance. The following methodology determines how the collection policy determines whether to stream events to the Guardium appliance.

The collection policy is comprised of one or more rules. Each rule includes a list of filtering criteria (fields), which is used to determine the events that are streamed. An event is streamed to the appliance if the fields within the event match all of the fields defined within any rules of the collection policy. (Evaluation of the rules within the collection policy is *or*.) For example, if a collection policy is composed of three rules (rule 1, rule 2, and rule 3), an event is streamed if it matches rule 1, or rule 2, or rule 3.

Each rule is made up of filter types and values (fields) that are used to determine if an event should be collected. If the fields of the rule are equivalent to the corresponding fields in the event, the rule evaluates the event to be true, or a match, and the event is captured. A rule is considered true if one of each specified filter type and value matches that of the event. (Evaluation of the rule is *and*.) For example:

- If a rule is comprised of the filters **DBUser**=User1 and **PLAN**=DSNTEP2, an event is collected by the rule if both **DBUser**=User1 and **PLAN**=DSNTEP2 are present in the event. If only one of the filtering criterion is present, or neither of the filtering criteria are present, the event does not meet the conditions of the rule and will not be collected by the rule.
- If a rule is comprised of the filters **NET_PROTOCOL**=TSO and **OS_USER**=User1, then only TSO workload events executed by User1 will be collected by the rule (wherein User1 is **Original Auth ID**). Non-TSO workloads run by User1 will not be collected by the rule, nor will TSO workloads run by User2.

The following sections further describe how to filter the collector agent.

Collected event types

All event types are collected with the SQL Collection mechanism, which is not dependent on other SQL Trace information such as the Db2 Trace (IFI) or SMF data. Filtering criteria is defined and managed through the IBM Guardium system interface. This table lists the types of events that can be collected.

<i>Table 4. Collected event types</i>
Collected event types
All reads (SQL SELECT)
All changes (SQL UPDATE, INSERT, DELETE)
Authorization
Audit data for Db2 utilities
Grant/Revoke
Access attempts
Binds/Rebinds
Commit/Rollbacks
Db2 commands
Db2 utilities
Failed logins
Create, Alter, Drop table
Create, Alter, Drop all other object types
Static SQL host variables
Static SQL text
Dynamic SQL host variables
Dynamic SQL text
Negative SQL events
SQL events involving Accelerated/IDAA tables

Information collected for CICS events

For events that are collected with **Net Prtcl** of a type that originates from CICS, the Internet Protocol (IP) address is reported as **Terminal ID** and the CICS End User is reported as the **DB2 User Name** in the IBM Guardium system interface.

Audit data for Db2 Utilities

You can collect table information for Db2 utility operations that are run against tablespaces. The IBM Guardium S-TAP for Db2 collector agent reports the name of the table associated with the tablespace. Configure audit data for Db2 utilities according to the following rules.

Set the **STAP_UTILITY_TS_TO_TABLE** parameter to Y to collect audit data for Db2 utilities. See [“Collector agent parameters” on page 31](#) for more information.

Audit data for Db2 utilities is collected according to the following rules:

- When a single table is contained in the tablespace, the table information is reported.
- When more than one table is contained in the tablespace, the product can be configured to report either:

No tables

The tablespace is reported, but no tables are reported.

All tables in the tablespace

Utility operations are reported against the accessed table.

This option can result in false positives being reported against tables in the tablespace that were not affected by the running of the utility.

Filtering

IBM Guardium S-TAP for Db2 V10.1.3 greatly simplifies the filtering process from that which was used in past product versions. All filtering occurs at the point of collection regardless of the field types that are included in the rules for the active collection policy. Filtering occurs at the point of collection with or without the specification of object types, which results in efficient CPU usage.

Filtering occurs when you create a filter that uses one or more of the following filter fields:

Net Prtcl

Specifies the appliance connection type to Db2.

OS User

Specifies the original operator user ID that is used to connect to Db2.

DB User

Specifies the primary AUTHID that is used for authorization within Db2. In most situations, this value is the same as OS User.

App. User (PROG=program)

Specifies a valid DB2 program name, such as DSNTEP2.

App. User (PLAN=plan)

Specifies a valid DB2 plan name, such as DSNTEP2.

Client Info (APPL=transaction name)

Specifies a valid program (or user workstation transaction) name, such as db2.exe.

Client Info (WKSTN=workstation name)

Specifies a valid user workstation name, such as PCsys1.

Client Info (USER=user name)

Specifies a valid user name, such as PCuser1.

Object type (%/SYSIBM.SYSTABLE)

Specifies a table.

These fields can be fully qualified, or partially qualified by using the percent sign wildcard character. For more information about using wildcard characters, see [“Filter wildcard support”](#) on page 22.

The most efficient CPU usage is achieved when you create a filter that eliminates the greatest number of events. To increase filtering efficiency, refine your filtering criteria by indicating the additional filtering types with specific values that are associated with the data that you want to collect.

Improving filtering efficiency

You can improve the CPU efficiency of filtering by including filter types in the filter. Specifying the plan, auth ID, connection type, operator ID, program, workstation user, workstation name, or object filter types that are associated with the performed action improves efficiency, as shown in the following example.

Example

To capture access to a table called *MY.TABLE*, you could create the following filter:

Filter 1

Schema.Table equal to *MY.TABLE*

This filter causes IBM Guardium S-TAP for Db2 to capture only those events that access *MY.TABLE*.

To increase efficiency in this example, specify a filter field, such as plan, even if you are sure that plan is the only plan that accesses this table. To capture access to the table *MY.TABLE* for an application that runs under a specific plan, such as *MYPLAN*, the following is an example of a more efficient filter:

Filter 2

Plan equal to *MYPLAN*

Schema.Table equal to *MY.TABLE*

Specifying the plan results in only those events with the specified plan and object being streamed to appliance. Fewer events streamed to the appliance results in improved CPU usage.

Event types and filtering

The following table shows the correlation between the event type and filtering. You can define and manage filtering criteria by setting the Database Type to **DB2 Collection Profile** in the **Guardium Policy Builder** of the Guardium appliance interface.

If you enable collection of SELECT/UPDATE/INSERT/DELETE events, then the event collection is subjected to additional filtering. If you enable collection of event types other than SELECT/UPDATE/INSERT/DELETE, then the events are collected without being subjected to filtering.

Table 5. Event types and filtering	
Event type	Subjected to filtering?
SELECT/UPDATE/INSERT/DELETE (SUID)	Yes
CREATE/ALTER/DROP	No
GRANT/REVOKE	No
SET CURRENT SQLID	No
Db2 COMMANDS	No
Db2 UTILITIES	No
FAILED LOGINS	No
NEGATIVE SQLCODEs	No
COMMIT/ROLLBACK	No
BINDS/REBINDS	No

Enabling the collection of specific event types

The active policy determines which event types are enabled for collection. If the event type is enabled within a rule for the active policy, it is enabled for all rules within the active policy.

An event that is enabled in Rule 1 is subjected to subsequent rule filters. The following is an example using ASC event type collection:

- Rule 1 contains an Object field value of %/%.%.
- Rule 1 contains **AUTHID** filtering for User 1.
- Rule 2 contains **AUTHID** filtering for User 2.
- **SELECT/UPDATE/DELETE/INSERT/SET CURRENT USERID/CREATE/ALTER/DROP** events are collected for all tables for both User 1 and User 2.

Tip: This example could be simplified by placing both AUTHIDs into a group within a single rule.

The following is an example using event type collection:

- Rule 1 contains the collection of **Utility** events.
- Rule 1 contains **AUTHID** filtering for User 1.

- Rule 2 does not contain the collection of **Utility** events, but it contains **AUTHID** filtering for User 2.
- All **Utility** events are collected because they are enabled for Rule 1.

This list describes how you can enable the collection of specific event types:

SELECT/UPDATE/INSERT/DELETE (SUID)

Enable collection by including any filter type or non-blank value in the **Object** field of the rule.

Two target records are reported for nested INSERT/UPDATE/DELETE events: SELECT, and either INSERT, UPDATE, or DELETE. All nested INSERT/UPDATE/DELETE events are considered Table Change events. If the table filter is set to collect only READ events, then these events are filtered out (not collected).

Wildcarding can be used within the **Object** field value, for example: %/SYSIBM.SYSTABLES or %/%%.

CREATE/ALTER/DROP

Collection is automatically enabled by including any filter type or non-blank value in the **Object** field of the rule.

Wildcarding can be used within the **Object** field value, for example: %/SYSIBM.SYSTABLES or %/%%.

GRANT/REVOKE

Enable collection through the **GRANT/REVOKE** command setting.

SET CURRENT SQLID

Collection is automatically enabled by including any filter type or non-blank value in the **Object** field of the rule.

Wildcarding can be used within the **Object** field value, for example: %/SYSIBM.SYSTABLES or %/%%.

DB2 COMMANDS

Enable collection through the **DB2 Commands** command setting.

DB2 UTILITIES

Enable collection through the **UTILITES** command setting.

FAILED LOGINS

Enable collection through the **FAILED AUTHID CHANGES** command setting.

NEGATIVE SQLCODES

Enable collection through the presence of a negative SQLCODE list. Only one list is allowed per policy.

SQLCODE collection can be added to an active collection policy. A policy that contains a single rule with only negative SQLCODES results in an inactive policy.

COMMIT/ROLLBACK

Enable collection by adding **COMMIT/ROLLBACK** to the Guardium appliance policy.

Filtering by database name

IBM Guardium S-TAP for Db2 enables you to filter by database name. You can specify database name filters, on a per-rule basis, to be included in the SQL activity filters.

The following operations are supported:

Included operations

The event is audited if any of the objects are in any of the DBNAMEs.

Excluded operations

If all of the objects are not in any of the DBNAMEs, then it is considered a match.

Example: All of the objects must be in one or more of the DBNAMEs for them to be excluded. If an object is from a DBNAME that is not in the list, then it is considered a match. If any database that is accessed by the query is not in the EXCLUDE DB list, then the query must be captured.

Wildcarding

Filter values can include the percent sign (%) as a wildcard character.

Filter wildcard support

When you are creating a filter, value strings can include the percent sign (%) as a wildcard character. The wildcard character (%) enables the collector to match strings without you having to provide all possible string values for a filter value.

Note: The use of wildcards in filters can potentially result in the collection of significant amounts of captured data.

Filtering fields can be fully qualified, or partially qualified, by using the percent sign wildcard character. You can insert the wildcard character (%) anywhere within the value string. The presence of the wildcard character (%) represents a string of zero or more characters. It can be embedded within a string in the following ways to achieve the following results:

%

Matches all strings.

%a

Matches all strings that end with the letter *a*, for example: *a*, *ba*, *cba*.

a%

Matches all strings that start with the letter *a*, for example: *a*, *ab*, *abc*.

a%a

Matches all strings the begin and end with the letter *a*, for example *a*, *aba*, *aca*.

Note: The wildcard character (%) cannot be used explicitly as part of the filter value.

Policy pushdown

At startup, the IBM Guardium S-TAP for Db2 collector agent waits for a policy to be streamed (or pushed down) from the Guardium system before activating a collection. When the collector agent receives a policy, it inactivates the active collection (if a collection is active), updates the collection profile with the new policy, and then activates the collection policy.

The following processing occurs in the collector agent when a policy is received:

1. The new policy is compared to the currently active policy if the new policy contains one or more rules.
 - a. If the policies are identical, no further processing is required.
 - b. If the policies are not identical, the policy is written to DD:ADHPLCY (if defined) and it becomes the active collection policy.
2. If the new policy does not apply to this subsystem, processing continues without any changes. In this case, if there is an active policy, the collection continues to use it. If no policy is active, none is started.
3. If the new policy is inactive (contains no general audit settings, table or target definitions), the active policy is inactivated.

Policy persistence

For a policy to be pushed down, the z/OS collector agent requires connection to the Guardium appliance. If the z/OS collector agent is unable to connect to the appliance, the z/OS collector agent will read the policy from the ADHPLCY DD (if it is defined in the started task JCL). The z/OS collector agent will activate collection based on the policy that is read from the DD until a connection with the appliance is established. When the connection is established, the policy that is pushed down from the appliance replaces the policy that was read from the DD.

The file contents defined by the ADHPLCY DD contains the policy from the last successful policy pushdown from the appliance.

If ADHPLCY is defined, it must point to a data set that is allocated with a record format of fixed blocked (RECFM=FB) and a record length (LRECL) greater than or equal to 80.

Suggested ADHPLCY DD settings are as follows:

- Record format (RECFM): FB
- Record length (LRECL): 80
- Block size (BLKSIZE): 3120
- Data set name type (DSNTYPE): LIBRARY
- Data set organization (DSORG): PO

The ADHPLCY data set should be allocated with a minimum of 50 primary tracks and 10 secondary tracks. The ADHPLCY data set can be sequential, PDS, or PDS/E. If you use PDS or PDS/E, the space requirements might need to be increased in relation to the number of members that are contained within the data set.

For more information about creating, activating, and inactivating policies from the Guardium system interface, see the how-to topics in the *Security Guardium V10.1.3* documentation in the IBM Knowledge Center.

For more information about using data sets, see the z/OS documentation in the IBM Knowledge Center, https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.idad400/toc.htm.

Streaming audit data to multiple systems

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

Multistream mode provides a mechanism for distributing a high-volume workload over multiple connected appliances. In multistream mode, a single audit event is only sent to a single appliance. Multistream mode does not enable mirroring of the same set of audit events to multiple appliances.

IBM Guardium S-TAP for Db2 sends events to a single appliance until a ping occurs, or the number of records that is specified by **MEGABUFFER_COUNT** is reached.

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

The **APPLIANCE_SERVER** parameter specifies the first appliance to which audit events are streamed. The collection policy that is pushed down from the first appliance determines which events are collected and streamed to all appliances that are enabled for multistreaming.

The IBM Guardium S-TAP for Db2 agent streams events to the first appliance, then sequentially to each subsequent appliance in the multistreaming set. Each appliance in the multistreaming set then processes (logs and discards) each event in accordance with the locally installed policies.

Starting and stopping the collector agent

After you configure the product and review the data collection information, you can start the collector agent. Use the commands provided to start and stop the collector agent started task from a cataloged procedure library.

Procedure

1. To start the collector agent, use the **START** command.
Example: **/S ADHCSSID**
2. To stop the collector agent, use the **STOP** command, or the **MODIFY** command with the **STOP** parameter.

Example:

```
/P ADHCSSID
```

or

```
/F ADHCSSID,STOP
```

Including or excluding failed accesses and negative SQL code

IBM Guardium S-TAP for Db2 enables you to include or exclude failed accesses and negative SQL code on a per-policy basis.

In the Guardium appliance interface, create a list of SQL codes to include or exclude during data collection. A policy can contain either all values to be included, or all values to be excluded. In an *include* list, any SQL activity that fails within the SQLCODE list will be collected. In an *exclude* list, any SQL activity that does not fail within the SQLCODE list will be collected.

Note:

- No other filtering criteria will be ANDed with the SQLCODE filter rule when determining the collection status of the event.
- Enabling AUDIT TRACE CLASS 1 (collection of failed accesses) is deprecated because negative SQL codes for these failed accesses will be collected.
- Failed access events are streamed to the appliance if the negative SQL code is:
 - Included in the list of negative SQLCODE to be captured
 - Not based on *ALL FAILED AUTHORIZATIONS* being included in the **COMMANDS** filter setting for the policy. *ALL FAILED AUTHORIZATIONS* can be removed from the **COMMANDS** filter setting.

Quarantining SQL activity

IBM Guardium S-TAP for Db2 enables you to quarantine the SQL activity of specific users for specific periods of time.

Quarantining a user of a specific Db2 subsystem means that for the period of time that is specified, the quarantined user will not be able to run SQL statement in the targeted Db2 subsystem. If a quarantined user attempts access during a restricted time, access will be denied. Use the Guardium appliance interface to quarantine user activity.

Note: Quarantine does not take effect immediately. The SQL statement that produces the event to trigger the quarantine is completed before the quarantine takes effect. It is possible for additional SQL statements to be run by the quarantined user before the quarantine takes effect.

SQL Blocking

You can block the SQL activity of Db2 users' (Auth IDs) access to specific tables and databases. SQL statements that are run against accelerated tables are eligible for blocking if the blocking filtering criteria is met. If a SQL statement matches the blocking criteria, the SQL statement is prevented from running. Use the Guardium appliance interface to define blocking policies.

Enabling blocking policy

Blocking policy pushdown maps blocking policies to the S-TAP blocking mechanism within the collector agent. At startup, the collector agent checks if a blocking policy was streamed (or pushed down) from the IBM Guardium system when a collection policy was pushed. When the collector agent receives a blocking policy, it inactivates any incidence of active blocking, updates the blocking policy, and activates blocking.

When a blocking policy is received, the collector agent completes the following steps:

1. Compares the new blocking policy to the currently active blocking policy, if the new policy contains one or more rules.
 - If the blocking policies are identical, the collector agent determines that no further processing is required.
 - If the blocking policies are different, then the new blocking policy replaces the old one.
2. Evaluates the pushed-down list and filters to determine which events to block.
3. Validates the list of supplied objects.
 - The object must exist at the time of the installation of the blocking policy.
 - If a table that is included in the blocking policy does not exist when the blocking policy is installed, message ADHP190W is generated to identify the table.
 - Blocking is not enabled for tables that are reported by a ADHP190W message.
 - The obid/dbid for the object are checked for performance reasons.
 - If the object is dropped and then recreated, the policy must be reinstalled.

If the field values of the SQL event match corresponding filter values (blocking rule conditions) in the blocking policy, then the SQL statements are blocked and ended with a -807 error code.

For more information about creating, activating, and inactivating blocking policies from the IBM Guardium system interface, refer to the Security Guardium documentation in the IBM Knowledge Center.

Enable or disable blocking on the host

If permitted, you can enable blocking, disable blocking, or report the blocking status (enabled or disabled) by using the following operator commands:

- **/F <adhstc>,BLOCKING ENABLE**
- **/F <adhstc>,BLOCKING DISABLE**
- **/F <adhstc>,BLOCKING STATUS**

These commands override and determine the blocking status whether or not a blocking policy is present. By default, blocking is enabled at startup; but if you use the **/F <adhstc>,BLOCKING DISABLE** command and push down blocking rules, the blocking rules will be processed and blocking will be established within the z/OS agent, but blocking will not be enabled. If you use the **/F <adhstc>,BLOCKING ENABLE** command, blocking is not activated until a blocking policy is pushed down.

The ADHPARMS z/OS collector agent parameter, **STAP_BLOCKING**, controls whether the blocking operator command is permitted and whether blocking is enabled or disabled. For more information about **STAP_BLOCKING**, see [“Collector agent parameters” on page 31](#).

Controlling host variable collection

IBM Guardium S-TAP for Db2 enables you to specify, on a per-rule basis, whether host variable information will be sent to the appliance for activity that matches that rule.

In the Guardium appliance interface, specify whether host variable information should be sent to the appliance for activity that matches a rule. When host variable collection is enabled, up to 256 bytes per variable of host variable data is sent to the Guardium appliance. For enhanced security of Personally Identifiable Information (PII), host variables are not collected by default in IBM Guardium S-TAP for Db2 V10.0 and later.

In the Guardium appliance interface, specify whether host variable information should be sent to the appliance for activity that matches a rule.

The Guardium appliance interface can be overridden by the **FORCE_LOG_LIMITED** parameter. This parameter enables you to restrict the collection of personal data by controlling whether the active policy controls the collection of host variables.

- If **FORCE_LOG_LIMITED** is set to *Y*, the policy setting for the collection of host variables is ignored, and host variables are not collected.
- If **FORCE_LOG_LIMITED** is set to *N*, the collection of host variables is controlled by the host variable settings in the active policy.

For more information, see [Collector agent parameters](#).

Collecting Command activity by using the Audit SQL Collector

IBM Guardium S-TAP for Db2 enables you to collect Command activity by using the Audit SQL Collector.

Command events are not subjected to filtering. All command events are streamed directly to the Guardium appliance for post-collection filtering. All command events are streamed directly to the Guardium appliance for optional post-collection filtering.

Collecting SET CURRENT SQLID events by using the Audit SQL Collector

IBM Guardium S-TAP for Db2 V10.1.3 enables you to collect SET CURRENT SQLID events by using the Audit SQL Collector.

In IBM Guardium S-TAP for Db2 V10.1.3, IFI TRACE CLASS 7 is no longer enabled, and SET CURRENT SQLID events are automatically collected by using the Audit SQL Collector. SET CURRENT SQLID events are streamed to the Guardium appliance without being subjected to filtering.

Chapter 4. Reference information

These reference topics are designed to provide you with quick access to information about IBM Guardium S-TAP for Db2 sample library members, parameters, and variables.

Topics:

- [“Sample library members” on page 27](#)
- [“Collector agent parameters” on page 31](#)
- [“Collector agent sample parameter file” on page 45](#)
- [“ADHEMAC1 edit macro variables” on page 46](#)

Other resources

The following IBM documentation provides more information about configuring and operating this product.

- [IBM Ported Tools for z/OS: Open SSH User's Guide](#)
- [z/OS UNIX System Services Planning](#)
- [z/OS MVS JCL User's Guide](#)
- [Db2 Administration Guide](#)
- [Monitoring and Tuning Db2 Performance](#)

Sample library members

Use the following sample library members that are included with IBM Guardium S-TAP for Db2 for installation and configuration.

Table 6. Installation and configuration sample library members		
Member	Type	Description
ADHBIND	JCL	Bind job used to bind DBRMs.
ADHBINDB	JCL	Bind job used to bind packages.
ADHCFGF	80-byte sequential or partitioned data set	A listing of required parameters that control how the collector is implemented.
ADHCFGPE	80-byte sequential or partitioned data set	A listing of optional parameters that control how the collector is implemented.
ADHCSSID	Procedure	IBM Guardium S-TAP for Db2 collector started task procedure. Runs an instance of the IBM Guardium S-TAP for Db2 collector started task.
ADHGRANT	JCL	Grants required authorizations to USERID and PLAN .
ADHEMAC1	(edit macro)	Customizes the variables that appear in the DDL and JCL to be run.
ADHMSTR	JCL	Stops the IBM Guardium S-TAP for Db2 master address space.

Table 6. Installation and configuration sample library members (continued)

Member	Type	Description
ADHSJ000	JCL	Allocates VSAM product control file.
ADHSJ001	JCL	Sets product configuration options.
ADHSJ003	JCL	Generates the product control file content report.
ADHSTAPD	JCL	Produces an IBM Guardium S-TAP for Db2 diagnostic report.
ADHTCPD	JCL	Produces a TCP/IP diagnostic report to use for troubleshooting network connectivity and throughput issues.

Related tasks

Defining the collector agent started task JCL

The collector agent runs as a started task. The sample library member ADHCSSID contains the sample JCL to set up the IBM Guardium S-TAP for Db2 collector agent started task.

MODIFY command

The **MODIFY** command allows you to issue requests against, and dynamically change, characteristics of an active S-TAP task.

The abbreviated version of the **MODIFY** command is the letter F. The general format of **MODIFY** is as follows:

```
>>--MODIFY+---procname--,--parameter-----><
      '-F-----'
```

wherein:

procname

The name of the member in a procedure library that was used to start the server or address space.

parameter

Any of the parameters that are valid for the server.

S-TAP supported MODIFY options with descriptions

The following is a sample syntax diagram:

```
>>--MODIFY+---procname,--+STAP+-----+
      |                                     |
      |      +- ,HELP -----|
      |      +- ,ALL-----|
      |      +- ,POLICY-----|
      |      +- ,COUNTS-----|
      |      +- ,CONFIG-----|
      |      +- ,HISTORY_QUEUE--|
      |      +- ,HISTORY_FILTER-|
      |      +- ,HISTORY_IO-----|
      |      +- ,BLOCKING-----|
      |      +- ,QUARANTINE-----|
      |      +- ,GET_STATUS-----|
      |      +- BLOCKING--+ ENABLED-----|
      |      |             +- DISABLED---|
      |      |             +- STATUS-----|
      |      +- ,MUSTGATHER-----|
      |      +- ,TRACE_POLICY,ENABLE----|
      |      +- ,TRACE_POLICY,DISABLE---|
      |      +- ,TRACE_COMPILE,ENABLE---|
      |      +- ,TRACE_COMPILE,DISABLE--|
      |      +- ,TRACE_PROTOBUF,ENABLE--|
      |      +- ,TRACE_PROTOBUF,DISABLE-|
      |      +- ,LOG_EVENTS,ENABLE-----|
      |      +- ,LOG_EVENTS,DISABLE-----|
      |      +- ,LOG_LEVEL,F|I|W|E|S----|
      |      +- ,RESET_CONFIG-----|
```

Note the space (rather than the comma) before BLOCKING ENABLED, DISABLED, and STATUS.

Options are defined as follows:

HELP

Display all available commands

STAP

Display the current status of the started task

ALL

View all log information

POLICY

View log information about the active policy

COUNTS

View a log of detailed counts

CONFIG

View a log about the current configuration

HISTORY_QUEUE

View log details about the internal events queue

HISTORY_FILTER

View log information about event filter results

HISTORY_IO

View log details about the streaming of events

BLOCKING

View log information about the active blocking policy

QUARANTINE

View log information about the active quarantine policy

GET STATUS

Request the most recent count of events that were received/processed by the appliance

BLOCKING

ENABLED: Enable the blocking feature. Blocking is activated if a blocking rule is pushed.

DISABLED: Disable the blocking feature.

STATUS: Display blocking status.

MUSTGATHER

Send a must-gather request to the appliance

TRACE_POLICY,ENABLE

View information about the policy component

TRACE_POLICY,DISABLE

Hide information about the policy component

TRACE_COMPILE,ENABLE

View information about the filter component

TRACE_COMPILE,DISABLE

Hide information about the filter component

TRACE_PROTOBUF,ENABLE

View information about the streaming component

TRACE_PROTOBUF,DISABLE

Hide information about the streaming component

LOG_EVENTS,ENABLE

Log events that are streamed to the appliance

LOG_EVENTS,DISABLE

Hide events that are streamed to the appliance

LOG_LEVEL,F|I|W|E|S

Control the amount of output log information that is generated by the agent: debugging, informational, warning, error, severe

RESET_CONFIG

Reset agent configurations to the default settings

The following example displays the active S-TAP policy:

F ADHPROC, STAP, POLICY

```
ADHP110I IBM Security Guardium DB2 S-TAP mode: STREAMING EVENTS
ADHP140I Event Counts:
ADHP141I CONNTYPE_OTHER (0) . . . . . 1
ADHP141I CONNTYPE_TSO (1) . . . . . 0
ADHP141I CONNTYPE_CALL_ATTACH (2) . . . . . 0
ADHP141I CONNTYPE_DLI_BATCH (3) . . . . . 0
ADHP141I CONNTYPE_CICS_ATTACH (4) . . . . . 0
ADHP141I CONNTYPE_IMS_ATTACH_BMP (5) . . . . . 0
ADHP141I CONNTYPE_IMS_ATTACH_MPP (6) . . . . . 0
ADHP141I CONNTYPE_DB2_PRIVATE_PROTOCOL (7) . . . . . 0
ADHP141I CONNTYPE_DRDA_PROTOCOL (8) . . . . . 0
ADHP141I CONNTYPE_IMS_CONTROL_REGION (9) . . . . . 0
ADHP141I CONNTYPE_IMS_TRANSACTION_BMP (10) . . . . . 0
ADHP141I CONNTYPE_DB2_UTILITIES (11) . . . . . 0
ADHP141I CONNTYPE_RRSF (12) . . . . . 0
ADHP142I MISC sent . . . . . 0
ADHP142I UTILITY sent . . . . . 0
ADHP142I DB2 COMMAND sent . . . . . 1
ADHP142I SELECT sent . . . . . 0
ADHP142I UPDATE sent . . . . . 0
ADHP142I DELETE sent . . . . . 0
ADHP142I INSERT sent . . . . . 0
ADHP142I REVOKE sent . . . . . 0
ADHP142I GRANT sent . . . . . 0
ADHP142I COMMIT-ROLLBACK sent . . . . . 0
ADHP142I BIND-REBIND sent . . . . . 0
ADHP142I FAILED_SQLCODE sent . . . . . 0
ADHP143I ALTER sent . . . . . 0
ADHP143I DROP sent . . . . . 0
ADHP143I CREATE sent . . . . . 0
ADHP144I Bytes sent . . . . . 363
ADHP145I Events Sent . . . . . 1
ADHP146I Statements processed . . . . . 0
ADHP140I Event Counts:
ADHQ3270I STAP INFO: STAGE1 FILTER IS..... ACTIVE
ADHQ3270I STAP INFO: STAGE2 FILTER IS..... NOTACTIV
ADHQ3270I STAP INFO: TOTAL EXEC SQL CALLS SEEN..... 0000000000000000
ADHQ3270I STAP INFO: STMTS PASSED STAGE1 FILTER.... 0000000000000000
ADHQ3270I STAP INFO: STMTS FAILED STAGE1 FILTER.... 0000000000000000
ADHQ3270I STAP INFO: STMTS PASSED, STAGE1 BYPASSED. 0000000000000000
ADHQ3270I STAP INFO: AUDS BLOCKS QUEUED..... 0000000000000000
ADHQ3270I STAP INFO: AUDS BLOCKS SENT TO APPLIANCE.. 0000000000000001
ADHQ3270I STAP INFO: AUDS BLOCKS NOT SENT TO APPL... 0000000000000000
ADHQ3270I STAP INFO: AUDS BLOCKS FREED ..... 0000000000000000
ADHQ3270I STAP INFO: AUDS BLOCKS FREED LOST ..... 0000000000000000
ADHQ3270I STAP INFO: BYTES SENT..... 000000000000016B
ADHQ3270I STAP INFO: UTILITY EVENTS QUEUED..... 0000000000000000
ADHQ3270I STAP INFO: UTILITY EVENTS FREED..... 0000000000000000
ADHQ3270I STAP INFO: UTILITY REQ COUNT..... 0000000000000000
```

The following example displays the S-TAP blocking status:

F ADHPROC, STAP, POLICY

```
ADHQ9899I - BLOCKING STATUS
ADHQ2023I - AUTHID BLOCKING IS ENABLED
ADHQ2034I - BLOCK TABLE 181_9901F000 HASH TABLES 181_99101000 SQLHS 1E8B6000

<policy>
  <selectblocking-rule>
    <target>
      <schema>DBTROS</schema>
      <name>TABLE1</name>
    </target>
    <target>
      <schema>DBTROS</schema>
      <name>TABLE2</name>
```

```
</target>
</selectblocking-rule>
</policy>
```

The following example displays the results of S_TAP GET_STATUS:

```
F ADHPROC,STAP,GET STATUS
ADHP170I - Event count reported by the appliance at time: 112
```

Requesting and viewing S-TAP logging information

Use the **S-TAP Logging** command to issue a request for logging information from the S-TAP agent collector.

About this task

From the **S-TAP control** panel of the IBM Guardium system interface:

Procedure

1. Locate the policy component for your S-TAP (for example, RS22:A91A:POLICY) and select the **G** icon.
2. Select **STAP Logging** for Command.
3. Select a logging level and click **Apply** to request S-TAP logging.
S-TAP logging levels provide log information as follows:

Level 0

Logs program levels, event queue statistics, agent configuration, policy, and event counts.

Level 1

Logs agent configuration, policy, and event counts.

Level 2

Logs agent configuration.

Level 3

Logs policy.

Level 4 or higher

Logs event counts.

4. To view the S-TAP logging information, locate the policy component of your S-TAP and click the **i** icon.

Collector agent parameters

The collector agent parameters are described in this section.

APPLIANCE_CONNECT_RETRY_COUNT

Required: No

Default: 0

Description: The number of consecutive failed connection attempts before terminating. The value of 0 indicates to never stop attempting connections. A value of 1 indicates a stop immediately after connection attempt fails. Range: 0 - 99999.

Syntax:

```
APPLIANCE_CONNECT_RETRY_COUNT(retry_count)
```

Example:

```
APPLIANCE_CONNECT_RETRY_COUNT(1000)
```

APPLIANCE_NETWORK_REQUEST_TIMEOUT

Default: 0

Range: 0 or 500 - 12000

Description: The value in milliseconds of the period of time to wait for network communication request send or receive to complete. A value of 0 results in no timeout period.

Syntax:

```
APPLIANCE_NETWORK_REQUEST_TIMEOUT(timeout)
```

Example:

```
APPLIANCE_NETWORK_REQUEST_TIMEOUT(0)
```

APPLIANCE_PING_RATE

Required: No

Default: 5

Description: Specifies the time interval between accesses to the Guardium system to prevent timeouts (disconnects) during idle periods. The value is in number of seconds.

Syntax:

```
APPLIANCE_PING_RATE(ping_interval)
```

Example:

```
APPLIANCE_PING_RATE(5)
```

APPLIANCE_PORT

Required: No

Default: 16022

Valid ports: 16022 or 16023

Description: The IP port number of the Guardium system to which the IBM Guardium S-TAP for Db2 audit data collector should connect. This parameter must be properly configured to enable collection of audit data and a connection to the IBM Guardium system. If port 16023 is used, encryption support is required for the connection to the appliance.

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

Syntax:

```
APPLIANCE_PORT(port_number)
```

Example:

```
APPLIANCE_PORT(16022)
```

APPLIANCE_RETRY_INTERVAL

Required: No

Default: 3

Description: Specifies the time interval between attempts to establish a connection to the IBM Guardium system. The value is in number of seconds.

Syntax:

```
APPLIANCE_RETRY_INTERVAL(retry_interval)
```

Example:

```
APPLIANCE_RETRY_INTERVAL(3)
```

APPLIANCE_SERVER**Required:** Yes**Default:** None

Description: The host name or IP address (in dotted-decimal notation, for example: 1.2.3.4) of the IBM Guardium system to which the IBM Guardium S-TAP for Db2 audit data collector should connect.

Note: This parameter must be properly configured to enable collection of audit data, and a connection to the IBM Guardium system. The value can contain up to 128 characters.

Syntax:

```
APPLIANCE_SERVER(hostname|ip_address)
```

Example:

```
APPLIANCE_SERVER(192.168.2.205)
```

APPLIANCE_SERVER_FAILOVER_[1-5]**Required:** No**Default:** None

Description: The host name or IP address (in dotted-decimal notation, for example: 1.2.3.4) of the IBM Guardium system to which the IBM Guardium S-TAP for Db2 audit data collector should fail over to if APPLIANCE_SERVER is not available.

Note:

1. This parameter must be properly configured to enable collection of audit data and a connection to the IBM Guardium system. The value can contain up to 128 characters.
2. The collector agent attempts to connect to the fail over systems beginning with APPLIANCE_SERVER_FAILOVER_1, and ending with APPLIANCE_SERVER_FAILOVER_5.
3. Both the **APPLIANCE_SERVER_FAILOVER_[1-5]** and **APPLIANCE_SERVER_[1-5]** parameters can be used to designate servers for multistreaming or failover. Use the **APPLIANCE_SERVER_LIST(MULTI_STREAM|FAILOVER)** parameter to designate how these parameters are used.

Syntax:

```
APPLIANCE_SERVER_FAILOVER_1(hostname|ip_address)
```

Example parameter settings to enable multistream support:

```
APPLIANCE_SERVER_LIST(MULTI_STREAM)
APPLIANCE_SERVER(guardium1.company.com)
APPLIANCE_SERVER_1(guardium2.company.com)
APPLIANCE_SERVER_2(guardium3.company.com)
```

APPLIANCE_SERVER_LIST(FAILOVER|MULTI_STREAM|HOT_FAILOVER)**Required:** No**Default:** FAILOVER

Description: If set to MULTI_STREAM, this parameter specifies that a Guardium appliance connection is to be established for each server that is identified by the **APPLIANCE_SERVER_n** parameter.

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

If set to FAILOVER, this parameter specifies that one Guardium appliance connection is to be active at a time.

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

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

If set to **HOT_FAILOVER**, this parameter causes all connection types (POLICY and ASC) for each connected Guardium appliance to be kept active by pings. You can specify the primary Guardium appliance by using the **APPLIANCE_SERVER** parameter. If the primary Guardium appliance becomes unavailable and failover occurs, **HOT_FAILOVER** maintains the activity of the primary appliance policy.

Syntax:

```
APPLIANCE_SERVER_LIST_FAILOVER
```

Example:

```
APPLIANCE_SERVER_LIST_FAILOVER
```

AUDIT

Required: Yes

Default: None

Description: The Db2 subsystem ID for the Db2 subsystem on which the IBM Guardium S-TAP for Db2 Collector Agent should capture query data.

Note: This parameter must be properly configured to enable collection of capture data. The value can contain up to 4 characters.

Syntax:

```
AUDIT(ssid)
```

Example:

```
AUDIT(DSN1)
```

AUTHID

Required: No

Default: Defaults to the user ID under which the started task will run.

Description: The AUTHID parameter defines the Db2 AUTHID that IBM Guardium S-TAP for Db2 uses when establishing a connection to Db2 during interval processing. If you are using RACF on your Db2 system, this ID must be defined to RACF. The AUTHID specified needs to be authorized through the resident security package, such as RACF, to perform the functions needed for all processes done by

the started task and the Collector Agent monitoring subsystem. Such processes include connecting to each of the monitored Db2 SSIDs and performing file update activities against the IBM Guardium S-TAP for Db2 VSAM control file.

Notes:

1. The ID specified in the startup parameter AUTHID must be a valid TSO user ID and not a RACF group name.
2. If the AUTHID parameter is defined in the RACF Started Procedures Table (ICHRIN03), it should not be used as a startup parameter. The Started Procedures Table (ICHRIN03) associates the names of started procedures with specific RACF user IDs and group names. It can also contain a generic entry that assigns a user ID or group name to any started task that does not have a matching entry in the table. However, it is recommended that you use the STARTED class for most cases rather than the started procedures table.

Syntax:

```
AUTHID(db2authid)
```

Where *db2authid* is the Db2 AUTHID that IBM Guardium S-TAP for Db2 uses when establishing a connection to Db2 during interval processing.

Example:

```
AUTHID(DB2USER)
```

CICS_USERID

Required: No

Default: N

Description: If set to Y, the **CICS_USERID** parameter enables the capture of CICS Login User ID for SQL statements that are run in Db2 for CICS. For more information see [“Enabling CICS Login User ID reporting”](#) on page 15.

Syntax:

```
CICS_USERID(Y|N)
```

Example:

```
CICS_USERID(Y)
```

COLLECT_COMMIT_ROLLBACK

Required: No

Default: N

Description: If set to Y, the **COLLECT_COMMIT_ROLLBACK** parameter enables the collection of COMMIT and ROLLBACK events.

Syntax:

```
COLLECT_COMMIT_ROLLBACK(Y|N)
```

Example:

```
COLLECT_COMMIT_ROLLBACK(Y)
```

DEBUG

Required: No

Default: N

Description: The DEBUG parameter turns on debug mode and produces diagnostic messages for use by IBM Software Support.

Syntax:

```
DEBUG (YES | NO)
```

Example:

```
DEBUG (Y)
```

FORCE

Required: No

Default: N

Description: The FORCE parameter forces installation of a monitoring agent. If you use this parameter, any return codes from any failure reported in message ADHQ2002E are overridden.

Note: This parameter should not be specified without instruction by IBM Software Support.

Syntax:

```
FORCE (YES | NO)
```

Example:

```
FORCE (Y)
```

FORCE_LOG_LIMITED

Required: No

Default: N

Description: This parameter enables you to restrict the collection of sensitive data by controlling whether the active policy controls the collection of host variables.

If this parameter is set to Y:

- The policy setting for collection of host variables is ignored and host variables are not collected.
- The **APPLIANCE_PORT** parameter must be set to 16023. Port 16023 is used for AT-TLS-configured encrypted communications. If APPLIANCE_PORT is not set to 16023, the S-TAP agent will generate a log message indicating the configuration inconsistency, and shut down.

If this parameter is set to N, the collection of host variables is controlled by the host variable settings in the active policy.

Syntax:

```
FORCE_LOG_LIMITED (YES | NO)
```

Example:

```
FORCE_LOG_LIMITED (Y)
```

HOSTVAR_LIMIT

Required: No

Default: 1500

Description: This parameter designates the number of storage blocks to be allocated for host variable collection per event. The valid range is 1 -- 9999. If this parameter is not customized, the default value of 1500 is set.

If error message ADHQ1203I is encountered with RC=0008 and RSN=003F, increase the HOSTVAR_LIMIT setting to accommodate the collection of host variables for the monitored workload.

If IBM Guardium S-TAP for Db2 and IBM Db2 Query Monitor for z/OS are simultaneously monitoring the same Db2 subsystem, both products must have matching HOSTVAR_LIMIT settings to avoid receiving a mismatch error.

Syntax:

```
HOSTVAR_LIMIT(n)
```

where *n* is an integer between 1 - 9999.

Example:

```
HOSTVAR_LIMIT(1500)
```

ISM_CONSTRAINT_AGE

Required: No

Default: 300

Description: This parameter controls how much time must have passed since the last storage constraint occurrence for a given ISM storage space before the constraint event is considered to have been relieved.

Syntax:

```
ISM_CONSTRAINT_AGE(n)
```

where *n* is an integer between 1 - 60000 specified in .01 seconds. The default value is 300.

Example:

```
ISM_CONSTRAINT_AGE(16)
```

ISM_ERROR_DETAIL

Required: No

Default: Y

Description: This parameter controls whether messages ADHQ1203I and ADHQ1204I are issued to provide detailed information for ISM Storage Constraint situations. The product recommendation is to leave this parameter set to **Y**. This setting can be overridden at run time with the **/f cqmstc, ISMERROR_DETAIL** command.

Syntax:

```
ISM_ERROR_DETAIL(Y|N)
```

Example:

```
ISM_ERROR_DETAIL(Y)
```

ISM_ERROR_BLOCKS

Required: No

Default: 256

Description: This parameter determines the number of ISM Error Blocks that are allocated when IBM Guardium S-TAP for Db2 initializes.

If this value is too low, message ADHQ1219W might be issued. ISM Error Blocks communicate a storage constraint event from somewhere in the product to the task that issues storage constraint messages. If you run out of ISM Error Blocks, the storage constraint message will not be issued.

However, an abend table entry will be created to document this event. This is most likely a temporary situation and it does not impact the overall performance of IBM Guardium S-TAP for Db2.

Syntax:

```
ISM_ERROR_BLOCKS(n)
```

where *n* is an integer, 16 - 8192. The default value is 256.

Example:

```
ISM_ERROR_BLOCKS(256)
```

ISM_ERROR_MSG_BLOCKS

Required: No

Default: 256

Description: This parameter determines the number of ISM Error Message Blocks that are allocated when IBM Guardium S-TAP for Db2 initializes. If this value is too low, duplicate ISM error message can be issued for the same space and reason instead of incrementing the occurrence count.

ISM Error Message Blocks are used by the task that issues storage constraint messages to do two things:

1. To consolidate similar storage constraint events to eliminate duplicate messaging for the same condition, and
2. To keep track of storage constraint events so that the Storage Constraint Relieved situation can be detected and messaged.

If you run out of ISM Error Message Blocks, this consolidation will not always occur. This would result in additional, duplicate messages in the log for the similar storage constraint events.

Syntax:

```
ISM_ERROR_MSG_BLOCKS(n)
```

where *n* is an integer between 16 - 8192. The default value is 256.

Example:

```
ISM_ERROR_MSG_BLOCKS(256)
```

MASTER_PROCNAME

Required: Yes

Default: None.

Description: The MASTER_PROCNAME parameter enables users to specify the PROCNAME to be used for the Master Address Space. Specifying this parameter causes IBM Guardium S-TAP for Db2 to use the Master Address Space with the same name.

- The MASTER_PROCNAME for IBM Guardium S-TAP for Db2 and Query Monitor must be the same when each is started at the same time for the same Db2 Subsystem.
- If this Master Address Space is already started, it is shared with other IBM Guardium S-TAP for Db2 subsystems that are already using it.
- If this Master Address Space has not already been started, it will start automatically.

Syntax:

```
MASTER_PROCNAME(procname)
```

where *procname* is the specified Master Address Space PROCNAME (character, 8 bytes.)

Example:

```
MASTER_PROCNAME(CQMMASSTR)
```

MAXIMUM_ALLOCATIONS**Required:** No**Default:** 2048

Description: This parameter determines the maximum amount of global shared memory to be allocated by IBM Guardium S-TAP for Db2 for internal Integrated Storage Manager spaces.

Syntax:

```
MAXIMUM_ALLOCATIONS(n)
```

where *n* is an integer between 512 - 32768 specified in megabytes; must be smaller than SMEM_SIZE.

Example:

```
MAXIMUM_ALLOCATIONS(2048)
```

MESSAGE_LOG_LEVEL**Required:** No**Default:** I

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

I

Includes all log messages with an *informational* severity or higher

W

Includes all log messages with a *warning* severity or higher

E

Includes all log messages with an *error* severity or higher

S

Includes all log messages with a *severe* severity or higher

The ADHPARMS file is read when the agent is started. Modifying the log-level setting in the ADHPARMS file does not implement the new setting until you restart the collector agent.

Note: During installation, it is recommended that you set the MESSAGE_LOG_LEVEL to I.

Syntax:

```
MESSAGE_LOG_LEVEL(I/W/E/S)
```

Example:

```
MESSAGE_LOG_LEVEL(I)
```

OUTAGE_SPILLAREA_SIZE**Required:** No**Default:** 0

Description: This parameter determines the maximum amount of memory to be allocated to support the retention of audit data in the event of a Guardium system connection outage.

Note: A value of 0 disables spillfile support. When enabled, OUTAGE_SPILLAREA_SIZE supersedes SEND_FAIL_EVENT_COUNT for temporary data retention.

Syntax:

```
OUTAGE_SPILLAREA_SIZE(n)
```

where *n* is an integer between 0 - 1024 specified in megabytes.

Example:

```
OUTAGE_SPILLAREA_SIZE(2)
```

PREFER_IPV4_STACK

Required: No

Default: N

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

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

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

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

Note: Whether or not this parameter is used, if the address returned from the DNS is not valid for the hostname, it will result in failure to connect to the appliance, and the IBM Guardium S-TAP for Db2 started task will terminate.

Syntax:

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

Example:

```
PREFER_IYP4_STACK(Y)
```

SEND_FAIL_EVENT_COUNT

Required: No

Default: 100

Description: Specifies the maximum number of events to be buffered during a communication outage with the Guardium system. Events are buffered in internal memory objects and streamed to the appliance at the time of reconnection.

Note: SEND_FAIL_EVENT_COUNT and OUTAGE_SPILLAREA_SIZE are mutually exclusive. When OUTAGE_SPILLAREA_SIZE is specified, spillfile support is enabled, which supersedes SEND_FAIL_EVENT_COUNT for temporary data retention.

Syntax:

```
SEND_FAIL_EVENT_COUNT (event_count)
```

where *event_count* is an integer between 0 – 1024 that represents the number of events to be buffered.

Example:

```
SEND_FAIL_EVENT_COUNT(100)
```

SMEM_SIZE(5|n)

Required: No

Default: 5

Description: This parameter determines the maximum amount global shared memory to be allocated by IBM Guardium S-TAP for Db2 for all purposes.

Syntax:

```
SMEM_SIZE(n)
```

where *n* is an integer between 3 - 32 specified in gigabytes; must be three times larger than MAXIMUM_ALLOCATIONS.

Example:

```
SMEM_SIZE(5)
```

STAP_BLOCKING

Required: No

Default: ENABLED

Description: The STAP_BLOCKING parameter controls whether blocking is enabled or disabled and whether the blocking operator command is permitted to enable, disable, or report status for blocking. This parameter cannot be overwritten by the BLOCKING operator command. STAP_BLOCKING parameter options are as follows:

- STAP_BLOCKING(ENABLED) enables the blocking feature. Blocking is activated if a blocking rule is pushed.
- STAP_BLOCKING(DISABLED) disables the blocking feature.
- STAP_BLOCKING(OPERATOR) enables the blocking feature and enables the BLOCKING operator command. Blocking is activated if a blocking rule is pushed.

Syntax: STAP_BLOCKING(ENABLED|DISABLED|OPERATOR)

Example: STAP_BLOCKING(ENABLED)

STAP_MEGABUFFER

Required: No

Default: Y

Description: When multiple IBM Guardium S-TAP for Db2 audit events are accumulated in a buffer, it is referred to as a megabuffer. A megabuffer reduces the CPU usage that is related to TCP/IP activity. To optimize IBM Guardium S-TAP for Db2 performance, **STAP_MEGABUFFER** must remain set to Y. However, **STAP_MEGABUFFER** can be set to N when buffering is not desired.

Setting the **STAP_MEGABUFFER** parameter to N eliminates buffering, and provides near real-time event streaming to the Guardium appliance. It also increases CPU usage, due to additional TCP/IP calls.

Syntax:

```
STAP_MEGABUFFER(Y|N)
```

Example:

```
STAP_MEGABUFFER(Y)
```

STAP_STREAM_EVENTS**Required:** No**Default:** Y

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

Syntax:

```
STAP_STREAM_EVENTS(Y|N)
```

Example:

```
STAP_STREAM_EVENTS(Y)
```

STAP_TERMINATE_OPTIMIZE**Required:** No**Default:** N

Description: This parameter can be used to improve the response time for processing **STAP_TERMINATE** requests from the Guardium appliance. Roundtrip time for **STAP_TERMINATE** activity is impacted by the **STAP_MEGABUFFER** parameter. **STAP_TERMINATE** policies require near real-time event recording to the IBM Guardium system to analyze events against the policy and issue the termination requests to IBM Guardium S-TAP for Db2. To enable near real-time event recording to the Guardium appliance, set the **STAP_MEGABUFFER** parameter to N.

Syntax:

```
STAP_TERMINATE_OPTIMIZE(Y|N)
```

Example:

```
STAP_TERMINATE_OPTIMIZE(N)
```

STAP_UTILITY_MULTITABLE**Required:** No**Default:** N

Description: The STAP_UTILITY_MULTITABLE parameter works in conjunction with the STAP_UTILITY_TS_TO_TABLE parameter. These parameters control how table information is reported for Db2 Utility access events that involve tablespaces. The STAP_UTILITY_MULTITABLE parameter controls the behavior of the collector when multiple tables are contained in the tablespace. When STAP_UTILITY_MULTITABLE is set to Y:

- The collector will report all tables in the tablespace that are impacted by the utility. This guarantees that tablespace access by a utility execution will result in an audit event against the table name.
- Tables within a tablespace, which were not accessed by the utility, might be reported.

When STAP_UTILITY_MULTITABLE is set to N, no attempt is made to report table information for multi-table tablespaces accessed by a utility. Only the tablespace name is reported.

Syntax:

```
STAP_UTILITY_MULTITABLE(Y|N)
```

Example:

```
STAP_UTILITY_MULTITABLE(N)
```

No table names are reported (default).

```
STAP_UTILITY_MULTITABLE(Y)
```

All table names are reported.

STAP_UTILITY_TS_TO_TABLE

Required: No

Default: Y

Description: The STAP_UTILITY_TS_TO_TABLE parameter controls how table information is reported for Db2 Utility accesses to tablespaces. When the parameter is set to Y, the collector queries the Db2 catalog. The collector then determines and reports on which table exists within the tablespace that has been accessed by the utility execution. If multiple tables are contained in the tablespace, the STAP_UTILITY_MULTITABLE parameter controls whether the collector reports either:

All tables

All table names in the accessed tablespace

No tables

Only the tablespace is reported.

This action is controlled by STAP_UTILITY_MULTITABLE parameter setting.

Syntax:

```
STAP_UTILITY_TS_TO_TABLE(Y|N)
```

Example:

```
STAP_UTILITY_TS_TO_TABLE(Y)
```

STARTUP_DIAGNOSTICS

Required: No

Default: N

Description: The STARTUP_DIAGNOSTICS parameter causes IBM Guardium S-TAP for Db2 to produce diagnostic information output during startup of the collector agent. This output might be useful to IBM Support when diagnosing reported problems.

Syntax:

```
STARTUP_DIAGNOSTICS(Y|N)
```

Example:

```
STARTUP_DIAGNOSTICS(Y)
```

SHUTDOWN_DIAGNOSTICS

Required: No

Default: N

Description: The SHUTDOWN_DIAGNOSTICS parameter causes IBM Guardium S-TAP for Db2 to produce diagnostic information output during shutdown (stop) of the collector agent. This output might be useful to IBM Support when diagnosing reported problems.

Syntax:

```
SHUTDOWN_DIAGNOSTICS(Y|N)
```

Example:

```
SHUTDOWN_DIAGNOSTICS(Y)
```

SUBSYS

Required: No

Default: The default value is the Db2 subsystem name.

Description: The SUBSYS parameter defines the SQL Collector subsystem name. The subsystem name does not need to correspond to a Db2 subsystem nor an MVS operating system name. The name must be 1-4 characters in length.

Syntax:

```
SUBSYS(ssid)
```

Where *ssid* is the 1-4 character SQL Collector subsystem name.

Note: The SQL Collector subsystem ID must be unique across the SYSPLEX. A SQL Collector component subsystem must be running on each LPAR that has a Db2 subsystem to be captured. When choosing a collector agent subsystem ID name, be sure it will not conflict with another on the SYSPLEX. If the specified SUBSYS is not unique across the SYSPLEX, message ADHQ1003E will be issued.

Example:

```
SUBSYS(ADH1)
```

TS_OFFSET(E|W.HH.MM)

Required: No

Default: None (no offset)

Description:

- This parameter enables you to adjust the event timestamps that are streamed to the appliance by specifying the amount of time to adjust (offset) based on timezone.
 - For example, if running with a clock that is set to UTC 0.0 in a timezone that it is UTC + 9, GMT can be considered 9 hours west of the current time. In this situation, the parameter should be set as follows: TS_OFFSET(W.09.00). Event timestamps will be adjusted (offset) by subtracting 9 hours from the original timestamp.
- If TS_OFFSET is not supplied, the timestamps that are streamed to the appliance are not adjusted based on timezone.

Syntax:

E|W

East or west offset from GMT

HH

Number of hours

MM

Number of minutes

Example: TS_OFFSET(W.09.00)

ZIIP_FILTER(Y|N)

Required: No

Default: ZIIP_FILTER(N)

Description:

- ZIIP_FILTER(Y) indicates that the z/OS image running the collector agent started task has an IBM System z® Integrated Information Processor (zIIP). In this case, allow collector agent to perform offload profile filtering to a zIIP.
- If ZIIP_FILTER(Y) is specified and the collector agent started task is running on a z/OS that has no zIIP, message ADHQ1060I is issued, indicating the WLM related service has failed. In this case, collector agent continues to run as if ZIIP_FILTER(N) were set.

Syntax: ZIIP_FILTER(Y)

Example: ZIIP_FILTER(Y)

ZIIP_TCP(Y|N)

Required: No

Default: ZIIP_TCP(N)

Description:

- ZIIP_TCP(Y) indicates that the z/OS image running the collector agent started task has an IBM System z Integrated Information Processor (zIIP). In this case, allow collector agent to offload TCP/IP message processing to a zIIP.
- If ZIIP_TCP(Y) is specified and the collector agent started task is running on a z/OS that has no zIIP, message ADHQ1060I is issued, indicating the WLM related service has failed. In this case, collector agent continues to run as if ZIIP_TCP(N) were set.

Note: ZIIP_TCP(Y) requires that zIIP filter support be enabled: ZIIP_FILTER(Y). If ZIIP_FILTER(N) and ZIIP_TCP(Y) are specified together, ZIIP_FILTER will be automatically set to Y.

Syntax: ZIIP_TCP(Y)

Example: ZIIP_TCP(Y)

/f cqmstc, ISMERROR_DETAIL(Y|N)

Description: This parameter controls whether ISM constraint message detail is on or off. When the parameter is specified, messages ADHQ1203I and ADHQ1204I are issued for ISM storage constraint situations.

Keeping connections active when HOT_FAILOVER is enabled

When the HOT_FAILOVER feature is enabled by the APPLIANCE_SERVER_LIST parameter, all connection types (POLICY and ASC) for each connected Guardium appliance are kept active by pings.

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

Collector agent sample parameter file

The following sample parameter file is the minimum set of parameters required in a collector agent parameter file (ADHCFGF). If you want to use this sample file, verify that the values on each parameter are appropriate for your environment.

```
- 5655-STP
- (C) COPYRIGHT ROCKET SOFTWARE, INC. 1999 - 2015 ALL RIGHTS RESERVED.
-
```

```

- MEMBER: ADHCFGP
-
- DESCRIPTION: THIS IS A SAMPLE MINIMUM ADHCFGP MEMBER
-               USED FOR IBM SECURITY GUARDIUM S-TAP for DB2 on z/OS
-               COLLECTOR AGENT STARTUP.
-               VERIFY THAT THE VALUES ON EACH PARM ARE APPROPRIATE
-               FOR YOUR ENVIRONMENT.
-
- NOTE:  AFTER USING THE EDIT MACRO, VERIFY THAT NONE OF THE
-         STATEMENTS EXCEED COLUMN 72 IN LENGTH.
-
-
SUBSYS(#SSID)           -
AUDIT(#SSID)           -
MASTER_PROCNAME(ADHMST31) -
APPLIANCE_SERVER(#APPSRV)

```

ADHEMAC1 edit macro variables

This table shows the ADHEMAC1 edit macro variables, including their default value and instructions for use. An example is also provided.

Table 7. ADHEMAC1 Edit macro variables		
Variable	Default	Instructions
#SSID	MYSSID	Change the default to a valid Db2 subsystem ID. Note: The ADHEMAC1 macro sets the SUBSYS parameter using the #SSID variable. Running the macro sets SUBSYS to the Db2 subsystem ID used by the collector agent task. Do not change the #SSID variable in the ADHEMAC1 macro to be anything other than the Db2 subsystem ID used by the collector agent task.
#ADHOWNER	&ZUSER	Change &ZUSER to the value of #ADHQUALIFIER. #ADHOWNER is used to configure the owner of the plans and packages. It is used as the owner value of objects created by statements contained within the package or plan.
#ADHQUALIFIER	SYSTOOLS	Change the default to the schema name being used with this product.
#ADHUSERID	&ZUSER	Use as the authorization ID for the collector agent task.
#SADHLOAD	ADH.IBMTAPE. SADHLOAD	Change the default to the data set containing the IBM Guardium S-TAP for Db2 load modules.
#SADHDBRM	ADH.IBMTAPE. SADHDBRM	Change the default to the data set containing the IBM Guardium S-TAP for Db2 DBRMs.
#SDSNLOAD	DSN.Vxxx.SDSNLOAD	Change the default to the data set containing the Db2 load modules.
#SDSNRUNL	DSN.Vxxx.RUNLIB.LOAD	Change the default to the data set containing the Db2 DSNTDP2 module.
#DSNTEP2	DSNTEP2	Change the default to the DSNTDP2 plan name.
ADHPLAN1	ADHPLAN1	Change the default to a valid plan name. This plan used to collect information about the Db2 System catalog during audit data collection.
#SZPARM	MYSSIDPARM	Change the default to the Db2 ZPARM member that is associated with the Db2 subsystem.
#SBSDS01	MYSSID.BSDS01	Change the default to the DSN of the bootstrap data set 01.
#SBSDS02	MYSSID.BSDS02	Change the default to the DSN of the bootstrap data set 02.
#SDSNEXIT	DSN.Vxxx.SDSNEXIT	Change the default to the data set containing the Db2 ZPARMs.

Table 7. ADHEMAC1 Edit macro variables (continued)

Variable	Default	Instructions
#SFECLOAD	None	Data set name of the required FEC load library.
#SCQCLOAD	None	Data set name of the required CQC load library.
#ADHCNTRLFILE	ADH.V0A00.CONTROL	Change the default to an appropriate DSN HLQ for the IBM Guardium S-TAP for Db2 VSAM Control file.
#APPSRVR	appliance.company.com	Host name or IP address of the IBM Guardium system.

The following example shows the contents of the ADHEMAC1 member:

```
ISREDIT MACRO (NP)
ISPEXEC VGET (ZUSER)
ISREDIT CHANGE ALL '#SSID' MYSSID
ISREDIT CHANGE ALL '#ADHOWNER' &ZUSER
ISREDIT CHANGE ALL '#ADHUSERID' &ZUSER
ISREDIT CHANGE ALL '#SADHLOAD' ADH.IBMTAPE.SADHLOAD
ISREDIT CHANGE ALL '#SADHDBRM' ADH.IBMTAPE.SADHDBRM
ISREDIT CHANGE ALL '#SDSNLOAD' DSN.Vxxx.SDSNLOAD
ISREDIT CHANGE ALL '#SDSNRUNL' DSNxxx.RUNLIB.LOAD
ISREDIT CHANGE ALL '#DSNTEP2' DSNTEP2
ISREDIT CHANGE ALL '#ADHPLAN1' ADHPLAN1
ISREDIT CHANGE ALL '#SZPARM' MYSSIDPARM
ISREDIT CHANGE ALL '#SBSDS01' MYSSID.BSDS01
ISREDIT CHANGE ALL '#SBSDS02' MYSSID.BSDS02
ISREDIT CHANGE ALL '#SDSNEXIT' DSN.Vxxx.SDSNEXIT
ISREDIT CHANGE ALL '#SFECLOAD' FEC.IBMTAPE.SFECLOAD
ISREDIT CHANGE ALL '#SCQCLOAD' CQC.IBMTAPE.SCQCLOAD
ISREDIT CHANGE ALL '#ADHCNTRLFILE' ADH.V0A00.CONTROL
ISREDIT CHANGE ALL '#APPSRVR' appliance.company.com
```

Related tasks

Customizing JCL members

Use the edit macro ADHEMAC1 to customize the variables in the JCL to be run. Running ADHEMAC1 allows you to modify members without requiring you to remember plan names, creators, and other variables from one editing session to the next editing session.

Chapter 5. Messages and codes for

These topics document the messages and error codes issued by . Messages are presented in ascending alphabetical and numerical order.

Error messages

messages adhere to the following format: ADHnnnx

Where:

ADH

Indicates that the message was issued by .

nnn

Indicates the message identification number.

x

Indicates the severity of the message:

Table 8. Error message severity codes	
Severity Code	Description
E	Indicates that an error occurred, which might or might not require operator intervention.
I	Indicates that the message is informational only.
S	Indicates that operator intervention is required before processing can continue.
W	Indicates that the message is a warning to alert you to a possible error condition.

Error messages and codes: ADHAxxx

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

ADHA507E	Callable service invocation failed with return code = rc and reason code = rs
-----------------	--

Explanation

A callable service invocation failed with a return code and reason code that are identified in the message.

User response

Refer to the *IBM Db2 for z/OS* product documentation for an explanation of this reason and return code.

Common causes of this error include:

Insufficient authorization to ADH PLAN specified in the control file

If either of these issues are indicated by the reason code, verify that SAMPLIB member ADHGRANT was customized and submitted during configuration of the IBM Guardium S-TAP for Db2 agent.

A DB2 Trace is currently running

Issue the Db2 command **-DISPLAY TRACE** to view info about any audit traces that might still be running. If audit traces are running, stop them by using the Db2 command **-STOP TRACE** and then restart the agent. If this does not resolve the problem, check for the existence of additional messages.

If the problem is not resolved after attempting all user responses for existing additional messages, contact IBM Software Support.

Error messages and codes: ADHGxxx

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

ADHG000I	Attempting connection to server server-address port=server-port
-----------------	--

Explanation:

The S-TAP collector will attempt to establish a TCP/IP connection to a Guardium system at the specified server address and port.

User response:

No action is required.

ADHG001I	Establishing ASC connection to server [server-address]
-----------------	---

Explanation:

The S-TAP collector is preparing to establish the TCP/IP connection to the specified Guardium system.

User response:

No action is required.

ADHG002I	Connection established to server [server-address]
-----------------	--

Explanation:

The S-TAP collector was successful in establishing a TCP/IP connection to the Guardium system.

User response:

No action is required.

ADHG003I	Connection re-established to [server-address]
-----------------	--

Explanation:

The S-TAP collector was successful in re-establishing a TCP/IP connection to the Guardium system following a disconnect.

User response:

No action is required.

ADHG004W	Connection was lost from server [server-address]
-----------------	---

Explanation:

The TCP/IP connection between the S-TAP collector and the Guardium system was lost. The S-TAP collector will automatically attempt to re-establish the connection, however a potential for data loss does exist if the connection is not re-established. A data loss condition is indicated by message ADHG006E.

User response:

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

ADHG005S	Unable to establish a connection to a server [server-address]
-----------------	--

Explanation:

The S-TAP collector was unable to establish a TCP/IP connection to the Guardium system.

User response

- Ensure that the Guardium system is listening for a connection at the server and port specified in message ADHG001I.
- Ensure that no firewalls are blocking connections between the collector and Guardium system.
- If port 16023 is used, ensure that AT-TLS has been configured properly between the z/OS LPAR and the appliance.

ADHG006E	Data loss has occurred as the result of a network send failure
-----------------	---

Explanation:

During a disconnected state, the S-TAP collector exceeded the number of events to retain in memory while waiting for the network connection to the Guardium system to be reestablished.

User response

- Determine the cause of the network interruption and correct the problem so that the connection can be reestablished.
- If deemed necessary, increase the SEND_FAIL_EVENT_COUNT value in the ASC ADHPARMS parameter file to increase the number of events that can be retained in memory during short outages.

ADHG007E	Unable to create a communications interface
-----------------	--

Explanation:

An attempt to create an internal communications interface failed.

User response:

Contact IBM Software Support.

ADHG008S	Required parameter was not supplied. Parameter=<i>parameter-name</i>
-----------------	---

Explanation:

A required parameter was not supplied.

User response:

Supply a parameter and value for the specified parameter.

ADHG009I	TCP/IP streaming disabled due to user setting.
-----------------	---

Explanation:

A debug setting was specified that has disabled TCP/IP streaming between the S-TAP collector and the Guardium appliance.

User response:

No action is required.

ADHG010I	Disconnecting from server <i>server-name</i>
-----------------	---

Explanation:

The S-TAP collector is disconnecting from the Guardium system.

User response:

No action is required.

ADHG011E	Unable to create an output stream
-----------------	--

Explanation:

An attempt to create an internal output stream failed.

User response:

Contact IBM Customer Support.

ADHG012E	Unable to set socket timeout value. rc=<i>return-code</i> reason=<i>reason-code</i>
-----------------	--

Explanation:

An attempt to set the timeout threshold in the socket interface failed.

User response:

Contact IBM Customer Support.

ADHG013I	Connection attempt timed out. Reattempting connection <i>reattempt-number</i> of total- <i>re-attempts</i>
-----------------	---

Explanation:

The S-TAP collector agent was unable to establish a TCP/IP connection to the Guardium system within the timeout period. The connection will be reattempted

until the *reattempt-number* specified meets the *total-re-attempts* number specified.

User response

- Ensure that the Guardium system is listening for a connection at the server and port specified in message ADHG001I.
- Ensure that there no firewalls are blocking connections between the collector and Guardium system.

ADHG014I	Spillfile support enabled. Spill area size: [<i>size</i>] MB
-----------------	---

Explanation:

A spillfile area was successfully allocated at the specified size.

User response:

No action is required.

ADHG015W	Primary server is unavailable
-----------------	--------------------------------------

Explanation:

A connection to the primary Guardium system is not available. Failover systems will be attempted for connection.

User response:

Determine the cause of the connection interruption to the primary Guardium system and attempt to restore the connection.

ADHG017W	Data is being temporarily stored in a spillfile until a connection is re-established
-----------------	---

Explanation:

A Guardium system connection is unavailable. Collected data is written to the spillfile area until a system connection can be established.

User response:

Determine the cause of the system connection outage and attempt to restore the connection.

ADHG018I	Spillfile contents have been successfully be sent to server [<i>server</i>]
-----------------	--

Explanation:

The Guardium system connection has been restored. The spillfile data that was collected during a connection outage has been sent to the specified system.

User response:

No action is required.

ADHG019S	Spillfile storage has been exhausted. Data loss will occur.
-----------------	--

Explanation:

A Guardium system connection is unavailable and the spillfile is out of space. Data collected after this time will be lost.

User response:

Determine the cause of the connection outage to the system and attempt to restore the connection. Notify others of the outage as necessary.

ADHG020I Registering server [server] as eligible for failover.

Explanation:

The specified server will be added to the list of failover servers to register for the connection. Registration is attempted after all failover servers have been added. A successful failover registration is indicated by message ADHG012I.

User response:

No action is required.

ADHG021E Spillfile is approaching [50% | 85% | 95% | 100\$] capacity.

Explanation:

A Guardium system connection is unavailable and the spillfile area is at the specified capacity.

User response:

Determine the cause of the connection outage to the system and attempt to restore the connection.

ADHG022I A connection has been established to failover server [server].

Explanation:

A connection to the primary Guardium system is not available. A connection has successfully been established to one of the specified failover server.

User response:

Determine the cause of the connection interruption to the primary system and attempt to restore the connection.

ADHG026W Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.

Explanation:

The APPLIANCE_PORT parameter currently supports a setting of 16022, but the parameter has been retained for future support. If APPLIANCE_PORT is specified with a value other than 16022, message ADHG026W is issued, and port 16022 will be used instead.

User response:

Change APPLIANCE_PORT parameter setting to 16022 or remove the parameter entirely.

ADHG027I Registering server server as eligible for multi-stream.

Explanation:

The specified server will be added to the list of servers that are eligible for multistream support.

User response:

No action is required.

ADHG030I Collector Agent is terminating

Explanation:

The collector is terminating.

User response:

No action is required.

ADHG031I V10.1.3 [component] connection established

Explanation:

The specified component successfully established a TCP/IP connection to the Guardium system.

User response:

No action is required.

ADHG097E Unexpected error: [error_description]. Return code: [return_code].

Explanation:

An unexpected error was encountered.

User response:

Contact IBM Software Support.

ADHG098I This event will be logged due to an unexpected data condition.

Explanation:

A collected event contained unexpected or invalid data fields. The event fields are written to DD:ADHLOG for use in diagnosing the problem.

User response:

Contact IBM Software Support with the error log.

ADHG099E Unexpected error: error-condition

Explanation:

An unexpected error was encountered.

User response:

Contact IBM Software Support.

ADHG210I A thread termination request was received for thread [thread-token]

Explanation:

A **-CANCEL THREAD** command was issued by as a result of a request received by the Guardium system. The command ended successfully. *Thread-token* represents the cancelled thread token, as would be reported by a **-DISPLAY THREAD DB2** command.

User response:

No action is required.

ADHG501E pbSend: Bad host name. code=error-code

Explanation:

While sending a message, the socket interface encountered a bad host name condition.

User response

- Verify that the host name value provided for APPLIANCE_SERVER in the ASC ADHPARMS parameter file is valid.
- Contact IBM Software Support.

ADHG502E pbSend: Interface not open. code= error-code

Explanation:

While sending a message, a problem was encountered with an internal interface.

User response:

Contact IBM Software Support.

ADHG503E pbSend: Socket I/O problem. code= error-code

Explanation:

While sending a message, the socket interface encountered a socket I/O problem.

User response:

Contact IBM Software Support.

ADHG550E Unable to send message. Connection to server is unavailable.

Explanation:

An attempt to send a status (non-audit) message to the Guardium system failed because a connection was unavailable.

User response:

Determine the cause of the connection outage to the system and attempt to restore the connection.

ADHG510E pbWrite: No such message. code= error-code

Explanation:

While building a message, a problem was encountered with an internal interface

User response:

Contact IBM Software Support.

ADHG511E pbWrite: Nested too deep. code= error-code

Explanation:

While building a message, a problem was encountered with an internal interface.

User response:

Contact IBM Software Support.

ADHG512E pbWrite: Stack underflow. code= error-code

Explanation:

While building a message, a problem was encountered with an internal interface.

User response:

Contact IBM Software Support.

ADHG513E pbWrite: Not in message. code= error-code

Explanation:

While building a message, a problem was encountered with an internal interface.

User response:

Contact IBM Software Support.

ADHG514E pbWrite: No such field in message. code= error-code

Explanation:

While building a message, a problem was encountered with an internal interface.

User response:

Contact IBM Software Support.

ADHG515E pbWrite: Not a 32-bit integer field. code= error-code

Explanation:

While building a message, a problem was encountered with an internal interface.

User response:

Contact IBM Software Support.

ADHG516E pbWrite: Not implemented. code= error-code

Explanation:

While building a message, a problem was encountered with an internal interface.

User response:

Contact IBM Software Support.

ADHG517E pbWrite: Not a message type. code= error-code

Explanation:

While building a message, a problem was encountered with an internal interface.

User response:

Contact IBM Software Support.

ADHG520W Encoding exception: Event exceeds protocol message size limit. code=error-code

Explanation:

The network protocol used to communicate to the Guardium system is limited to 64 KB in payload size. If

an audited event results in a payload that exceeds this limit, this message is issued, and a truncated message is built and sent to the system. This message is only issued once per collector instance. At termination, message ADHG521W reports the total number of events impacted by this exception. The specified *error-code* value is for use by technical support.

User response:

No action is required. If an excessive number of exceptions are observed, or if you are concerned that the exceptions are impacting audit data integrity, use APPLIANCE_PORT(16022), which uses a communications protocol capable of delivering events with larger payloads.

ADHG521W	Total encoding exceptions encountered due to exceeded message size: <i>exception-count</i>
-----------------	---

Explanation:

The network protocol used to communicate to the Guardium system is limited to 64 KB in payload size. If an audited event results in a payload that exceeds this limit, message ADHG520W is issued. At termination, this message reports the total number of events that have been impacted by this exception, displayed as *exception-count*.

User response:

No action is required. If an excessive number of exceptions are observed, or if you are concerned that the exceptions are impacting audit data integrity, use

APPLIANCE_PORT(16022), which uses a communications protocol capable of delivering events with larger payloads.

ADHG522E	Write failed length=<i>length</i> rc=<i>returncode</i> rsn=<i>reasoncode</i>
-----------------	---

Explanation:

During an attempted TCP/IP data send of the length specified, the send failed with the specified return and reason code.

User response

Refer to the IBM manual, *z/OS UNIX System Services Messages and Codes*, for an explanation of the reason code. The last 4 digits of the reason code correspond to the errors of the send API. Also, review the ADHLOG of the S-TAP Collector Agent for other messages that might indicate problems with the connection between the S-TAP Collector Agent and the Guardium appliance.

This send failure might be the result of excessive amounts of data being sent to the appliance. Refer to the appliance reporting to determine whether excessive numbers of events were sent to the appliance prior to the send failure. If you determine the failure to be the result of excessive amounts of data, review and modify the active policy to decrease the amount of data that is sent to the appliance.

Error messages and codes: ADHIxxxx

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

ADHI026W	Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.
-----------------	--

Explanation:

The APPLIANCE_PORT parameter currently supports a setting of 16022, but the parameter has been retained for future support. If APPLIANCE_PORT is specified with a value other than 16022, message ADHG026W is issued, and port 16022 will be used instead.

User response:

Change APPLIANCE_PORT parameter setting to 16022 or remove the parameter entirely.

ADHI031I	V10.1.3 [component] connection established
-----------------	---

Explanation:

The specified component successfully established a TCP/IP connection to the Guardium system.

User response:

None action is required.

ADHI530E	DB2 connection failed [<i>function</i>] SQLCODE=[<i>sqlcode</i>] RSN=[<i>reason-code</i>]
-----------------	--

Explanation:

A DB2 attachment facility error occurred.

User response:

An error occurred while performing a DB2 attachment function. See the *IBM DB2 for z/OS Messages and Codes* manual for more information about the return and reason codes.

ADHI531W	Option STAP_UTILITY_TS_TO_TABLE(Y) is ignored due to a previous error
-----------------	--

Explanation:

The option STAP_UTILITY_TS_TO_TABLE was set to enable collection of expanded utility information. However, an error occurred when attempting to

establish the DB2 connection, which is required for this feature. The option is disabled.

User response:

Review ADHLOG for occurrences of message ADHG503E to determine the cause of the DB2 connection failure.

ADHI612E Termination requested as the result of a previous error

Explanation:

An unrecoverable error condition was encountered. A shutdown request will sent to the collector agent.

User response:

Check the ADHLOG for prior errors and attempt to resolve any previous errors.

ADHI613E SQLCODE -805 encountered for plan name [plan_name]

Explanation:

A DB2 bind error -805 was encountered for the specified plan name.

User response:

Run the ADHBIND job located in the SADHSAMP library.

ADHI697E Unexpected error: [error_description]. Return code: [return_code]

Explanation:

An unexpected error was encountered.

User response:

Contact IBM Support.

ADHI699E Unexpected error: [error-condition]

Explanation:

An unexpected error was encountered.

User response:

Contact IBM Software Support.

Error messages and codes: ADHKxxxx

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

ADHK001I Scope expression received, len = length of expression text

Explanation:

The filter compiler has received a filter expression of length *length* and expression text of *expression Text*. Only the first line of the expression text is output with this message. Only issued when trace-filter is true.

User response:

None required.

ADHK002I Starting Compilation...

Explanation:

The expression compiler is starting to compile the filter expression. Only issued when trace-filter is true.

User response:

No action is required.

ADHK004I Constant Pool for routine: (at memoryLocation).

Explanation:

This is a debugging message that shows the memory location of an important data structure for the compiled filter. This line is followed by a hexadecimal printout of the contents of that memory. Only issued when trace-filter is true.

User response:

No action is required.

ADHK005W Level level 'compilerMessage'.

Explanation:

These are messages generated by the filter compiler if there is anything wrong with the generated filter expression. The compiled filter will not be used. The agent and/or collector will shut down.

User response:

Contact IBM Software Support. Provide the agent and/or collector logs along with the xml file for the active profile at the time the message was generated.

ADHK101I Compiling filter. Flags1 Flags; Compile Trace True/False; Runtime Trace RuntimeTraceFlag; RuntimeTrace RuntimeTraceValue; Stage 1 Requested True/False.

Explanation:

An informational message is issued whenever a new profile is about to be compiled into a compiled filter.

User response:

No action is required.

ADHK102I Rule Expression.

Explanation:

The following lines show the filter expression that was generated from the profile.

User response:

No response required.

ADHK103I Profile contained no filter information for this agent.**Explanation:**

The currently active filter had nothing specified to be collected in the current context. For example, in the ASC started task, if the filter has no targets, or if none of the targets had any events checked, then there is nothing for the ASC started task to collect.

User response:

No response is required, in general. However, if you had intended data to be collected, you may wish to review the active profile. If you believe the message is issued in error, contact IBM Software Support.

ADHK104I Filter Compile Failed.**Explanation:**

The expression that was generated from the currently active profile could not be compiled into a filter.

User response:

Contact IBM Software Support.

ADHK105I Variable text**Explanation:**

This message has been issued from the filter compiler

User response:

Contact IBM Software Support.

ADHK106I Compiled filter requires bytes bytes of dynamic save area.**Explanation:**

The compiled filter needs a certain amount of filter working memory to be able to do filtering, and this message only appears if the amount of filter working memory allocated (8192 bytes) is insufficient. This is unusual, and indicates a very large and complicated profile.

User response:

You can consider reducing the size of the profile through the use of wildcards. If that is not possible, contact IBM Software Support.

ADHK110I Rule expression:**Explanation:**

This message will be followed by a full, multi-line, display of the filter expression generated from the

profile. This message is only printed if trace-filter is true.

User response:

No action is required.

ADHK111I Compiling filter. flags1 flags1 trace=trace runtimeTraceFlag runtimeTraceFlag runtimeTrace runtimeTrace**Explanation:**

An informational message issued whenever a new profile is about to be compiled into a compiled filter.

User response:

No action is required.

ADHK203I Stage one filtering was not enabled.**Explanation:**

Stage 1 filtering must be enabled.

User response:

To enable stage 1 filtering, enter STAGE1_FILTER(Y) in the ADHCPARMS DD.

ADHK204I Error while creating stage one filter.**Explanation:**

A bug in the filtering code prevented the correct creation of a filter for stage 1. If the stage 2 filter compiled correctly, filtering proceeds successfully at a higher overhead.

User response:

Contact IBM Software Support with XML export of the profile, and the JES output that contained this message.

ADHK205I No valid stage one filter criteria found.**Explanation:**

Stage 1 filtering is based on a subset of the profile fields. If one or more rules in the profiles do not include at least one of the profile fields, then stage 1 filtering might not apply.

User response:

Review the filtering stages section of the User's Guide and adjust the profile accordingly.

Error messages and codes: ADHPxxxx

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

ADHP000I Attempting connection to server server-address port=server-port**Explanation:**

The S-TAP policy component will attempt to establish a TCP/IP connection to a Guardium system at the specified server address and port.

User response:

No action is required.

ADHP001I Establishing Policy connection to server [server-address]

Explanation:

The policy component is preparing to establish the TCP/IP connection to the specified Guardium system.

User response:

No action is required.

ADHP002I Connection established to server [server-address]

Explanation:

The S-TAP policy component was successful in establishing a TCP/IP connection to the Guardium system.

User response:

No action is required.

ADHP003I Connection was re-established to [server name]

Explanation:

The S-TAP policy component was successful in establishing a TCP/IP connection to the Guardium system following a disconnect.

User response:

No action is required.

ADHP004W Connection was lost from server [server-address]

Explanation:

The TCP/IP connection between the S-TAP policy component and the Guardium system was lost. The S-TAP policy component will automatically attempt to reestablish the connection, however a potential for data loss exists if the connection is not established. A data loss condition is indicated by message ADHP006E.

User response:

Determine the cause of the network interruption and correct the problem so that the connection can be established.

ADHP005S Unable to establish a connection to server [server-address]

Explanation:

The S-TAP Policy component was unable to establish a TCP/IP connection to the Guardium system.

User response

- Ensure that the Guardium system is listening for a connection at the server and port specified in message ADHP001I. .

- Ensure that there are no firewalls blocking connections between the collector and the Guardium system.

ADHP006E Data loss has occurred as the result of a network send failure

Explanation:

During a disconnection, the S-TAP policy component exceeded the number of events that can be retained in memory while waiting for the network connection to the Guardium system to be reestablished.

User response

- Determine the cause of the network interruption and correct the problem so that the connection can be established.
- If necessary, increase the SEND_FAIL_EVENT_COUNT value in the ASC ADHPARMS parameter file to increase the number of events that can be retained in memory during short outages.

ADHP007E Unable to create a communications interface

Explanation:

An attempt to create an internal communications interface failed.

User response:

Contact IBM Software Support.

ADHP008S Required parameter was not supplied. Parameter=parameter-name

Explanation:

A required parameter was not supplied.

User response:

Supply a parameter and value for the specified parameter.

ADHP009I TCP/IP streaming disabled due to user setting.

Explanation:

A debug setting was specified that has disabled TCP/IP streaming between the S-TAP policy component and the Guardium system.

User response:

No action is required.

ADHP010I Disconnecting from server server-name

Explanation:

The S-TAP policy component is disconnecting from the Guardium system.

User response:

No action is required.

ADHP012I Failover support enabled

Explanation:

One or more failover servers were successfully registered with the communications interface, enabling failover support.

User response:

No action is required.

**ADHP013I Connection attempt timed out.
Reattempting connection
retry-number of total-
retries.**

Explanation:

The S-TAP policy component was unable to establish a TCP/IP connection to the Guardium system within the timeout period. An attempt to be made to reestablish the connection until the *retry-number* reaches the *total-retries* number.

User response

- Ensure that the Guardium system is listening for a connection at the server and port specified in message ADHP001I.
- Ensure that no firewalls are blocking connections between the collector and Guardium system.

ADHP015W Primary server is unavailable

Explanation:

A connection to the primary Guardium system is not available. Failover appliances will be attempted for connection.

User response:

Determine the cause of the connection interruption to the primary system and attempt to restore the connection.

**ADHP017W Data is being temporarily stored in
a spillfile until a connection is re-
established**

Explanation:

A Guardium system connection is unavailable and collected data is being written to the spillfile area until an system connection can be restored.

User response:

Determine the cause of the connection outage to the system and attempt to restore the connection.

**ADHP018I Spillfile contents have been
successfully be sent to server
[server]**

Explanation:

The spillfile data that was collected during a connection outage has been sent to the specified Guardium system upon reconnection.

User response:

No action is required.

**ADHP019S Spillfile storage has been
exhausted. Dataloss will occur**

Explanation:

A Guardium system connection is unavailable and the spillfile is out of space. Data collected after this time will be lost.

User response:

Determine the cause of the connection outage to the system and attempt to restore the connection. Notify others of the outage as necessary.

**ADHP020I Registering server [server] as
eligible for failover**

Explanation:

The specified server will be added to the list of failover servers to register for the connection. Registration is attempted after all failover servers have been added. A successful failover registration is indicated by message ADHP012I.

User response:

No action is required.

**ADHP021E Spillfile is approaching [50% |
85% | 95% |100%] capacity**

Explanation:

A Guardium system connection is unavailable and the spillfile area has reached the specified percentage of capacity.

User response:

Determine the cause of the connection outage to the system and attempt to restore the connection.

**ADHP022I A connection has been established
to failover server [server]**

Explanation:

A connection to the primary Guardium system is not available. A connection has successfully been established to one of the specified failover server.

User response:

Determine the cause of the connection interruption to the primary system and attempt to restore the connection.

**ADHP023I A persisted policy from
DD:ADHPLCY is being used.**

Explanation:

The S-TAP policy component was unable to establish a connection to the Guardium system. A persisted policy from DD:ADHPLCY is being used.

User response:

No action is required.

ADHP026W **Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.**

Explanation:

The APPLIANCE_PORT parameter currently supports a setting of 16022, but the parameter has been retained for future support. If APPLIANCE_PORT is specified with a value other than 16022, message ADHG026W is issued, and port 16022 will be used instead.

User response:

Change APPLIANCE_PORT parameter setting to 16022 or remove the parameter entirely.

ADHP028E **Required policy not available at initialization.**

Explanation:

At startup, the policy manager did not receive a policy from the Guardium appliance or policy DD.

User response

If APPLIANCE_SERVER_LIST is set to *FAILOVER*, this problem can be resolved by verifying that either:

- the primary server is active and a policy is installed, or
- the persistence policy DD is configured and has a valid policy installed from a previous policy.

If APPLIANCE_SERVER_LIST is set to *MULTI_STREAM*, verify that the primary server is active during startup.

ADHP030I **Policy component is terminating**

User response:

No action is required.

ADHP031I **V10.1.3 component connection established**

Explanation:

The S-TAP Policy component successfully established a TCP/IP connection to the Guardium system.

User response:

No action is required.

ADHP093E **Policy discarded because all DB2 rules contain errors**

Explanation:

All of the **DB2 collection profile** interception policies that were pushed down from the Guardium appliance contain errors. As a result, collection is deactivated.

User response:

Review the ADHLOG for messages that were issued prior to this message that indicate why the DB2 rules

were discarded. Examples of relevant messages include ADHP096E and ADHP101W. Use the reason and value that is reported in the message to correct the incorrect value or error in the collection policy.

ADHP094E **Policy discarded due to error**

Explanation:

One or more errors were detected while processing an interception policy that was pushed down from the Guardium appliance. As a result, the entire policy, as well as any rules that are contained within the policy, are ignored.

User response:

Review the ADHLOG for messages that were issued prior to this message (for example, ADHP101W) that indicate why the policy was discarded. Use the reason and value that is reported in the message to correct the incorrect value or error in the collection policy.

ADHP095E **error: rule discarded due to error**

Explanation:

One or more errors were detected while processing an interception policy rule that was pushed down from the Guardium appliance. As a result, the rule containing these errors is ignored.

User response:

Review the ADHLOG for messages that were issued prior to this message that indicate why the rule was discarded. Examples of relevant messages include ADHP096E and ADHP101W. Use the reason and value that is reported in the message to correct the incorrect value or error in the collection policy.

ADHP096E **rule error: [error]**

Explanation:

An error was detected while processing an interception policy rule that was pushed down from the Guardium appliance.

User response:

Use the error text that is provided in this message to correct the value or error in the collection policy.

ADHP097E **Unexpected error: [error_description]. Return code: [return_code]**

Explanation:

An unexpected error was encountered.

User response:

Contact IBM Software Support.

ADHP099E **Unexpected error: error-condition**

Explanation:

An unexpected error was encountered.

User response:

Contact IBM Software Support.

ADHP101W **Invalid value for filter. Reason:**
[reason]. Value: [value]

Explanation:

An invalid value was detected while processing the collection policy received from the Guardium system.

User response:

Attempt to correct the invalid value or error in the collection policy by referencing the reason and value reported in the message.

ADHP102E **Invalid value for sqlcode:**
[*_sqlcode_*]

Explanation:

A SQL code that was detected while processing the collection policy from the IBM Guardium system is not valid.

User response:

Attempt to correct the SQL code in the collection policy by referencing the value that is reported in the message. See *SQL error codes* in the IBM Knowledge Center for more information.

ADHP110I **mode: *******

Explanation:

This message is issued when information about the event streaming mode is requested by issuing the **/F STAP** command, where ********* is either *STREAMING EVENTS* or *POLICY SIMULATION*.

User response:

No action is required.

ADHP111I **STAP command [STAP MODIFY**
command]

Explanation:

This message indicates that an S-TAP MODIFY command has been issued.

User response:

No action is required.

ADHP120I **Installed Policy:**

Explanation:

The header of the installed policy

User response:

No action is required.

ADHP121I **[policy segment]**

Explanation:

A segment of the installed policy

User response:

No action is required.

ADHP122I **Installed Quarantine:**

Explanation:

The header of the installed quarantine policy

User response:

No action is required.

ADHP123I **[quarantine segment]**

Explanation:

A segment of the installed quarantine policy

User response:

No action is required.

ADHP124I **Installed Blocking:**

Explanation:

The header of the installed blocking policy

User response:

No action is required.

ADHP125I **[blocking segment]**

Explanation:

A segment of the installed blocking policy

User response:

No action is required.

ADHP126I **STAP BLOCKING mode:**
[ENABLED|DISABLED|OPERATOR]

Explanation:

This message indicates whether S-TAP blocking is enabled, disabled, or in operator mode.

User response:

No action is required. See SQL Blocking for more information.

ADHP130I **Agent configuration:**

Explanation:

The header of the agent configuration

User response:

No action is required.

ADHP131I **[agent configuration segment]**

Explanation:

A segment of the agent configuration

User response:

No action is required.

ADHP140I **Event Counts:**

Explanation:

The header of the event collection statistics

User response:

No action is required.

ADHP141I **[event type] [total collected]**

Explanation:

The total count collected for the event

User response:

No action is required.

ADHP142I [event type] [total collected]**Explanation:**

The total count collected for the event

User response:

No action is required.

ADHP143I [event type] [total collected]**Explanation:**

The total count collected for the event

User response:

No action is required.

ADHP144I [event type] [total collected]**Explanation:**

The total count collected for the event

User response:

No action is required.

ADHP145I [event type] [total collected]**Explanation:**

The total count collected for the event

User response:

No action is required.

ADHP146I [event type] [total collected]**Explanation:**

The total count collected for the event

User response:

No action is required.

ADHP150I Program levels:**Explanation:**

The header of S-TAP program levels

User response:

No action is required.

ADHP151I [program level segment]**Explanation:**

A segment of S-TAP program levels

User response:

No action is required.

ADHP160I S-TAP allocation queue history:**Explanation:**

The header of S-TAP allocation queue history

User response:

No action is required.

ADHP161I TimeStamp-----Queued-----
Freed**Explanation:**

The subheader of S-TAP allocation queue history

User response:

No action is required.

ADHP162I [allocation queue segment]**Explanation:**

A segment of the allocation queue history

User response:

No action is required.

ADHP163I S-TAP filter history:**Explanation:**

The header of S-TAP filter history

User response:

No action is required.

ADHP164I TimeStamp----Pass Stage 1-- ---
Pass Stage2**Explanation:**

The subheader of the S-TAP filter history

User response:

No action is required.

ADHP165I [filter queue segment]**Explanation:**

A segment of S-TAP filter history

User response:

No action is required.

ADHP166I S-TAP IO history:**Explanation:**

The header of S-TAP IO history

User response:

No action is required.

ADHP167I TimeStamp-----Sent-----
Bytes sent-----Write time**Explanation:**

The subheader of S-TAP IO history

User response:

No action is required.

ADHP168I [filter queue segment]**Explanation:**

A segment of S-TAP IO history

User response:

No action is required.

ADHP170I Event count reported by the
appliance at time: [count]**Explanation:**

Number of collected events reported by the appliance.

User response:

No action is required.

ADHP179E **Option [option] is invalid for STAP command**

Explanation:

An invalid value was detected while processing the S-TAP command.

User response:

Check the command and try again.

ADHP180I **[policy | quarantine | blocking] policy push detected.**

Explanation:

A policy pushdown from the Guardium appliance has been detected.

User response:

No action is required.

ADHP183E **FORCE_LOG_LIMITED is enabled but APPLIANCE_PORT is not compatible.**

Explanation:

The **FORCE_LOG_LIMITED** parameter is enabled but **APPLIANCE_PORT** is not set correctly.

User response:

Check the compatible values for **FORCE_LOG_LIMITED** and **APPLIANCE_PORT**.

ADHP182I **SUPPORT_FORCE_LOG_LIMITED is enabled.**

Explanation:

The S-TAP has been configured not to collect host variables.

User response:

No action is required.

ADHP183I **FORCE_LOG_LIMITED is not supported by the appliance.**

Explanation:

The appliance does not support the **FORCE_LOG_LIMITED** feature.

User response:

Check for the compatible appliance with which to use the **FORCE_LOG_LIMITED** feature.

ADHP184I **A pushed down [policy | blocking | quarantine] is in use.**

Explanation:

Policy push down is in use.

User response:

No action is required.

ADHP185I **A [policy | quarantine | blocking] from DD is in use.**

Explanation:

A policy supplied by DD is in use rather than one from push down.

User response:

No action is required.

ADHP186I **A [policy | quarantine | blocking] from DD is in use, ignoring any pushed down policy.**

Explanation:

A policy supplied by DD is in use. Any pushed down policy will be discarded.

User response:

No action is required.

ADHP188I **Blocking policy removed.**

Explanation:

All blocking policies have been uninstalled.

User response:

No action is required.

ADHP189W **There is no table found in database: [database name]**

Explanation:

The database [database name] that was specified in the blocking policy is either empty or not defined.

User response:

Rebuild the blocking policy with a valid database for blocking to be active for the database.

ADHP190W **DB2 object: [object type] with name: [object name] does not exist.**

Explanation:

The DB2 object [object type] specified in the blocking policy does not exist.

User response:

Rebuild the blocking policy with valid blocking targets for blocking to be active for the DB2 object.

ADHP191W **Blocking is NOT ACTIVE because there is no valid target in the policy.**

Explanation:

No valid blocking target has been found in the blocking policy. Blocking will not be activated.

User response:

Rebuild the blocking policy with valid blocking targets for blocking to be activated.

ADHP192E **SQL statement execution was unsuccessful, SQLCODE is: [sqlcode value] SQLSTATE is: [sqlstate value]**

Explanation:

A SQL statement execution was unsuccessful during policy pushdown process.

User response:

Determine the cause of the SQLCODE. Correct the installed policy if necessary.

ADHP193I **STAP Logging command pushed down from UI to request STAP logging information.**

Explanation

S-TAP logging levels provide log information as follows:

Level 0

Logs program levels, event queue statistics, agent configuration, policy, and event counts.

Level 1

Logs agent configuration, policy, and event counts.

Level 2

Logs agent configuration.

Level 3

Logs policy.

Level 4 or higher

Logs event counts.

User response:

No action is required.

ADHP200E **Unexpected element in policy definition: <element>**

Explanation:

An unexpected element has been found while parsing policy.

User response:

Correct the unexpected element and update the policy.

ADHP201E **A policy must contain at least one rule**

Explanation:

No rule was found in the policy.

User response:

Update the policy to contains at least one rule.

ADHP203E **Duplicate schema specification: [schema-name]**

Explanation:

A duplicated schema within one target has been detected.

User response:

Update the policy with only one schema per target.

ADHP204E **Duplicate table specification: [table-name]**

Explanation:

A duplicate table within one target has been detected.

User response:

Update the policy with only one table per target.

ADHP205E **Duplicate First Read event specification.**

Explanation:

A duplicate First Read event has been detected.

User response:

Update the policy with only one First Read event per target.

ADHP206E **Duplicate First Change event specification.**

Explanation:

A duplicate First Change event has been detected.

User response:

Update the policy with only one First Change event per target.

ADHP207E **Expected <policy> specification but found <***>.**

Explanation:

The <policy> tag was expected but a different tag (<***>) was found.

User response:

Correct the policy.

ADHP208E **Policy syntax error**

Explanation:

A syntax error was found while parsing the policy.

User response:

Correct the policy.

ADHP209E **Error in opening data set: [dataset]**

Explanation:

An error occurred while opening a data set for policy parsing.

User response:

Make sure the dataset exists and is associated with the appropriate permissions.

ADHP210I **A thread termination request was received for thread [thread ID]**

Explanation:

A termination request was received for thread [thread ID].

User response:

No action is required.

ADHP211W **Policy syntax error [error]**

Explanation:

A syntax error was found while parsing the policy.

User response:

Correct the policy.

ADHP212W **[policy | quarantine | blocking] not enabled for ddname [ddname]
reason: XML error**

Explanation:

The policy from DD is not enabled because a syntax error was found.

User response:

Correct the policy in the DD.

ADHP213E **Blocking policy syntax error:
Invalid network [network]**

Explanation:

Network value is not valid in the installed blocking policy.

User response:

Correct the network value and reinstall the blocking policy.

ADHP214E **Blocking policy syntax error:
Invalid netmask [netmask]**

Explanation:

Netmask value is not valid in the installed blocking policy.

User response:

Correct the netmask value and reinstall the blocking policy.

ADHP215E **Blocking policy syntax error:
Invalid IP address [IP address]**

Explanation:

IP address value is not valid in the blocking policy.

User response:

Correct the IP address value and reinstall the blocking policy.

ADHP216W **Blocking policy is ignored due to a
previous error.**

Explanation:

The installed blocking policy contains a syntax error. The blocking policy is discarded.

User response:

Resolve the error and reinstall the blocking policy.

ADHP217W **Incomplete rule discarded. Rule
name: [_rule-name_]**

Explanation:

An incomplete policy rule is detected.

System action:

The rule is discarded.

User response:

Use the **Guardium Policy Builder** of the Guardium appliance interface to define and manage data collection and filtering. Correct the specified rule *rule-name* and add the necessary filters to make it a complete rule.

ADHP218W **Only one SQLCODE list is allowed.
SQLCODE is discarded: [sqlcode]**

Explanation:

More than one SQLCODE list is detected.

System action:

The first list is accepted. Additional lists are discarded.

User response:

Ensure that there is only one SQLCODE list for each installed policy.

ADHP220I **Appliance connect retry count has
been reached, appliance ping rate
is now increased to [number]**

Explanation:

Ping rate has been increased to a larger value after reaching the specified number of **APPLIANCE_CONNECT_RETRY_COUNT** attempts.

User response:

No action is required.

ADHP250E **Unable to send message.
Connection to server is
unavailable.**

Explanation:

S-TAP was unable to send messages to the appliance.

User response:

Make sure the appliance is online and reachable by the S-TAP.

ADHP550E **Unable to send message.
Connection to server is
unavailable**

Explanation:

An attempt to send a non-audit status message to the Guardium system failed because no connection to the appliance is available.

User response:

Determine the cause of the connection outage to the system and attempt to restore the connection.

Error messages and codes: ADHQxxxx

The following information is about error messages and codes that begin with ADHQ. These messages are generated from the collector agent.

ADHQ1000E NOT APF AUTHORIZED

Explanation

The collector agent started task or job is not APF authorized.

User response

The collector agent requires that the target load libraries be APF-authorized.

Explanation

This message appears during normal shutdown of the Collector Agent and indicates the collector is undergoing shutdown.

User response

No action is required.

**ADHQ1001I DB2 QUERY COMMON COLLECTOR
INITIALIZATION IN PROGRESS
FOR SUBSYSTEM**

Explanation

This message appears during the normal initialization process of the collector agent.

User response

No action is required.

**ADHQ1005I QUERY COMMON COLLECTOR
TERMINATION COMPLETE FOR
SUBSYSTEM *ssid***

Explanation

The collector agent subsystem has been terminated. This message could appear as part of normal shutdown or as a failure to connect to a subsystem.

User response

Investigate other write-to-operator (WTO) messages preceding this one to determine the reason for the termination.

**ADHQ1002I DB2 AUDIT SQL COLLECTOR
INITIALIZATION COMPLETE FOR
SUBSYSTEM**

Explanation

This message appears during the normal initialization process of the collector agent and confirms the initialization process has completed.

User response

No action is required.

**ADHQ1006E *statement* DD STATEMENT
MISSING**

Explanation

The parameter DD statement (for example, ADHCFGP DD statement) is missing from the JCL for the collector agent started task.

User response

Create the necessary DD statement and code the appropriate parameters in the data set.

**ADHQ1003E SUBSYSTEM *ssid* ALREADY
ACTIVE**

Explanation

The collector agent indicated in the message is already active and can therefore cannot process another activate command.

User response

Verify that you are activating the correct system. If you are attempting to activate a subsystem that is already active, do not attempt activation.

**ADHQ1007E INVALID USERID SPECIFIED FOR
AUTHID**

Explanation

The user ID entered in the AUTHID parm in the ADHCFGP data set has not been defined to RACF or an equivalent security system.

User response

Correct the user ID, or ensure the ID is defined to your security system.

**ADHQ1004I QUERY COMMON COLLECTOR
TERMINATION IN PROGRESS FOR
SUBSYSTEM *subsystem***

ADHQ1010I DEBUG MODE ON

Explanation

Debugging mode has been turned on.

User response

None required.

ADHQ1011I DEBUG MODE OFF

Explanation

Debugging mode has been turned off.

User response

None required.

ADHQ1016E INVALID COMMAND SYNTAX

Explanation

The command syntax is invalid.

User response

Correct the command.

ADHQ1017E INVALID COMMAND

Explanation

An invalid MVS Modify command was issued.

User response

Correct the command and execute it again.

**ADHQ1019I INTERVAL EXTERNALIZATION
MODE OFF**

Explanation

The collector agent subsystem was started with externalization mode set to off.

User response

No action is required.

**ADHQ1020E DB2 SUBSYSTEM *ssid* IS NOT
DEFINED**

Explanation

The DB2 subsystem indicated in the message is not defined.

User response

Verify that you have specified the correct DB2 subsystem.

ADHQ1024E *dsn* SPECIFICATION INVALID

Explanation

The data set name listed in this message is not valid.

User response

Verify that you specified the correct data set name in ADHCFGP.

**ADHQ1026E SHARED MEMORY FAILURE FOR
OBJECT *object request RC =rc*
RS=*rs***

Explanation:

A shared memory failure has occurred for the indicated object.

User response:

Contact IBM Software Support.

**ADHQ1027I CPU=*CPU Type-CPU Model-CPU
Manufacturer. OS Name OS
Version.OS Release.OS
Modification.***

Explanation:

This message displays information about the CPU and the operating system.

User response:

No action is required.

**ADHQ1028E Component requires a 64 bit
processor and z/OS 1.5 or higher.**

Explanation:

Your system does not meet the minimum system requirements.

User response:

Upgrade to the minimum requirements.

**ADHQ1031E Serious error in master address
space *address space*.**

Explanation:

A serious error has occurred in the master address space specified.

User response:

Verify that the master address space is available.

ADHQ1032I Recreating master address space.

User response:

No action is required.

**ADHQ1033E Unable to create master address
space *address space*.**

Explanation:

DB2 Query Monitor is not able to create the master address space specified.

User response:

Many issues that cause this error relate to security setup. If you encounter this message, send your console log to IBM Software Support.

ADHQ1034I Master address space has started.

User response:

No action is required.

ADHQ1035E Unable to restart master (RS=rc).

Explanation:

The master address space could not be restarted.

User response:

verify the master address space is available and restart.

ADHQ1055E CQM1055E DB2 ssid IS EXPERIENCING STORAGE CONSTRAINTS, DATA LOSS MAY OCCUR, REASON=code

Explanation:

The DB2 subsystem indicated in the message is experiencing storage constraints.

User response:

Verify that your DB2 subsystem has the needed storage allocations.

ADHQ1060I ZIIP SUPPORT IS NOT ACTIVE. nnnnnnnn RC=yy RSN=zzzzzzzz nnnnnnnn is the name of the service that failed with a nonzero return code (RC).

Explanation

Table 9. Return code explanations	
Service	Description
IWM4ECRE (WLM Enclave Create)	The return codes and reason codes are documented in <i>z/OS V1R10.0 MVS Programming Workload Management Services</i> .
IWM4EoCT (WLM CPU Offload Time Service)	The return codes and reason codes are not documented in any existing WLM manual. However, RC=4 typically means no ZIIP is configured on the instance of z/OS. If you have a ZIIP processor and it is properly configured, report the RC to the vendor.
MAXWFLOAD (Enclave SRB load service)	An error occurred trying to LOAD ADHMAXWF (the enclave SRB routine that runs on the ZIIP). Make sure you have the correct STEPLIB configured.

Table 9. Return code explanations (continued)

Service	Description
IEAVAPE (Z/OS Allocate Pause Element)	These return codes are described in <i>z/OS V1R10.0 MVS Programming Assembler Services References V2</i> . If the ADHQ1060I has IEAVAPE has the failing service, contact the vendor for resolution.

ADHQ1061E MISSING PARAMETER: parameter

Explanation

The specified parameter has not been defined in the sample library member ADHCFGP.

User response

Add the missing parameter to the ADHCFGP sample library member.

ADHQ1062E COMMUNICATION INTERFACE DISABLED BY CROSS MEMORY FAILURE

Explanation

A cross memory failure has occurred and as a result the communication interface has been disabled.

User response

Troubleshoot the memory failure and restart the ASC.

ADHQ1062I ZIIP SUPPORT IS INSTALLED

Explanation:

The collector agent has detected that WLM is configured for zIIP support. This does not necessarily indicate that zIIP processors are installed or are available for zIIP offload of collector agent processing.

User response:

No action is required.

ADHQ1065E REQUIRED DATA ACCESS COMMON COLLECTOR MODULE NOT FOUND

Explanation:

The started task did not find the Data Access Common Collector (CQC) initialization module, which prevented successful startup.

User response:

Verify that the Data Access Common Collector (CQC) has been installed and that the load library is included in the started task STEPLIB concatenation

ADHQ1066E **Subsystem terminating due to abend while compiling the collection profile. SVCDUMP collected.**

Explanation:

An abend was detected when compiling the collection profile. A memory dump was collected to gather the diagnostic information.

User response:

If you are unable to take corrective measures to resolve the abend, then the SVCDUMP, the collector joblog, and the details of the collection profile in use should be reported to IBM Software Support for resolution of this error.

ADHQ1070E **Terminating due to XML profile processing error RC (xxxxxxx)**

Explanation:

A policy is sent from the Guardium system to the collector agent during their initial communication. If the policy received by the collector agent is not composed of valid XML syntax, the collector terminates.

User response:

Verify that the Guardium system is properly configured, using the APPLIANCE_SERVER parameter. The system should be set up to accept connections from collectors. If the problem persists, contact IBM Software Support with the return code specified in this message.

ADHQ1071E **Terminating due to missing XML profile at start up**

Explanation:

A policy is sent from the Guardium system to the collector agent during their initial communication. If the policy is not received by the collector agent during the initial communication set up, then the collector terminates.

User response:

Verify that the Guardium system is properly configured, using the APPLIANCE_SERVER parameter. The appliance should be set up to accept connections from collectors. If the problem persists, contact IBM Software Support.

ADHQ1080I **POLICY MANAGER STARTED.**

Explanation:

The internal policy manager task has started.

User response:

No action is required.

ADHQ1081I **POLICY MANAGER STOPPED.**

Explanation:

The internal policy manager task has stopped.

User response:

No action is required.

POLICY PUSH DETECTED.

Explanation:

A policy was received from the appliance.

User response:

No action is required.

ADHQ1083I **POLICY PUSH SENT.**

Explanation:

The policy was sent to Audit SQL Collector.

User response:

No action is required.

ADHQ1084I **QUARANTINE ONLY POLICY DETECTED.**

Explanation:

A pushed policy was included on a quarantine list. The currently active audit policy is unchanged and is still active.

User response:

No action is required.

ADHQ1085I **CURRENT QUARANTINE POLICY IS REMOVED.**

Explanation:

A new policy push occurred which resulted in the removal of the quarantine list.

User response:

No action is required.

ADHQ1086I **BOTH NEW POLICY AND QUARANTINE POLICY DETECTED.**

Explanation:

A new policy push occurred, which resulted in new policy and quarantine lists to be activated.

User response:

No action is required.

ADHQ1086E **ADHQ1086E statement DD STATEMENT MISSING**

Explanation:

The parameter DD statement (for example, ADHPARMS DD statement) is missing from the JCL for the collector agent started task.

User response:

Create the necessary DD statement and code the appropriate parameters in the data set.

ADHQ1153E **RETURN CODE *return_code* REASON CODE *reason_code* WAS ENCOUNTERED DURING**

**TRANSLATION SOURCE CCSID
ccsid TARGET CCSID ccsid**

Explanation

An error was encountered during the translation of the indicated CCSIDs. This may be the result of not having defined conversion paths between the CCSID of the collected SQL text and CCSID 1208 when performing a DB2 offload.

User response

To offload SQL text, verify that all necessary CCSID paths to 1208 are installed. You must define conversion paths between the CCSID of the collected SQL text and CCSID 1208.

ADHQ1202I	STORAGE CONSTRAINT RELIEVED FOR SPACE – space – OCCURRENCES: count
------------------	---

Explanation

An Integrated Storage Manager error had previously occurred due to a storage constraint for the space named in the message. The storage constraint has now been relieved. The number of storage constraint occurrences for this incident is displayed in the message.

User response

No action is required.

ADHQ1203I	ASID=asid,TCB=tcb,CPID=cpid, MODULE=module,ADDR=addr, RC=rc,RSN=rsn
------------------	--

Explanation

A Integrated Storage Manager error has occurred. This message provides details that can be used by IBM Software Support to diagnose the situation.

User response

Provide the text of this message to IBM Software Support.

ADHQ1204I	FUNC=func,SP=subpool,FLG2=flag ,FLG3=flag
------------------	--

Explanation

A Integrated Storage Manager error has occurred. This message provides details that can be used by IBM Software Support to diagnose the situation.

User response

Provide the text of this message to IBM Software Support.

ADHQ1205E	ISM ERROR OCCURRED, DETAIL FOLLOWS: note
------------------	---

Explanation

A Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that have been produced to IBM Software Support.

ADHQ1209I	ISM ERROR RC=rc,RSN=rsn,SPACE – space
------------------	--

Explanation

A Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that have been produced to IBM Software Support.

ADHQ1210E	ISM SPACE IS DISABLED – space
------------------	--------------------------------------

Explanation

A Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that have been produced to IBM Software Support.

ADHQ1211I	AN ABEND OCCURRED DURING ISM PROCESSING FOR SPACE – space
------------------	--

Explanation

A Query Monitor Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any dumps that may have been produced to IBM Software Support.

**ADHQ1212E AN ERROR OCCURRED IN THE
EXTENT EXIT ROUTINE FOR
SPACE – *space***

Explanation

A Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that might have been produced to IBM Software Support.

**ADHQ1213W SPACE IS FULL AND NO MORE
EXTENTS CAN BE OBTAINED FOR
SPACE – *space***

Explanation

A Integrated Storage Manager operation has failed because no more extents can be obtained for the space named in the message. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM Software Support to diagnose the situation.

User response

This may be a temporary situation due to the level of DB2 activity currently monitored by . If message ADHQ1202I is also issued to indicate that the Storage Constraint has ended, then processing resumes. If this situation occurs frequently, adjust the amount of data collected by , or increase the amount of available memory by using the MAXIMUM_ALLOCATIONS and SMEM_SIZE parameters.

If you need assistance with modifying these parameters, provide the text of this message and messages ADHQ1203I and ADHQ1204I to IBM Software Support.

**ADHQ1214W OWNER LIMIT EXCEEDED FOR
SPACE – *space***

Explanation

A Monitor Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that might have been produced to IBM Software Support.

**ADHQ1215W SPACE IS FULL AND NO MORE
LARGE EXTENTS CAN BE
OBTAINED FOR SPACE – *space***

Explanation

A Monitor Integrated Storage Manager operation has failed because no more large extents can be obtained for the space named in the message. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM Support to diagnose the problem.

User response

This might be a temporary situation due to the level of DB2 activity currently being monitored by . If message ADHQ1202I is also issued to indicate that the Storage Constraint has ended, then processing resumes. If this situation occurs frequently, adjust the amount of data collected by , or increase the amount of available memory by using the MAXIMUM_ALLOCATIONS and SMEM_SIZE parameters.

If you need assistance with modifying these parameters, provide the text of this message and messages ADHQ1203I and ADHQ1204I to IBM Software Support.

**ADHQ1216E EXTENT PROCESSING FAILED
(ABEND) FOR SPACE – *space***

Explanation:

A Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that have been produced to IBM Software Support.

**ADHQ1217W SPACE IS FULL AND NO MORE
LARGE EXTENTS CAN BE
OBTAINED FOR SPACE – *space***

Explanation

A Integrated Storage Manager operation has failed because the request would have exceeded the maximum storage allocation specified in the MAXIMUM_ALLOCATIONS parameter in ADHPARMS. At the time of the error, was attempting to allocate additional storage for the space named in the message. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM Software Support to diagnose the situation.

User response

This might be a temporary situation due to the level of DB2 activity currently being monitored by . If message ADHQ1202I is also issued to indicate that the Storage Constraint has ended, then processing resumes. If this situation occurs frequently, adjust the amount of data collected by , or increase the amount of available memory by using the MAXIMUM_ALLOCATIONS and SMEM_SIZE parameters.

If you need assistance with modifying these parameters, provide the text of this message and messages ADHQ1203I and ADHQ1204I to IBM Software Support.

**ADHQ1218W MAXIMUM EXTENTS HAS BEEN
REACHED FOR SPACE – *space***

Explanation

An Integrated Storage Manager operation has failed because the request would have exceeded the maximum number of extents allowed for the space named in the message. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM Software Support to diagnose the situation.

User response

This might be a temporary situation due to the level of DB2 activity currently being monitored. If message ADHQ1202I is issued later to indicate that the Storage Constraint has ended, then processing resumes normally. If this situation rarely occurs, it might not be a problem. If this situation occurs frequently, adjust the amount of data collected by , or increase the amount of available memory by using the MAXIMUM_ALLOCATIONS and SMEM_SIZE parameters.

If you need assistance with tuning these parameters, provide the text of this message and messages

ADHQ1203I and ADHQ1204I to IBM Software Support.

**ADHQ1219W ALL ISMERROR MESSAGE BLOCKS
ARE IN USE**

Explanation

An Integrated Storage Manager error has occurred. However there were no free ISMERROR message blocks available.

User response

Increase the value of the **ISM_ERROR_BLOCKS** parameter in the ADHPARMS file. If this parameter is already set to the maximum value and the problem persists, contact IBM Software Support.

**ADHQ1500E ABNORMAL EOT FOR *subtask*
SUBTASK**

Explanation

An abnormal end of task occurred for the subtask indicated in the message.

User response

Verify conditions surrounding the abnormal end of task and reissue the subtask.

**ADHQ2001E DB2 SUBSYSTEM *ssid* ALREADY
MONITORED BY SUBSYSTEM *ssid***

Explanation

The indicated DB2 subsystem is already being monitored by the collector agent shown in the message.

User response

A DB2 subsystem can only be monitored by a single collector agent. To monitor the DB2 subsystem with another collector agent, first stop the monitoring of the DB2 subsystem by the collector agent (shown in the message).

**ADHQ2002E MONITORING AGENT
INSTALLATION FAILED FOR
SUBSYSTEM *ssid***

Explanation

A monitoring agent was unable to start. Another SQL-type monitoring product might be active within the specified DB2 subsystem.

User response

Check to see if another SQL-type monitoring product is active. If so, shut down the other product and restart the S-TAP collector. If this does not resolve the problem, contact IBM Software Support.

If you encounter message ADHQ2002E and receive a memory dump, contact IBM Software Support and provide the memory dump for diagnostic purposes.

**ADHQ2003I FORCING MONITORING AGENT
INSTALLATION FOR *ssid***

Explanation

The collector agent has detected that a monitoring agent is already active, but is forcing installation because FORCE (Y) was included.

User response

No action is required.

**ADHQ2005I MULTIPLE MONITORING AGENT
INSTALLATION FOR SUBSYSTEM
*ssid***

Explanation

The collector agent has installed multiple monitoring agents for the subsystem shown in the message.

User response

No action is required.

**ADHQ2008E DB2 SYSTEM *ssid* IS BEING
MONITORED BY A 2.2 OR BELOW
VERSION CQM SUBSYSTEM AND
CANNOT BE AUDITED**

Explanation

This message indicates an incompatibility between DB2 Query Monitor and S-TAP. InfoSphere Guardium S-TAP for DB2 Version 9.1 will not start auditing a DB2 subsystem that is running Query Monitor at Version 3.1 or earlier.

User response

Ensure that you are running compatible versions of S-TAP and Query Monitor, or run only one product at a time.

**ADHQ2009E DB2 SYSTEM *ssid* WAS
PREVIOUSLY MONITORED BY A
2.2 OR EARLIER CQM SUBSYSTEM
qmid WHICH HAS NOT APPLIED
APAR PK55535.**

Explanation:

You must apply Query Monitory V2R2 APAR PK55535.

User response:

Apply the required maintenance.

**ADHQ2010I CURRENTLY ACTIVE POLICY
RESULTS IN DISABLED
COLLECTION**

Explanation

The currently installed collection policy, as received from the Guardium system, results in no ASC collection. This can be the result of:

- No policies are installed on the system.
- No DB2 Collection Profile policies are installed on the system.
- No DB2 Collection Profile policies matching the Svc. Name of the collector agent SSID are installed on the system.
- No DB2 Collection Profile policies contain Object entries that would result in ASC collection.

User response:

If ASC collection is expected when this message is issued, review installed policy definitions in the Guardium system administration interface for the previously listed conditions. If no ASC collection is expected when this message is issued, no action is required.

**ADHQ2013I CURRENTLY ACTIVE POLICY
RESULTS IN GRANT/REVOKE
COLLECTION**

Explanation:

The activated policy enables the collection of GRANT and REVOKE SQL statements. GRANT and REVOKE SQL statements are collected if they match the policy filter criteria.

User response:

No action is required.

**ADHQ2014I CURRENTLY ACTIVE POLICY
RESULTS NO HOST VARIABLE
COLLECTION.**

Explanation:

Host variables, which are also known as BIND variables, are not collected.

User response:

No action is required.

**ADHQ2015I CURRENTLY ACTIVE POLICY
RESULTS NEGATIVE SQL CODES
COLLECTION.**

Explanation:

The active policy contains a negative SQL code list that results in the collection of events ending with a negative SQL code.

User response:

No action is required.

ADHQ2016I	CURRENTLY ACTIVE POLICY RESULTS DB2 COMMANDS COLLECTION.
------------------	---

Explanation:

Collection of COMMAND events is enabled.

User response:

No action is required.

ADHQ2017I	CURRENTLY ACTIVE POLICY RESULTS IN DBNAMES OPTIMIZATION.
------------------	---

Explanation:

The currently active policy contains rules with DBNAME filters, which enables optimized filtering of audit events.

User response:

No action is required.

ADHQ2018I	CURRENTLY ACTIVE POLICY RESULTS IN A QUARANTINE LIST.
------------------	--

Explanation:

The active policy contains a quarantine list that might cause DB2 activity to be quarantined.

User response:

No action is required.

ADHQ2019I	CURRENTLY ACTIVE POLICY RESULTS IN DB2 UTILITIES COLLECTION
------------------	--

Explanation:

The active policy enables the collection of DB2 utilities.

User response:

No action is required.

ADHQ2020I	CURRENTLY ACTIVE POLICY RESULTS IN FAILED LOGIN COLLECTION.
------------------	--

Explanation:

The active policy enables the collection of Failed Login events.

User response:

No action is required.

ADHQ2100E	UNRECOGNIZED PARAMETER
------------------	-------------------------------

Explanation

The collector agent has encountered an unrecognized parameter.

User response

Check the startup parameters to ensure that the parameters specified are all valid.

ADHQ2101E	PARAMETER ERROR DETECTED FOR <i>parameter</i>
------------------	--

Explanation

The collector agent has encountered an error in one of the startup parameters.

Note: Message ADHQ2101E can be issued when the collector agent is started if the ADHCFGP file specifies primary space allocations for back store data sets that are less than the default.

User response

Check the startup parameters to ensure that all are specified properly. Check that primary space allocations for back store data sets are not set for less than their default values.

ADHQ2103E	DUPLICATE PARAMETER DETECTED FOR <i>parameter</i>
------------------	--

Explanation

Duplicate parameters were specified in the Query Common Collector startup parameters.

User response

Check the startup parameters to ensure that all are specified properly. Remove any duplicate parameters.

ADHQ2110E	TERMINATING DUE TO ERRORS IN PARAMETER FILE
------------------	--

Explanation

An error in the collector agent parameter file caused the termination of processing.

User response

Verify that the input you specified for your collector agent parameters in ADHCFGP is valid and correct for your objectives.

ADHQ2111E	ERROR READING PARAMETER DATASET - MEMBER NOT FOUND
------------------	---

Explanation

The collector agent encountered an error while attempting to read the ADHCFGP data set. The ADHPARMS DD statement specified a PDS data set and the member name specified did not exist.

User response

Correct the JCL specification for the ADHPARMS DD statement and specify a valid member name.

**ADHQ2402I DATASPACE MANAGEMENT IN
PROGRESS FOR *dsmt***

Explanation

Indicates dataspace management is in progress for the subsystem shown in the message.

User response

No action is required.

**ADHQ2403I *n* DATASPACE PAGES RELEASED
FOR *ssid***

Explanation

Displays the number of dataspace pages that have been released for the subsystem shown in the message.

User response

No action is required.

**ADHQ2408E INVALID REPLY. REPLY "U" TO
ACCEPT OR "R" TO REJECT**

Explanation

The replay you entered is not valid.

User response

Enter U to accept or R to reject.

**ADHQ2601E ALLOCATION FAILED FOR VSAM
DATASET *dsn* RETCD=*rc* REAS=*rs***

Explanation

This message is issued by the started task if there is a problem during the dynamic allocation of a data set. When this message occurs, the collector agent stops and the startup process and terminates.

User response

To further diagnose and resolve the problem using the return code and reason code listed in the message,

refer to the *MVS Programming Authorized Assembler Services Guide* (SA22-7608-07).

**ADHQ2603E DEALLOCATION FAILED FOR
DATASET *data_set*
RETCD=*return_code*
REAS=*reason_code***

Explanation

This message reports errors encountered during the execution of a CLOSE macro instruction.

User response

To further diagnose and resolve the problem using the return code and reason code listed in the message, refer to the *z/OS V1R1.0 DFSMS/DFP Diagnosis Reference* (GY27-7618-01) or the following Web page:

http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/BOOKS/dgt2r101/20.8.1.2

**ADHQ3001I DB2 STARTUP DETECTED FOR
SUBSYSTEM *ssid***

Explanation

The collector agent determined that a DB2 subsystem in its monitor list has started.

User response

No action is required.

**ADHQ3002I MONITORING AGENT STARTED
FOR SUBSYSTEM *ssid***

Explanation

has initiated monitoring for the named subsystem.

User response

No action is required.

**ADHQ3003I DB2 SHUTDOWN DETECTED FOR
SUBSYSTEM *ssid***

Explanation

The collector agent determined that a DB2 subsystem in its monitor list has shut down.

User response

No action is required.

**ADHQ3005I MONITORING AGENT
DEACTIVATED FOR *ssid***

Explanation

The monitoring agent has been deactivated for the indicated Collector Agent.

User response

None required.

**ADHQ3006I AUDITING AGENT ACTIVATED
FOR *ssid***

Explanation

The collector agent has been instructed to start the monitoring agent for a given DB2 subsystem when it becomes active. Monitoring of SQL for the DB2 subsystem will start when the monitoring agent is started indicated by message ADHQ3002I. Monitoring will continue after message ADHQ3002I is issued until one of the following events occur:

1. The DB2 subsystem is stopped.
2. A deactivate for the monitoring agent is performed.
3. The collector agent subsystem that is monitoring the DB2 subsystem is stopped.

User response

No action is required.

ADHQ3192E LEVEL STATUS DB2(*ssid*) message

Explanation:

This message displays if a mismatch in code level exists between and Query Monitor. One message per mismatched code level will occur.

User response:

Ensure that all the programs listed have the Query Monitor and corresponding maintenance applied.

ADHQ3192I LEVEL STATUS DB2(*ssid*) message

Explanation:

This message displays if a mismatch in code level exists between and DB2 Query Monitor. This message occurs once per mismatched code level.

User response:

Verify that all the programs listed have the Query Monitor and corresponding S-TAP for DB2 maintenance applied.

ADHQ3200I DISPLAY AGENTS

Explanation

This message is used in conjunction with other messages to indicate display agents.

User response

No action is required.

**ADHQ3201I DB2 SUBSYSTEM *ssid* AGENT
ADDRESS *address***

Explanation

Indicates the DB2 subsystem and agent address.

User response

None required.

ADHQ3202I *ssid* AGENT ADDRESS *address*

Explanation

Indicates the monitoring agent address.

User response

No action is required.

ADHQ3203I ASC DIAGNOSTIC DISPLAY:

Explanation

Indicates ASC diagnostic display is in effect.

User response

No action is required.

ADHQ3204I SDA ADDRESS *address*

Explanation

Indicates the SDA address.

User response

No action is required.

ADHQ3205I *ssid* ADDRESS *address*

Explanation

This message is used in conjunction with other messages to indicate the address.

User response

None required.

**ADHQ3206I DIAGNOSTIC DATA FOR ABEND
AT PSW *psw***

Explanation

The message displays diagnostic data for the abend.

User response

No action is required.

ADHQ3207I SYSTEM COMPLETION CODE *code*

Explanation

The message indicates the system completion code.

User response

No action is required.

ADHQ3208I OCCURRENCES *n* DATE *date* TIME *time*

Explanation

Indicates the number of occurrences and the date and time at which the took place.

User response

None required.

ADHQ3209I GPR 0-3 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM Software Support.

ADHQ3210I GPR 4-7 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM Software Support.

ADHQ3211I GPR 8-11 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM Software Support.

ADHQ3212I GPR 12-15 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM Software Support.

ADHQ3213I AR 0-3 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM Software Support.

ADHQ3214I AR 4-7 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM Software Support.

ADHQ3215I AR 8-11 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM Software Support.

ADHQ3216I AR 12-15 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM Software Support.

**ADHQ3240I DB2 QM DATASPACE USAGE
DISPLAY:**

Explanation

This message appears in conjunction with other messages as a result of the MVS Modify command **DISPLAY DATASPACE**.

User response

No action is required.

ADHQ3241I *dataspace DATASPACE*
Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS Modify command DISPLAY DATASPACEs.

User response

No action is required.

ADHQ3242I **NODE SIZE *size***
Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS Modify command **DISPLAY DATASPACEs**. This message lists the node size for the named data space.

User response

No action is required.

ADHQ3243I **TOTAL NODES *n***
Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS Modify command DISPLAY DATASPACEs. This message lists the total number of nodes allowed for the named data space.

User response

No action is required.

ADHQ3244I **AVAILABLE NODES *n***
Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS Modify command DISPLAY DATASPACEs. This message lists the total number of nodes available for use by the named data space.

User response

No action is required.

ADHQ3245I **PERCENT UTILIZED *n***
Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS Modify command DISPLAY

DATASPACEs. This message lists the percentage of nodes used for the named data space.

User response

No action is required.

ADHQ3250I **POSTING INTERVAL PROCESSOR**
Explanation

This message appears to inform you that the interval processor has been started through an MVS Modify **INTERVAL** command.

User response

No action is required.

ADHQ3251I **INTERVAL PROCESSOR NOT POSTED - DB2 UNAVAILABLE**
Explanation

The interval processor was not started because a DB2 subsystem is not available.

User response

Verify the status of all monitored DB2 subsystems.

ADHQ3252I **INTERVAL PROCESSING ALREADY IN PROGRESS**
Explanation

This message appears to inform you that the interval processor was already started through an MVS Modify **INTERVAL** command.

User response

No action is required.

ADHQ3308E **DB2 SYSTEM ssid IS MONITORED BY DB2 QUERY MONITOR ssid WHICH HAS MISMATCHED OBJ AGENT**
Explanation:

This message indicates that the maintenance levels of one or more object modules do not match between the and Query Monitor installations. The maintenance code levels for and Query Monitor installations must match.

User response:

Ensure that the maintenance levels match between the and Query Monitor installations. Apply maintenance as required to one or both environments to ensure that the maintenance levels match.

ADHQ3315E MASTER SUBSYSTEM DOES NOT MATCH

Explanation:

For monitoring and auditing to be active on the DB2 subsystem, a DB2 subsystem that is monitored by DB2 Query Monitor or Workload Replay for DB2 for z/OS or audited by must have a matching MASTER_PROCNAME parameter between the Query Monitor subsystem and the Workload Replay DB2 subsystem, or the ASC started task.

User response:

Update the MASTER_PROCNAME parameter for DB2 Query Monitor, , or Workload Replay so that the same MASTER_PROCNAME is in use by all products for the monitored DB2 subsystem. After updating the MASTER_PROCNAME, restart the started task for the task that is affected by the parameter change.

ADHQ3402I ISSUING COMMAND *cmd*

Explanation

Indicates command execution.

User response

No action is required.

**ADHQ3551E VSAM LOGIC ERROR
ENCOUNTERED WHILE
ACCESSING CONTROL FILE FOR
DB2 *ssid*. VSAMRC='rc'
VSAMRS=X'rs'**

Explanation

A VSAM logic error was encountered when accessing the control file for the DB2 subsystem indicated in the message.

User response

Verify that the DB2 control file for the DB2 subsystem listed in the message has been properly allocated and that the appropriate DB2 subsystem and plan names information have been specified correctly.

**ADHQ3552E SETUP INFORMATION MISSING
FROM CONTROL FILE FOR DB2
*ssid***

Explanation

There is insufficient information in the control file for the DB2 subsystem indicated in the message.

User response

Modify the control file to include the necessary information.

ADHQ3553E *message* ERROR *message*

Explanation

An error has occurred. This message is customized to display various messages such as initialization errors.

User response

Contact IBM Software Support.

**ADHQ4001E CONNECT TO DB2 *ssid* FAILED FOR
PLAN *plan* RETURN CODE *rc*
REASON CODE *rs***

Explanation

was not able to connect to the DB2 subsystem using the plan shown in the message.

User response

Refer to *DB2 Universal Database for z/OS V8 Messages* (GC18-9602-01) and *DB2 Universal Database for z/OS V8 Codes* (GC18-9603-01) to further diagnose and resolve the problem.

**ADHQ4003E CONNECT FAILED - DB2 NOT
OPERATIONAL**

Explanation:

The collector agent was not able to connect to the DB2 subsystem because DB2 is not currently operational.

User response:

Verify that DB2 is functioning correctly.

**ADHQ5010I MONITORING AGENT
DEINSTALLATION IN PROGRESS
FOR SUBSYSTEM *ssid***

Explanation

The monitoring agent deinstallation is in progress for the DB2 subsystem indicated in the message.

User response

No action is required.

**ADHQ5011I MONITORING AGENT
DEINSTALLATION COMPLETE FOR
SUBSYSTEM *ssid***

Explanation

The monitoring agent deinstallation completed for the DB2 subsystem indicated in the message.

User response

No action is required.

**ADHQ5012I REQUESTING MONITORING
AGENT ACTIVATION FOR DB2
SUBSYSTEM *ssid***

Explanation

The monitoring agent for the indicated DB2 subsystem is being requested for activation.

User response

No action is required.

**ADHQ5013I REQUESTING MONITORING
AGENT DEACTIVATION FOR DB2
SUBSYSTEM *ssid***

Explanation

The monitoring agent for the indicated DB2 subsystem is being requested for deactivation.

User response

No action is required.

**ADHQ6101E LOCATE FAILED FOR *dataset*
RO=*code* RC=*rc***

Explanation

A catalog located failed during interval data set expiration processing. r0 contains the contents of the register zero and rc is the LOCATE return code.

User response

See *z/OS DFSMSdfp Advanced Services* (SC26-7400-02) for a description of the return codes issued by LOCATE.

**ADHQ6102E SCRATCH FAILED FOR *file*
SCRATCH STATUS CODE=*code*
RO=*ro***

Explanation

The scratch failed for the indicated file.

User response

See *z/OS DFSMSdfp Advanced Services* (SC26-7400-02) for a description of the return codes issued by LOCATE.

**ADHQ7001E *table* TABLE NOT LOCATED IN DB2
CATALOG**

Explanation

The table indicated in the message cannot be found in the DB2 catalog.

User response

Verify that the table you specified exists.

**ADHQ7008E QUERY COMMON COLLECTOR *ssid*
NOT VALID OR HAS NOT BEEN
STARTED SINCE IPL**

Explanation

The collector agent shown in the message is not a valid collector agent.

User response

Verify that you specified the correct Query Common Collector subsystem ID, and that the collector agent is available.

**ADHQ7009E OUT OF SPACE CONDITION
DETECTED WHILE WRITING TO
THE *dsn* DATASET**

Explanation

An out-of-space condition was encountered when attempting to write to the data set indicated in the message.

User response

Verify that adequate space has been allocated to the data set.

**ADHQ7010E MISSING "ADD" PARAMETER FOR
parameter AT LINE *line* COLUMN
*column***

Explanation

The ADD parameter is missing for the indicated line and column.

User response

Specify an ADD parameter.

**ADHQ7011E INTERNAL ERROR - UNABLE TO
RESOLVE ALTERNATE COLUMN
*column***

Explanation

There has been an internal error.

User response

Contact IBM Software Support.

**ADHQ7015E NUMBER OF BSDS
SPECIFICATIONS INVALID OR
MISSING**

Explanation

An invalid number of BSDS parameters has been sent as input to the ADH#CTLF utility.

User response

Verify that the two boot strap data sets used for your DB2 subsystem are properly specified.

**ADHQ7016E DUPLICATE RECORD STORE
ATTEMPTED FOR DB2 SUBSYSTEM
ssid**

Explanation

This message describes an error condition when attempting to load records into the control file that already exist without specifying REPLACE(Y) for the DB2 subsystem indicated in the message.

User response

Edit your ADH#CTLF job to include REPLACE(Y). Refer to the instructions in SADHSAMP library member ADH#CTLF for details.

**ADHQ8001E ERRORS DETECTED IN *parameters*
PARAMETERS:**

Explanation

Errors have been detected in ADHCFGP.

User response

Verify that the parameters you specified in ADHCFGP are correct and modify any syntax errors before proceeding.

**ADHQ8002E UNIDENTIFIED KEYWORD
DETECTED AT LINE *line* COLUMN
*column***

Explanation

An unknown keyword has been found.

User response

Verify the correct syntax and modify the keyword as needed.

**ADHQ8003E INVALID SYNTAX SPECIFIED FOR
parameter NEAR LINE *line*
COLUMN *column***

Explanation

The syntax specified for the parameter indicated in the message is not valid.

User response

Correct the syntax and resubmit the job.

**ADHQ8004E PARAMETER LENGTH EXCEEDED
FOR *parameter* NEAR LINE *line*
COLUMN *column***

Explanation

The length of the value specified for the parameter indicated in the message exceeded the valid length for that parameter.

User response

Correct the syntax and resubmit the job.

**ADHQ8005E PARAMETER MISSING FOR
parameter NEAR LINE *line*
COLUMN *column***

Explanation

A required parameter is missing from ADHLOADP.

User response

Correct the syntax and resubmit the job.

**ADHQ8006E NON NUMERIC DATA SPECIFIED
FOR *parameter* NEAR LINE *line*
COLUMN *column***

Explanation

Non-numeric data was specified in ADHLOADP for the parameter listed in the message.

User response

Specify numeric data for the parameter.

**ADHQ8007E INVALID VALUE SPECIFIED FOR
parameter NEAR LINE *line*
COLUMN *column***

Explanation

An invalid value was specified in ADHLOADP.

User response

Correct the value and resubmit the job.

ADHQ8008E *value MUST BE value THAN value*

Explanation

The value of the parameter shown in the message must be within the specified range.

User response

Correct the value of the parameter so it falls within the range indicated in the message text.

ADHQ8009E **DUPLICATE PARAMETER**
parameter AT LINE line COLUMN
column

Explanation

A parameter you specified is a duplicate.

User response

Correct the syntax to eliminate the duplicate parameter.

ADHQ8010E **DUPLICATE SUBPARAMETER**
DETECTED FOR PARAMETER
parameter AT LINE line COLUMN
column

Explanation

A sub-parameter you specified is a duplicate.

User response

Correct the syntax to eliminate the duplicate sub-parameter.

ADHQ8011E **DB2 VERSION NOT SUPPORTED**

Explanation

The version of DB2 with which you are attempting to use is not supported by unload functionality of the collector agent.

User response

The collector agent unloads data to DB2 Version 8, DB2 Version 9, or DB2 Version 10.

ADHQ8012E **ERROR OPENING DDNAME**
ddname

Explanation

The collector agent encountered an error attempting to open the TEXTDATA data set.

User response

Verify that the TEXTDATA data set is configured properly and has adequate space available.

ADHQ8013E **INVALID PARAMETER LENGTH**
FOR parameter

Explanation

The value you specified for the TBCREATOR parameter is too long and is therefore invalid.

User response

Specify a valid value for TBCREATOR. Valid values are up to eight characters in length.

ADHQ8014E **LOGIC ERROR: error**

Explanation

The collector agent has encountered a logic error.

User response

Contact IBM Software Support.

ADH8022I *adh parameter value*

Explanation

This message is used to display the contents of the ADHPARMS file that was processed when was started.

User response

No action is required.

ADH9899I *adh modify command*

Explanation

This message is used to display the text of a modify command that was issued to .

User response

No action is required.

Chapter 6. ADHP102E

Invalid value for sqlcode: [*_sqlcode_*]

Explanation:

A SQL code that was detected while processing the collection policy from the IBM Guardium system is not valid.

User response:

Attempt to correct the SQL code in the collection policy by referencing the value that is reported in the message. See *SQL error codes* in the IBM Knowledge Center for more information.

Chapter 7. ADHP102E

Invalid value for sqlcode: [*_sqlcode_*]

Explanation:

A SQL code that was detected while processing the collection policy from the IBM Guardium system is not valid.

User response:

Attempt to correct the SQL code in the collection policy by referencing the value that is reported in the message. See *SQL error codes* in the IBM Knowledge Center for more information.

Notices

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

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

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

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

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com)[®] are trademarks or registered marks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at: <http://www.ibm.com/legal/copytrade.shtml>.

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

Terms and conditions for product documentation

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

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

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

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

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

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

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

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

Privacy policy considerations

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

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

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

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at <http://www.ibm.com/privacy> and IBM’s Online Privacy Statement at <http://www.ibm.com/privacy/details> the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at <http://www.ibm.com/software/info/product-privacy>.

Index

A

About this information [v](#)
accessibility
 overview [6](#)
additional documentation [27](#)
ADHEMAC1 edit macro variables [46](#)

C

CICS Login User ID reporting [15](#)
collector agent
 configuration [11](#)
collector agent started task [12](#)
compatibility with Db2 Query Monitor [3](#)
compatibility with other products [3](#)
compatible releases and maintenance levels [3](#)
components
 Guardium system [2](#)
configuration
 ADHCFGP data set [11](#)
 collector agent started task [12](#)
configuring
 additional Db2 collections [13](#)
control file
 creating [9](#)
 required statements [10](#)
cookie policy [87](#)
customizing
 JCL members [9](#)

D

data collection
 DB2 utilities [18](#)
 process [17](#)
 source of collected event types [18](#)
Db2 Query Monitor
 compatibility with collector agent [3](#)
documentation
 accessing [5](#)
 sending feedback [5](#)
dynamic LPA facility service CSVDYLPA [9](#)

E

error messages
 codes [49](#)
 collector agent messages [64](#)

F

features and functions overview [1](#)
filtering
 combined filters [19](#)
 controlling [17](#)

filtering (*continued*)
 efficiency [19](#)
 event types [19](#), [20](#)
 process [19](#)
 Stage 1 [19](#)
 Stage 2 [19](#)
 wildcarding (%) [22](#)

G

globalization [5](#)
Guardium system
 connection [31](#)

I

IBM Guardium S-TAP for Db2 [2](#)
installation environment
 architecture diagram [2](#)

J

JCL
 ADHBIND [11](#)

L

legal notices
 cookie policy [87](#)
 notices [87](#)
 programming interface information [87](#)
 trademarks [87](#)
links
 non-IBM Web sites [88](#)
LOAD library
 APF authorizing [8](#)

M

Master Address Space
 considerations for stopping [15](#)
 overview [14](#)
 usage considerations [14](#)
MODIFY command [28](#)
Multistreaming
 Enabling multistream mode [23](#)

N

notices [87](#)

P

parameters [31](#)
policy pushdown [22](#)

programming interface information [87](#)

R

reader comment form [5](#)
reference information [27](#)
reporting
 CICS Login User ID [15](#)

S

S-TAP logging
 requesting [31](#)
 viewing [31](#)
sample library members [27](#)
sample parameter file [45](#)
screen readers and magnifiers [6](#)
service information [5](#)
SQL Blocking [24](#)
SQL event filtering
 Stage 1 filtering [19](#), [20](#)
 Stage 2 filtering
 improving efficiency [19](#)
support information [5](#)

T

technotes [5](#)
trademarks [87](#)

U

upgrading from previous versions [7](#)
user IDs
 required user ID authorizations [4](#)

V

V10.1.3 enhancements [1](#)



Product Number: 5655-STQ

SC27-8020

