11.3

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.

2024-04-24 Edition

This edition applies to Version 11 Release 3 of IBM® Security Guardium® S-TAP® for Db2 on z/OS® (product number 5656-STQ) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this information..... vii

Chapter 1. Environment and requirements..... 1
The IBM Security Guardium S-TAP for Db2 on z/OS architecture and components.....1
Hardware and software prerequisites.....3
Compatibility with IBM Db2 Query Monitor for z/OS and other products..... 3
Db2 function level support.....4
Upgrading from previous versions of IBM Security Guardium S-TAP for Db2.....5
IBM Security Guardium S-TAP for Db2 security.....6
IBM Security Guardium S-TAP for z/OS security recommendations..... 6
APF authorizing the LOAD library data set.....6
Required user ID authorizations..... 7
Globalization..... 7
Service updates and support information.....8
Product documentation and updates.....8
Accessibility features.....9

Chapter 2. Configuring IBM Security Guardium S-TAP for Db2 on z/OS..... 11
Enabling the dynamic LPA facility service CSVDYLPA.....12
Service class considerations..... 12
Customizing JCL members..... 12
Creating the IBM Security Guardium S-TAP for Db2 control file..... 12
Configuring the IBM Security Guardium S-TAP for Db2 control file..... 13
Required statements for each subsystem.....13
Configuring the collector agent..... 14
Configuring the JCL for ADHBIND.....14
Configuring the JCL for ADHGRANT.....14
Configuring the ADHCFGP data set.....14
Defining the collector agent started task JCL.....15
Collector agent parameters.....16
APPLIANCE_CONNECT_RETRY_COUNT..... 16
APPLIANCE_NETWORK_REQUEST_TIMEOUT.....17
APPLIANCE_PING_RATE..... 17
APPLIANCE_PORT.....18
APPLIANCE_RETRY_INTERVAL..... 18
APPLIANCE_SERVER.....19
APPLIANCE_SERVER_LIST..... 19
AUDIT.....21
AUTHID..... 21
CICS_USERID..... 22
COLLECT_COMMIT_ROLLBACK.....22
DEBUG..... 22
DIAG_THRESHOLD.....23
DIAG_THRESHOLD_DUMPS.....23
FORCE..... 24
HOSTVAR_LIMIT..... 24
ISM_CONSTRAINT_AGE.....25
ISM_ERROR_DETAIL.....25
/f cqmstc, ISMERROR_DETAIL..... 26
ISM_ERROR_BLOCKS..... 26

ISM_ERROR_MSG_BLOCKS....27
MASTER_PROCNAME....27
MAXIMUM_ALLOCATIONS....28
MESSAGE_LOG_LEVEL....28
OUTAGE_SPILLAREA_SIZE....29
PREFER_IPV4_STACK....30
SEND_FAIL_EVENT_COUNT....30
SMEM_SIZE....31
STAP_BLOCKING....32
STAP_MEGABUFFER....32
STAP_STREAM_EVENTS....33
STAP_STREAM_GTT_EVENTS....33
STAP_TERMINATE_OPTIMIZE....34
STAP_UTILITY_MULTITABLE....34
STAP_UTILITY_TS_TO_TABLE....35
STARTUP_DIAGNOSTICS....35
SHUTDOWN_DIAGNOSTICS....36
SUBSYS....36
TS_OFFSET....37
ZIIP_FILTER....37
ZIIP_TCP....38
Configuring the collector agent for additional Db2 subsystems....38
Configuring data streaming modes....39
Configuring Single Appliance mode....40
Configuring Failover mode....41
Configuring Hot Failover mode....41
Configuring Multistream mode....42
Configuring Mirroring mode....42
Support Services Address Space overview....43
Usage considerations for the Primary Address Space....43
Stopping the Primary Address Space....44
Enabling CICS Login User ID reporting....44

Chapter 3. Managing data collection....45
Data collection process....45
Collection policy....45
Collected event types....46
Filtering....48
Event types and filtering....49
Filtering by database name....51
Filter wildcard support....51
Policy pushdown....51
Starting and stopping the collector agent....52
Quarantining SQL activity....53
SQL Blocking....53

Chapter 4. Reference information....55
Sample library members....55
MODIFY command....56
S-TAP logging....59
Keeping connections active when HOT_FAILOVER is enabled....59
Collector agent sample parameter file....59
ADHEMAC1 edit macro variables....60

Chapter 5. Messages and codes for IBM Security Guardium S-TAP for Db2 on z/OS....63
Error messages....63

Error messages and codes: ADHAxxx..... 63
Error messages and codes: ADHGxxx..... 64
Error messages and codes: ADHIxxxx..... 69
Error messages and codes: ADHKxxxx..... 70
Error messages and codes: ADHPxxxx.....71
Error messages and codes: ADHQxxxx..... 80
Error messages and codes: FECxxxx.....99

Notices.....115
Trademarks..... 116
Terms and conditions for product documentation..... 116
Privacy policy considerations..... 117

Index..... 119

About this information

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

These topics provide instructions for installing, configuring, and using IBM Security 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 installation
- Install and operate
- Customize your environment
- Diagnose and recover from problems
- Design and write applications
- Use with other Db2® or IMS products

Tip: To find the most current version of this information, always use the Security Guardium Documentation: https://www.ibm.com/docs/en/guardium

Chapter 1. Environment and requirements

The IBM Security Guardium S-TAP for Db2 on z/OS (IBM Security Guardium S-TAP for Db2) collects and correlates data access information from Db2 to produce a comprehensive view of business activity for auditors. IBM Security 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 Security 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, TRUNCATE, MERGE)
- Reads of an object (SQL SELECT)
- LOCK of either TABLE or TABLESPACE object
- 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, DROP, and RENAME 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 Security Guardium S-TAP for Db2 uses Db2 data sharing to obtain audit information from all members of the data sharing group.

IBM Security Guardium S-TAP for Db2 on z/OS architecture and components

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

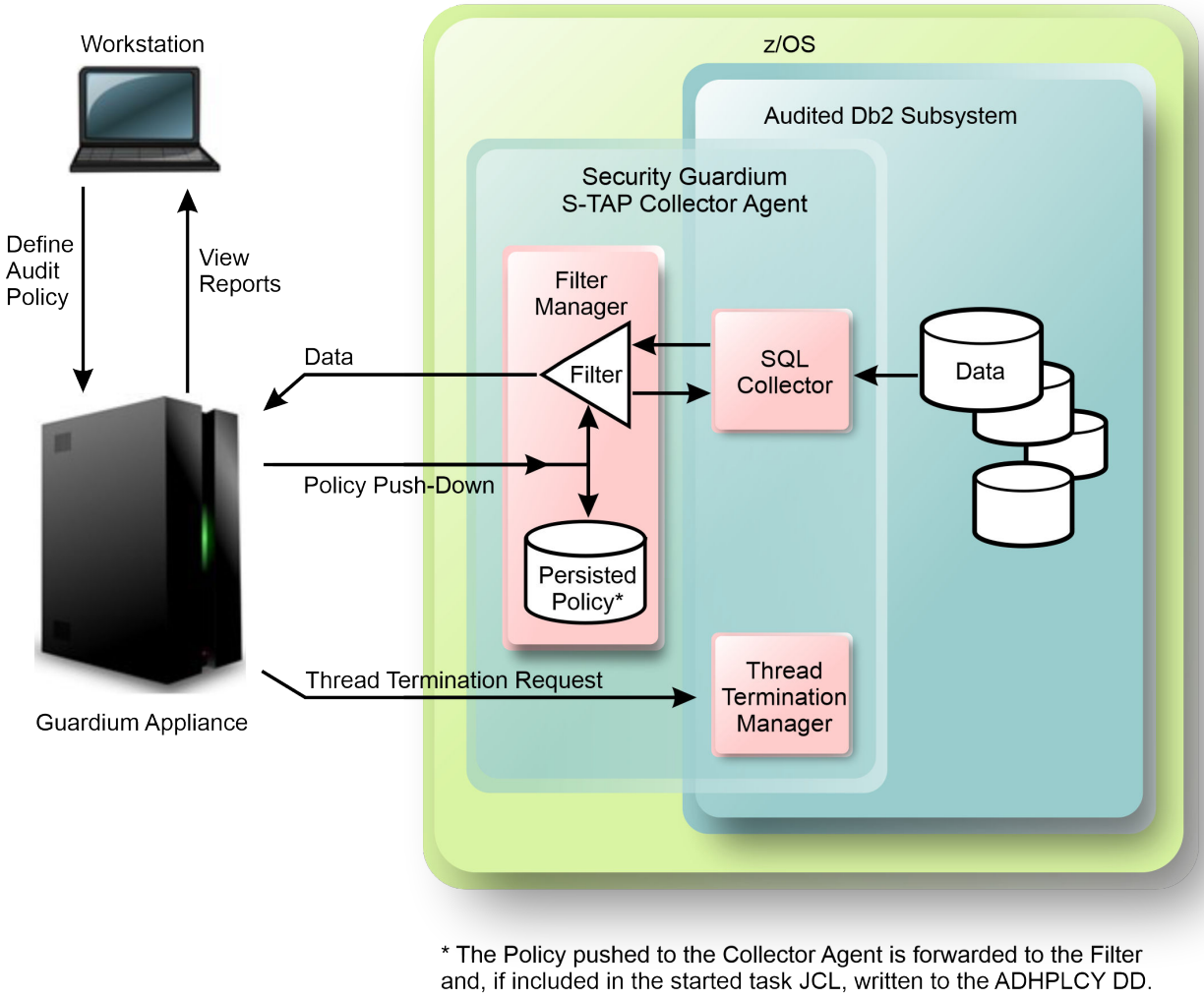

Figure 1. The IBM Security Guardium S-TAP for Db2 V11.3 architecture

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 Security 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 Security 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 51.

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 Security 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.

Hardware and software prerequisites

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

FEC common code FMID H25F132 is required and must be on your system to successfully install this product.

IBM Db2 Data Access Common Collector for z/OS V1.1 (CQC) common code FMID HCQC110 is required and must be on your system to successfully install this product.

Hardware requirements

Any hardware capable of running Db2 for z/OS Version 11 or later, until end of service.

Collector agent requirements

- Db2 Version 11 or later, until end of service.
- z/OS Version 2 Release 3 or later, until end of service.
- You must run the IBM Security Guardium S-TAP for Db2 collector agent on an operating system version that is equivalent to the operating system version you perform the product SMP/E installation.
- You must configure and enable Resource Recovery Services (RRS) to use the RRSAF attachment facility to connect to Db2.

Compatibility with IBM Db2 Query Monitor for z/OS

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

To implement Db2 Query Monitor, your site must meet operating system, environment, hardware, software, and network requirements. For information about installing and operating Db2 Query Monitor, see IBM Db2 Query Monitor for z/OS.

Compatible releases and maintenance levels

The two products can coexist in the following ways:

LPAR
: The two product's releases can coexist on the same LPAR when each uses a different primary name, but both 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.

The following table uses these product abbreviations:

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

Table 1. Compatible releases and maintenance levels				
	CQM 3.3	**CQM 3.4**	**STP 10.1.3**	**STP 11.3**
CQM 3.3	–––	–––	Db2	Db2
CQM 3.4	–––	–––	Db2	Db2
STP 10.1.3	Db2	Db2	–––	LPAR
STP 11.3	Db2	Db2	LPAR	–––

Db2 function level support

When you activate new Db2 function levels in a Db2 subsystem or data sharing group, enhancements might become available that impact IBM Security Guardium S-TAP for Db2.

The levels of function level support are defined as follows:

Tolerated
IBM Security Guardium S-TAP for Db2 works as it did on a previous release or function level of IBM Security Guardium S-TAP for Db2, but does not support the new features of this function level.

Supported
IBM Security Guardium S-TAP for Db2 supports most, but not necessarily all, of the new function-level features that IBM deems the most significant.

General considerations

S-TAP uses FMID HCQC110 to install monitoring agents in Db2. Hence, when Db2 is stopped and restarted, S-TAP detects whether Db2 startup and its monitoring agents are installed. It is recommended to follow these best practices for S-TAP and Db2 maintenance, or when activating a Function Level:

- When applying service levels for Db2, apply the same to S-TAP.
- When stopping Db2, stop S-TAP as well. This can clean up the S-TAP-started task memory that is associated with the previously running Db2.
- For a new function level or version of Db2, it is recommended to stop S-TAP and STAPMSTR.
- For STAP-only service upgrades, it is recommended to stop both S-TAP and STAPMSTR. After maintenance, recycle both S-TAP and STAPMSTR to avoid missing the STAPMSTR restart when it is required.
- When applying service levels to z/OS, the current service levels of S-TAP should be installed.

The following function levels are tolerated or supported by IBM Security Guardium S-TAP for Db2 and are listed with the corresponding PTF, if any are available. PTFs are listed with the function level they were first introduced. Later function levels require installation of PTFs introduced by prior function levels.

IBM Security Guardium S-TAP for Db2 PTFs in support of Db2 13 function levels

Db2 13 function level	Toleration PTF	Support PTF
FL504 - October 2023	No PTF required	No PTF required
FL503 - February 2023	No PTF required	No PTF required
FL502 - October 2022	No PTF required	No PTF required
FL501 - May 2022	• IBM Security Guardium S-TAP for Db2: UI79611 • IBM Db2 Data Access Common Collector: UI80706	No PTF required

Db2 13 function level	Toleration PTF	Support PTF
FL500 - May 2022	• IBM Security Guardium S-TAP for Db2: UI79611 • IBM Db2 Data Access Common Collector: UI80706	No PTF required

IBM Security Guardium S-TAP for Db2 PTFs in support of Db2 12 function levels

Db2 12 function level	Toleration PTF	Support PTF
FL509: APAR PH33015 - February 2021	No PTF required	No PTF required
FL508: APAR PH29392 - October 2020	No PTF required	No PTF required
FL507: APAR PH24371 - June 2020	No PTF required	No PTF required
FL506: APAR PH16829 - October 2019	No PTF required	No PTF required
FL505: APAR PH09191 - June 2019	No PTF required	No PTF required
FL504: APAR PH07672 - April 2019	No PTF required	No PTF required
FL503: APAR PH00506 - October 2018	No PTF required	No PTF required
FL502: APAR PI95511 - May 2018	No PTF required	No PTF required
FL501: APAR PI70535 - May 2017	No PTF required	No PTF required
FL500: October 2016	No PTF required	No PTF required

Upgrading from previous versions of IBM Security Guardium S-TAP for Db2

You can upgrade to IBM Security Guardium S-TAP for Db2 V11.3 from IBM Security Guardium S-TAP for Db2 V9.0, V9.1, V10.0, or V10.1.3 by completing these steps.

Procedure

1. Stop the previous version's collector agent.
2. Stop the previous version's master address space using SAMPLIB member ADHMSTR.

   Note: The ADHMSTR JCL is used to stop the master address space. The address space can be stopped only if all IBM Security Guardium S-TAP for Db2 and Db2 Query Monitor (if installed and active) systems have been stopped.
3. Complete the SMP/E installation of IBM Security Guardium S-TAP for Db2 V11.3.
4. APF-authorize the V11.3 SADHLOAD, SCQCLOAD, and SFECLOAD data sets.
5. Customize and run the V11.3 Db2 bind job in SADHSAMP(ADHBIND).
6. Customize and run the V11.3 Db2 grant job in SADHSAMP(ADHGRANT).
7. Update the collector started task JCL (ADHC*ssid*) to:

- Remove the previous version of the product SADHLOAD, SCQCLOAD, and SFECLOAD data sets.
- Include the new V11.3 product SADHLOAD, SCQCLOAD, and SFECLOAD data sets in the STEPLIB DD concatenation members.

8. Update the V11.3 collector configuration member SADHSAMP(ADHCFGP).

   Tip: For this step, use the configuration from V10.1.3 to update for V11.3.
9. Start the collector address space by entering `/S ADHC`*`ssid`* at the z/OS command prompt.

What to do next

You can now install policies on the z/OS host using the IBM Security Guardium interface.

IBM Security Guardium S-TAP for Db2 security

IBM Security Guardium S-TAP for Db2 requires access to data sets and components.

IBM Security Guardium S-TAP for z/OS security recommendations

The following security recommendations apply to S-TAP for Db2, IMS, and Data Sets.

- Define the ID assigned to the S-TAP started tasks via system authorization facility (SAF) to the S-TAP product load libraries with READ ONLY access.
- The ID assigned to the S-TAP started tasks should not be able to log on to TSO and should be designated for the exclusive use of the S-TAP started tasks.
- Ensure that the only TSO ID's able to update access to the S-TAP product load libraries are those that perform product installation and apply product maintenance.
- Security administrators need to work with systems programmers to ensure that the contents of APF/LINKLIST/LPA lists of program libraries are maintained correctly. Update access to these libraries must be defined for each library, independently of the RACF controls.
- Ensure verify the source of all APF authorized and system code that you install. If possible, get statements of assurance from the suppliers.
- Manage your APF lists with great care. Double-check entries. Do not leave dead entries in the list for simplicity or ease of use. Use a formal checker for the lists if possible.
- Do not grant READ access for any configuration libraries except to users with a defined business need.
- Strictly follow the documented values for UACC values for system data sets.

For details on security practices, see *IBM Redbooks Solution Guide* Securing the IBM Mainframe.

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 Security Guardium S-TAP for Db2 data set, as specified by ADHEMAC1 macro value #SADHLOAD, as an APF authorized library.

About this task

The IBM Security 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
- adhhlq.SADHLOAD
- the FEC data set fechlq.SFECLOAD (where *adhhlq* and *fechlq* are the data set high level qualifier where S-TAP and FEC products are installed)

- the CQC data set cqchlq.SCQCLOAD (where adhhlq 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.

Required user ID authorizations

To operate IBM Security 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 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 Security 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 Security 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

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

Information on the web

IBM Security Guardium on IBM Documentation provides current product documentation that you can view, print, and download:

https://www.ibm.com/docs/en/guardium

The Db2 Tools Product Documentation web page provides current product documentation that you can view, print, and download:

https://www.ibm.com/support/pages/db2-tools-zos-product-documentation

You can access documentation for many Db2 Tools from IBM Documentation:

https://www.ibm.com/docs/en

IBM Redbooks® publications that cover Db2 Tools are available at:

http://www.redbooks.ibm.com

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 https://www.ibm.com/support/pages/about-my-notifications.
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 Security 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.

Important: If a user ID and/or S-TAP for z/OS collector agent started task name is changed or a new ID or procedure is added after you completed configuration, that user ID or S-TAP z/OS collector agent started task name is considered new and you'll need to complete some configuration steps again, as follows.

For any new or changed user ID or S-TAP z/OS collector agent started task name, complete:

- Step 3 | Binding DBRMs using the JCL bind job
- Step 7 | Configuring the collector agent

For any new or changed user ID:

- Verify user ID authorizations shown in “Required user ID authorizations” on page 7.

Before you begin

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

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

Table 2. Configuration steps

Step	Configuration step	SADHSAMP sample library member
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 Security Guardium S-TAP for Db2 control file	ADHSJ000
6	Configuring the IBM Security 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

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 Security 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 Security Guardium S-TAP for Db2 control file

IBM Security 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 Security 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 Security Guardium S-TAP for Db2 control file

IBM Security 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 Security 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 Security 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 13.

   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

Table 3. Required statements for each subsystem (continued)	
Statement	**Setting**
UPDATE DB2 LOADLIB 1	#SDSNEXIT
UPDATE DB2 LOADLIB 2	#SDSNLOAD
SET PRODUCT CFG	NULL
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 Security 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 Security 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 Security 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 Security 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 Security 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 Security 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 ADHC*SSID* contains the sample JCL to set up the IBM Security 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 ADHC*SSID* 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 ADHC*SSID* 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 ADHC*SSID*, 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 Security Guardium S-TAP for Db2 collector agent configuration file.

   DB2PARMS
   DB2PARMS must name the IBM Security 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 51.

   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 Security Guardium S-TAP for Db2 collector agent log messages will be written.

   STEPLIB
   STEPLIB must include the IBM Security 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 Security Guardium S-TAP for Db2 for installation and configuration.

Collector agent parameters

The collector agent parameters are described in this section.

APPLIANCE_CONNECT_RETRY_COUNT

Use APPLIANCE_CONNECT_RETRY_COUNT to specify the number of consecutive failed connection attempts before terminating.

Required
No

Default
0

Permitted values
0 - 65535

Description

Specify the number of consecutive failed connection attempts before terminating. Set to 0 to never stop attempting connections. Set to 1 to stop immediately after a connection attempt fails.

Notes

None

Syntax

```
APPLIANCE_CONNECT_RETRY_COUNT(retry_count)
```

Example

```
APPLIANCE_CONNECT_RETRY_COUNT(1000)
```

APPLIANCE_NETWORK_REQUEST_TIMEOUT

Use APPLIANCE_NETWORK_REQUEST_TIMEOUT to specify the period of time to wait for a network send or receive request to complete.

Required

No

Default

500

Permitted values

0 or 500 - 12000 milliseconds

Description

Specify the period of time to wait for a network send or receive request to complete. A value of 0 results in an infinite timeout period.

Notes

None

Syntax

```
APPLIANCE_NETWORK_REQUEST_TIMEOUT(milliseconds)
```

Example

```
APPLIANCE_NETWORK_REQUEST_TIMEOUT(0)
```

APPLIANCE_PING_RATE

You can ping the IBM Security Guardium system to prevent timeouts and disconnects during idle times. Do not change the value of this keyword unless directed by IBM Support.

Required

No

Default

5

Permitted Values

1 - 65535 seconds

Description

Specify the number of seconds between pings checking that the IBM Security Guardium system is active and available for communications. These checks can prevent timeouts and disconnects during idle periods.

Notes

None

Syntax

```
APPLIANCE_PING_RATE(ping_interval)
```

Example

```
APPLIANCE_PING_RATE(5)
```

APPLIANCE_PORT

APPLIANCE_PORT sets the port that Guardium appliance listens to the S-TAP and is dedicated to the IP address of the appliance.

Required
No

Default
16022

Valid ports
16022 or 16023

Description
Specify the port number used to communicate with the IBM Security Guardium system.

Notes
You must correctly configure this keyword to enable collection of audit data and a connection to the IBM Security Guardium system. Note the following:

- If port 16023 is used, encryption support is required to connect to the appliance.

Syntax

```
APPLIANCE_PORT(port_number)
```

Example

```
APPLIANCE_PORT(16022)
```

APPLIANCE_RETRY_INTERVAL

APPLIANCE_RETRY_INTERVAL specifies the time between attempts to connect to IBM Security Guardium system.

Required
No

Default
3

Permitted Values
0 - 65535 seconds

Description
Specify the time in seconds between attempts to establish a connection to the IBM Security Guardium system after a connection attempt fails.

Notes
None

Syntax

```
APPLIANCE_RETRY_INTERVAL(retry_interval)
```

Example

```
APPLIANCE_RETRY_INTERVAL(3)
```

APPLIANCE_SERVER

APPLIANCE_SERVER specifies the address of the IBM Security Guardium system you want to connect to. Use this keyword to enable collection of audit data and a connection to the IBM Security Guardium system.

Required
Yes

Default
No default

Permitted Values
Maximum 53 characters

Description

Identify the host name or IP address of the IBM Security Guardium system you want to connect to. In multistream processing scenarios, this address specifies the first IBM Security Guardium to use.

You can specify the address as a host name, as four numbers separated by periods, or as an IPV6 address, for example:

- *guardium.customer.net*
- 188.128.6.42
- 2001:21:21:55:53::25

Notes
None

Syntax

```
APPLIANCE_SERVER(address)
```

Example

```
APPLIANCE_SERVER(192.168.2.205)
```

APPLIANCE_SERVER_LIST

Use APPLIANCE_SERVER_LIST to determine streaming behavior when multiple appliances are defined.

Required
No

Default
FAILOVER

Permitted Values

Value	Description
FAILOVER	Set to **FAILOVER** to make one Guardium appliance connection 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. You can set the next available server using **APPLIANCE_SERVER_n** or **APPLIANCE_SERVER_FAILOVER_n**. • After a failover occurs, the connection to the primary server is retried at regular intervals you can set using **APPLIANCE_PING_RATE**.

Value	Description
MULTI_STREAM	Set to **MULTI_STREAM** to establish a Guardium appliance connection for each server identified by the **APPLIANCE_SERVER_n** or **APPLIANCE_SERVER_LIST_n** keyword. • If a connection is lost, S-TAP audit events continue to transmit over the remaining appliance connection. • Lost connections are retried at regular intervals you can set using **APPLIANCE_PING_RATE**.
HOT_FAILOVER	Set to **HOT_FAILOVER** to keep each connected Guardium appliance active via pings, and send the same events data to all connected Guardium appliances. Set the connection types (POLICY and ASC) for each connected Guardium appliance to keep active via pings. You can specify the primary Guardium appliance using **APPLIANCE_SERVER**. If the primary Guardium appliance becomes unavailable and failover occurs, **HOT_FAILOVER** maintains the activity of the primary appliance policy.
MIRROR	Set to **MIRROR** to keep each connected Guardium appliance active via pings, and send the same events data to all connected Guardium appliances. Set the connection types (POLICY and ASC) for each connected Guardium appliance to keep active via pings. You can specify the primary Guardium appliance using **APPLIANCE_SERVER**. If the primary Guardium appliance becomes unavailable and failover occurs, **MIRROR** maintains the activity of the primary appliance policy.

Description

When you use **APPLIANCE_SERVER_LIST** and you specified a spill file with keyword **OUTAGE_SPILLAREA_SIZE**, when all connections fail, events are buffered to the spill file until a connection becomes available. If no spill file is specified, and all connections fail, data loss occurs.

Notes

None

Syntax

```
APPLIANCE_SERVER_LIST(FAILOVER)
```

Example

```
APPLIANCE_SERVER_LIST(FAILOVER)
```

AUDIT

Specify a Db2 subsystem ID for the Db2 subsystem you want to capture query data on.

Required
Yes

Default
No default

Permitted Values
Maximum 26 characters

Description
Set a Db2 subsystem ID for the Db2 subsystem that the IBM Security Guardium S-TAP for Db2 collector agent captures query data on.

Notes
None

Syntax

```
AUDIT(ssid)
```

Example

```
AUDIT(DSN1)
```

AUTHID

Specify a Db2 user name Db2 uses to establish a connection to Db2 during interval processing.

Required
No

Default
Defaults to the user ID used to run the started task.

Permitted Values
A valid TSO user ID.

Description
The AUTHID parameter defines the Db2 AUTHID that Db2 uses to establish 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 you specify must be authorized through the resident security package, such as RACF, so that the started task and Collector Agent monitoring subsystem can complete processes. These processes include connecting to each of the monitored Db2 SSIDs and performing file update activities against the Db2 VSAM control file.

Notes

- The ID specified in the startup parameter AUTHID must be a valid TSO user ID and not a RACF group name.
- If the AUTHID parameter is defined in the RACF Started Procedures Table (ICHRIN03), do not use that parameter for startup. The Started Procedures Table (ICHRIN03) associates the names of started procedures with specific RACF user IDs and group names, and 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 instead of the started procedures table.

Syntax

```
AUTHID(db2authid)
```

Example

```
AUTHID(DB2USER)
```

CICS_USERID

Use CICS_USERID to enable capture of CICS Login User ID for SQL statements run in Db2 for CICS.

Required
N

Default
N

Permitted Values
N, Y

Description
If set to Y, you can capture CICS Login User ID for SQL statements run in Db2 for CICS. For more information, refer to *Enabling CICS login user ID reporting* in this guide.

Notes
None

Syntax

```
CICS_USERID(N)
```

Example

```
CICS_USERID(Y)
```

COLLECT_COMMIT_ROLLBACK

COLLECT_COMMIT_ROLLBACK enables collection of COMMIT and ROLLBACK events.

Required
No

Default
N

Permitted Values
N, Y

Description
Set to Y to collect COMMIT and ROLLBACK events.

Notes
None

Syntax

```
COLLECT_COMMIT_ROLLBACK(N)
```

Example

```
COLLECT_COMMIT_ROLLBACK(Y)
```

DEBUG

Enable DEBUG to produce diagnostic messages that help troubleshoot issues.

Required
No

Default
N

Permitted Values
N, Y

Description
Enable debug mode and produce diagnostic messages that IBM Software Support can use to troubleshoot.

Notes
None

Syntax

```
DEBUG(N)
```

Example

```
DEBUG(Y)
```

DIAG_THRESHOLD

Specify the number of internal abends that, when exceeded, causes message ADHQ4401I to be issued. Change the value for this parameter only under the direction of IBM Support.

Required
No

Default
1000000

Permitted Values
0 - 99999999

Description
When this parameter is set to 0, the internal diagnostic threshold checker is not activated and ADHQ4401W is not issued. Additionally, regardless of the value of DIAG_THRESHOLD_DUMPS, no dumps are produced for internal abends.

If a value greater than 0 is specified for this parameter, message ADHQ4401I is issued if that value is exceeded.

Notes
None

Syntax

```
DIAG_THRESHOLD(n)
```

Example

```
DIAG_THRESHOLD(1000000)
```

DIAG_THRESHOLD_DUMPS

Specify the number of dumps to produce after the threshold for an internal abend set by DIAG_THRESHOLD is exceeded. Change the value for this parameter only under the direction of IBM Support.

Required
No

Default
1

Permitted Values
0 - 5

Description
When set to a value greater than 0, message ADHQ4402I is issued and a dump is produced.

Note: It is possible that not all dumps will be produced if the Db2 thread encounters the internal abend and an asynchronous dump is still in progress for that thread. In such cases, a return code might be reported that indicates another dump from an abend event is still in progress.

When this parameter is set to 0, no dumps are produced and message ADHQ4402I is not issued after the threshold value set by DIAG_THRESHOLD is exceeded.

Notes
None

Syntax

```
DIAG_THRESHOLD_DUMP(n)
```

Example
If, for example, the following is specified, a dump is generated for the 3 next occurrences after 999999 (1000000,1000001,1000002):

```
DIAG_THRESHOLD_DUMPS(3)
DIAG_THRESHOLD(1000000)
```

And if the following is specified, message ADHQ4401I is issued only once after 1000000 and no dumps are produced:

```
DIAG_THRESHOLD_DUMPS(0)
DIAG_THRESHOLD(1000000)
```

FORCE

The FORCE parameter forces installation of a monitoring agent.

Required
No

Default
N

Permitted Values
N, Y

Description
If you use this parameter, return codes from any failure reported in message ADHQ2002E are overridden.

Notes
Do not change the value of this parameter unless directed by IBM Support.

Syntax

```
FORCE(N)
```

Example

```
FORCE(Y)
```

HOSTVAR_LIMIT

HOSTVAR_LIMIT sets the number of storage blocks to allocate for host variable collection per event.

Required
No

Default
1500

Permitted Values
1 - 9999 storage blocks

Description

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

If Db2 and Db2 Query Monitor are simultaneously monitoring the same Db2 subsystem, both products must have matching HOSTVAR_LIMIT settings to avoid receiving a mismatch error.

Notes
None

Syntax

```
HOSTVAR_LIMIT(n)
```

Example

```
HOSTVAR_LIMIT(1500)
```

ISM_CONSTRAINT_AGE

ISM_CONSTRAINT_AGE determines when a constraint occurrence is considered relieved.

Required
No

Default
300

Permitted Values
1 - 60000 milliseconds

Description
For a given ISM storage space, specify how much time must pass between storage constraint occurrences after which the constraint event is considered relieved.

Notes
None

Syntax

```
ISM_CONSTRAINT_AGE(milliseconds)
```

Example

```
ISM_CONSTRAINT_AGE(16)
```

ISM_ERROR_DETAIL

ISM_ERROR_DETAIL controls whether messages ADHQ1203I and ADHQ1204I are issued to provide detailed information for ISM Storage Constraint situations.

Required
No

Default
Y

Permitted Values
N, Y

Description
It is recommended to leave this parameter set to Y. You can override this parameter at run time with the **/f cqmstc,ISMERROR_DETAIL** command.

Notes
None

Syntax

```
ISM_ERROR_DETAIL(Y)
```

Example

```
ISM_ERROR_DETAIL(Y)
```

/f cqmstc, ISMERROR_DETAIL

/f cqmstc, ISMERROR_DETAIL 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.

Required
No

Default
N

Permitted Values
N, Y

Description
You can override ISM_ERROR_DETAIL at run time with /f cqmstc,ISMERROR_DETAIL.

Notes
None

Syntax

```
/f cqmstc,ISMERROR_DETAIL(N)
```

Example

```
/f cqmstc,ISMERROR_DETAIL(Y)
```

ISM_ERROR_BLOCKS

Set ISM_ERROR_BLOCKS to determine the number of ISM Error Blocks allocated when Db2 initializes.

Required
No

Default
256 error blocks

Permitted Values
1 - 1024 error blocks

Description

If this value is too low, message ADHQ1219W might be issued. ISM Error Blocks communicate a storage constraint event 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 does not impact the performance of Db2.

Notes
None

Syntax

```
ISM_ERROR_BLOCKS(n)
```

Example

```
ISM_ERROR_BLOCKS(256)
```

ISM_ERROR_MSG_BLOCKS

ISM_ERROR_MSG_BLOCKS determines the number of ISM Error Message Blocks allocated when Db2 initializes.

Required
No

Default
256

Permitted Values
16 - 8192

Description

Specify the number of ISM Error Message Blocks allocated when 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:

- To consolidate similar storage constraint events to eliminate duplicate messaging for the same condition
- 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. Additional, duplicate messages show up in the log for similar storage constraint events.

Notes
None

Syntax

```
ISM_ERROR_MSG_BLOCKS(n)
```

Example

```
ISM_ERROR_MSG_BLOCKS(256)
```

MASTER_PROCNAME

MASTER_PROCNAME enables you to specify the PROCNAME to be used for the Primary Address Space.

Required
No

Default
No default

Permitted Values
character, maximum of 8 bytes

Description
Use of this parameter causes Db2 to use the Primary Address Space with the same name.

- The MASTER_PROCNAME for Db2 and Query Monitor must be the same when each is started at the same time for the same Db2 Subsystem.
- If this Primary Address Space is already started, it is shared with other Db2 subsystems that are already using it.

- If this Primary Address Space has not already been started, it will start automatically.

Notes
None

Syntax

```
MASTER_PROCNAME(procname)
```

Example

```
MASTER_PROCNAME(CQMMASTR)
```

MAXIMUM_ALLOCATIONS

Use MAXIMUM_ALLOCATIONS to specify the maximum amount of global shared memory that Db2 allocates for internal Integrated Storage Manager spaces.

Required
No

Default
2048 megabytes

Permitted Values
512 - 32768 megabytes

Description

Use this parameter in conjunction with the SMEM_SIZE parameter. The SMEM_SIZE parameter value must be equal to or greater than four times the MAXIMUM_ALLOCATIONS parameter value. If you specify a SMEM_SIZE value less than four times the value of MAXIMUM_ALLOCATIONS, then Db2 automatically adjusts the SMEM_SIZE value to be four times greater than the MAXIMUM_ALLOCATIONS value.

If Db2 and Db2 Query Monitor are simultaneously monitoring the same Db2 subsystem, the MAXIMUM_ALLOCATION value(s) from the respective product (either Query Monitor or STAP) is used to limit the amount of memory allocated from the shared memory objects. The MAXIMUM_ALLOCATIONS values for the two products do not have to match.

Notes
None

Syntax

```
MAXIMUM_ALLOCATIONS(n)
```

Example

```
MAXIMUM_ALLOCATIONS(2048)
```

MESSAGE_LOG_LEVEL

Use MESSAGE_LOG_LEVEL to specify the severity of error messages you want to log for.

Required
No

Default
I

Permitted Values
I, W, E, S

Description

Table 4. Message severity codes and descriptions.

During installation, set MESSAGE_LOG_LEVEL to I to generate messages for installation problems. After the installation is complete, revert the value to the default.

Message severity code	Description
I	Includes all log messages
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* error code

Notes

Changes to the log-level setting are not applied until you restart the collector agent.

Syntax

```
MESSAGE_LOG_LEVEL(I)
```

Example

```
MESSAGE_LOG_LEVEL(W)
```

OUTAGE_SPILLAREA_SIZE

OUTAGE_SPILLAREA_SIZE sets the size of the spill file to use in the event of a Guardium system connection outage.

Required

No

Default

No default

Permitted Values

0 – 1024 megabytes

Description

A value of 0, or the absence of this keyword, disables spill area support and the creation of a spill file.

If you enable OUTAGE_SPILLAREA_SIZE, an internal memory buffer (a spill file) is created that temporarily stores events in the case of a Guardium appliance connection outage. Events are stored in the memory buffer until the memory buffer is full or a connection is restored to the appliance. When connectivity is re-established, events are streamed to the appliance in order of 'first in first out' (oldest event first) until emptied. The memory buffer is not circular. When the spill file is full, events are no longer stored and are discarded.

The spill file is meant for short-term outages only because when a connection is restored, the Guardium system clears the spill file content before continuing to send data.

When you enable a spill file and do not specify a secondary APPLIANCE_SERVER_FAILOVER address, or none of the secondary APPLIANCE_SERVER_FAILOVER addresses respond, the Guardium product writes to the spill file

Notes

When enabled, this parameter supersedes SEND_FAIL_EVENT_COUNT for temporary data retention.

Syntax

```
OUTAGE_SPILLAREA_SIZE(n)
```

Example

```
OUTAGE_SPILLAREA_SIZE(2)
```

PREFER_IPV4_STACK

You can use PREFER_IPV4_STACK to return an IPV4 address of the host name used to connect to the Guardium appliance.

Required
No

Default
N

Permitted Values
N, Y

Description

If set to Y, this keyword causes a request to be issued to the Domain Name Server (DNS) for an IPV4 address of the host name specified by the APPLIANCE_SERVER keyword:

- The DNS lookup request for an IPV4 address is attempted. If an IPV4 address is defined for the host name, the DNS responds with the value used to connect to the Guardium appliance.
- If the DNS defines only an IPV6 address, the DNS responds with the IPV6 address used to connect to the Guardium appliance.
- If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS responds with both addresses, and the IPV4 address is used to connect to the appliance.

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

- The DNS lookup request for an IPV6 address is attempted. If an IPV6 address is defined for the host name, the DNS responds with the value used to connect to the Guardium appliance.
- If the DNS defines only an IPV4 address, the DNS responds with the IPV4 address used to connect to the Guardium appliance.
- If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS responds with both addresses, and the IPV4 address is used to connect to the appliance.

Notes
Whether or not this keyword is used, an invalid address for the host name returned from the DNS results in failure to connect to the appliance, and the started task terminates.

Syntax

```
PREFER_IPV4_STACK(N)
```

Example

```
PREFER_IVP4_STACK(Y)
```

SEND_FAIL_EVENT_COUNT

SEND_FAIL_EVENT_COUNT sets the maximum number of events to buffer during a communication outage with the Guardium system.

Required
No

Default
100

Permitted Values
0 – 1024 maximum number of events to be buffered

Description
Specify the maximum number of events to buffer 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.

Notes
SEND_FAIL_EVENT_COUNT and OUTAGE_SPILLAREA_SIZE are mutually exclusive. When you use OUTAGE_SPILLAREA_SIZE, a spill file is created that supersedes SEND_FAIL_EVENT_COUNT for temporary data retention.

Syntax

```
SEND_FAIL_EVENT_COUNT(event_count)
```

Example

```
SEND_FAIL_EVENT_COUNT(100)
```

SMEM_SIZE

Use SMEM_SIZE to specify the maximum amount of global shared memory to allocate by IBM Security Guardium S-TAP for Db2 for all purposes.

Required
No

Default
16

Permitted Values
10 - 128 gigabytes

Description

The SMEM_SIZE parameter value must be equal to or greater than four times the MAXIMUM_ALLOCATIONS parameter value. If you specify a SMEM_SIZE value less than four times the value of MAXIMUM_ALLOCATIONS, then IBM Security Guardium S-TAP for Db2 automatically adjusts the SMEM_SIZE value to be four times greater than the MAXIMUM_ALLOCATIONS value.

If IBM Security Guardium S-TAP for Db2 and Db2 Query Monitor are simultaneously monitoring the same Db2 subsystem, the SMEM_SIZE value(s) from the respective product (either Db2 Query Monitor or IBM Security Guardium S-TAP for Db2) is used to set the local shared memory object. The SMEM_SIZE values for the two products do not have to match.

Notes
None

Syntax

```
SMEM_SIZE(n)
```

Example

```
SMEM_SIZE(16)
```

STAP_BLOCKING

The STAP_BLOCKING parameter controls whether blocking is enabled and whether the blocking operator command is permitted to enable, disable, or report status for blocking.

Required
No

Default
ENABLED

Permitted Values
ENABLED, DISABLED, OPERATOR

Description
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.

Notes
None

Syntax

```
STAP_BLOCKING(ENABLED)
```

Example

```
STAP_BLOCKING(ENABLED)
```

STAP_MEGABUFFER

STAP_MEGABUFFER improves the efficiency of communications with the appliance.

Required
No

Default
Y

Permitted Values
N, Y

Description

When multiple IBM Security 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 Db2 performance, **STAP_MEGABUFFER** must remain set to Y. However, you can set **STAP_MEGABUFFER** 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 might also increase CPU usage, due to additional TCP/IP calls.

Notes
None

Syntax

```
STAP_MEGABUFFER(Y)
```

Example

```
STAP_MEGABUFFER(Y)
```

STAP_STREAM_EVENTS

STAP_STREAM_EVENTS determines whether events are streamed to the IBM Security Guardium.

Required
No

Default
Y

Permitted Values
N, Y

Description
The default value Y enables streaming consistent with the active policy. Specify N to disable streaming and enable Simulation mode.

At startup, the agent address space issues message AUV1070I: TCP/IP STREAMING DISABLED DUE TO USER SETTING.

Notes
None

Syntax

```
STAP_STREAM_EVENTS(Y)
```

Example

```
STAP_STREAM_EVENTS(Y)
```

STAP_STREAM_GTT_EVENTS

STAP_STREAM_GTT_EVENTS controls the collection of global temporary table events.

Required
No

Default
N

Permitted Values
N, Y

Description
Set to Y to enable the collection of global temporary table events.

Notes
None

Syntax

```
STAP_STREAM_EVENTS(N)
```

Example

```
STAP_STREAM_EVENTS(Y)
```

STAP_TERMINATE_OPTIMIZE

You can use **STAP_TERMINATE_OPTIMIZE** to improve response time for processing **STAP_TERMINATE** requests from the Guardium appliance.

Required
No

Default
N

Permitted Values
N, Y

Description
Use **STAP_TERMINATE_OPTIMIZE** in conjunction with **STAP_MEGABUFFER**.

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 Security Guardium to analyze events against the policy and issue the termination requests to IBM Security Guardium S-TAP for Db2. To enable near real-time event recording to the Guardium appliance, set the **STAP_MEGABUFFER** parameter to N.

Notes
None

Syntax

```
STAP_TERMINATE_OPTIMIZE(N)
```

Example

```
STAP_TERMINATE_OPTIMIZE(N)
```

STAP_UTILITY_MULTITABLE

The STAP_UTILITY_MULTITABLE parameter works in conjunction with the STAP_UTILITY_TS_TO_TABLE parameter to control how table information is reported.

Required
No

Default
N

Permitted Values
N, Y

Description
STAP_UTILITY_MULTITABLE and **STAP_UTILITY_TS_TO_TABLE** control how table information is reported for Db2 Utility access events that involve tablespaces. **STAP_UTILITY_MULTITABLE** controls the behavior of the collector when multiple tables are contained in the tablespace. When STAP_UTILITY_MULTITABLE is set to Y:

- The collector reports all tables in the tablespace that are impacted by the utility. This guarantees that tablespace access by a utility execution 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.

Notes
None

Syntax

```
STAP_UTILITY_MULTITABLE(N)
```

Example

```
STAP_UTILITY_MULTITABLE(Y)
```

STAP_UTILITY_TS_TO_TABLE

The STAP_UTILITY_TS_TO_TABLE parameter works in conjunction with the STAP_UTILITY_MULTITABLE parameter to control how table information is reported for Db2 Utility accesses to tablespaces.

Required
No

Default
Y

Permitted Values
N, Y

Description
When this 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 table names in the accessed tablespace
- Only the tablespace is reported.

Notes
None

Syntax

```
STAP_UTILITY_TS_TO_TABLE(Y)
```

Example

```
STAP_UTILITY_TS_TO_TABLE(Y)
```

STARTUP_DIAGNOSTICS

STARTUP_DIAGNOSTICS causes IBM Security Guardium S-TAP for Db2 to produce diagnostic information output during startup of the collector agent.

Required
No

Default
N

Permitted Values
N, Y

Description
You can use the diagnostic information output when communicating with IBM Support about problems you report.

Notes
None

Syntax

```
STARTUP_DIAGNOSTICS(N)
```

Example

```
STARTUP_DIAGNOSTICS(Y)
```

SHUTDOWN_DIAGNOSTICS

Use SHUTDOWN_DIAGNOSTICS to produce diagnostic information.

Required
No

Default
N

Permitted Values
N, Y

Description
The SHUTDOWN_DIAGNOSTICS parameter causes Db2 to produce diagnostic information output during shutdown (stop) of the collector agent. Do not change the value of this parameter unless directed by IBM Support.

Notes
None

Syntax

```
SHUTDOWN_DIAGNOSTICS(N)
```

Example

```
SHUTDOWN_DIAGNOSTICS(Y)
```

SUBSYS

SUBSYS defines the SQL Collector subsystem name.

Required
No

Default
The Db2 subsystem name.

Permitted Values
1-4 characters

Description

Choose any subsystem ID to identify this particular instance of Db2.

The subsystem name you define does not need to correspond to a Db2 subsystem nor an MVS™ operating system name.

Notes
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.

Syntax

```
SUBSYS(Db2_subsystem_name)
```

Example

```
SUBSYS(ADH1)
```

TS_OFFSET

Use TS_OFFSET to adjust the event timestamps streamed to the appliance.

Required
No

Default
No default (no offset)

Permitted Values

E|W
East or west offset from GMT

HH
Number of hours

MM
Number of minutes

Description
You can adjust event timestamps streamed to the appliance by specifying the amount of time offset by time zone. For example, if you are adjusting the offset of time zone UTC 0.0 from time zone UTC + 9, GMT, the UTC 0.0 time zone is west of and nine hours earlier than UTC + 9. In this example, event timestamps are offset by subtracting 9 hours from the original timestamp, resulting in `TS_OFFSET(W.09.00)`.

If you do not configure TS_OFFSET, the timestamps streamed to the appliance are not adjusted for timezone.

Notes
None

Syntax

```
TS_OFFSET(E|W.HH.MM)
```

Example

```
TS_OFFSET(W.09.00)
```

ZIIP_FILTER

Enabling ZIIP_FILTER allows the collector agent to perform offload profile filtering to an IBM System z Integrated Information Processor (zIIP).

Required
No

Default
N

Permitted Values
N, Y

Description

- Specify Y so that the z/OS image running the collector agent started task has a zIIP and allow the collector agent to perform offload profile filtering to a zIIP.
- N specifies that the collector agent started task is running on a z/OS that has no zIIP, and that message ADHQ1060I is issued indicating the WLM related service has failed. In this case, the collector agent continues to run as if ZIIP_FILTER(N) were set.

Notes
None

Syntax

```
ZIIP_FILTER(N)
```

Example

```
ZIIP_FILTER(Y)
```

ZIIP_TCP

ZIIP_TCP enables the z/OS image running the collector agent started task to have an IBM System z® Integrated Information Processor (zIIP).

Required
No

Default
N

Permitted Values
N, P

Description

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

Notes
Enabling NZIIP_TCP(Y) requires you to enabled zIIP support using ZIIP_FILTER(Y). If ZIIP_FILTER(N) and ZIIP_TCP(Y) are both enabled, ZIIP_FILTER is automatically set to Y.

Syntax

```
ZIIP_TCP(N)
```

Example

```
ZIIP_TCP(Y)
```

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 Security 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.

Configuring data streaming modes

IBM Security Guardium S-TAP for Db2 collects and streams audit event data to the Guardium system. You can choose from the following data streaming modes.

The mode you choose depends on:

- the number of connected Guardium appliances you want to stream data to.
- how you want Security Guardium S-TAP to handle data in the event of a connection outage.

Single Appliance
Single appliance mode enables data to stream to one connected appliance. Single Appliance mode does not provide failover during a connection outage and you cannot specify backup failover appliances.

Failover
Failover mode enables data to stream to one or more backup failover appliances when a connection outage occurs.

Hot Failover
Hot Failover mode enables data to stream to backup failover appliances when a connection outage occurs. However, in Hot Failover mode, connections to all appliances you specify with APPLIANCE_SERVER_*n* are initiated at S-TAP startup and the connections are always kept active.

Multistream
Multistream mode enables data streaming to the primary appliance and five additional multiple connected Guardium appliances.

Mirror
Mirroring mode enables you to stream the same event data to all connected appliances, known as mirroring. Mirroring mode supports ports 16022 and 16023.

Note: The MIRROR mode should not be enabled if aggregation of the appliances is occurring. Aggregation of appliances included in one or more STAP(s) operating in MIRROR mode may result in duplicated events and alerts.

The following table lists parameters that configure the four modes of data streaming.

Table 5. Data Streaming Parameters

Parameter	Permitted Values	Description
APPLIANCE_SERVER_LIST	FAILOVER HOT_FAILOVER MULTI_STREAM MIRROR	Specify the data streaming mode. If you use Single Appliance mode, you do not need to configure this parameter.
APPLIANCE_SERVER	IP address or hostname	Specify the IP address or hostname of the primary appliance to stream to.
APPLIANCE_SERVER_*n*	IP address or hostname	Specify the IP address or hostname of the failover appliances where *n*=1-5. During a connection outage, Guardium S-TAP attempts to connect to failover appliances in the order you number them. Not required for Single Appliance mode.
OUTAGE_SPILLAREA_SIZE()	0 – 1024 Default: 15	Define spill areas that prevent data loss.

Configuring Single Appliance mode

Single Appliance mode enables data to stream to one connected appliance. Single Appliance mode does not provide failover during a connection outage and you cannot specify backup failover appliances.

About this task

When a connection outage occurs in Single Appliance mode, Security Guardium S-TAP continues to collect data. During short-term outages, spill areas prevent data loss until connectivity is restored at which point data streaming to the appliance resumes.

Procedure

1. Specify the IP address or hostname of the primary appliance server using keyword APPLIANCE_SERVER.
2. To prevent data loss, define spill areas using keyword OUTAGE_SPILLAREA_SIZE().

Example

Example Single Appliance configuration:

```
APPLIANCE_SERVER(192.168.2.1)
OUTAGE_SPILLAREA_SIZE(15)
```

Configuring Failover mode

Failover mode enables data to stream to one or more backup failover appliances when a connection outage occurs.

About this task

Events are first streamed to the appliance specified by APPLIANCE_SERVER. During a connection outage, Guardium S-TAP attempts to connect to appliances in the order you number them using parameter APPLIANCE_SERVER_*n*.

In Failover mode, policies are pushed to the S-TAP from the active appliance. For example, if a connection outage occurs with the appliance you specified with APPLIANCE_SERVER and a connection is established with the failover appliance specified with APPLIANCE_SERVER_1, a new policy is activated and pushed by the failover appliance. For this reason, install the same policy for all appliances you define using parameters APPLIANCE_SERVER and APPLIANCE_SERVER_*n.*

Note: In Failover mode, install the same policy for all appliances you specify in APPLIANCE_SERVER through APPLIANCE_SERVER_*n*. Failover connections to subsequent appliances use newly activated policies.

Procedure

1. Specify the IP address or hostname of the primary appliance server using keyword APPLIANCE_SERVER.
2. Set the value of parameter APPLIANCE_SERVER_LIST to FAILOVER.
3. Specify the number of failover appliances using keyword APPLIANCE_SERVER_*n* where *n*=1-5
4. To prevent data loss, define spill areas using keyword OUTAGE_SPILLAREA_SIZE().

Example

Example Failover configuration:

```
APPLIANCE_SERVER(192.168.2.1)
APPLIANCE_SERVER_LIST(FAILOVER)
APPLIANCE_SERVER_1(192.168.2.101)
OUTAGE_SPILLAREA_SIZE(15)
```

Configuring Hot Failover mode

Like Failover mode, Hot Failover mode enables data to stream to backup failover appliances when a connection outage occurs. However, in Hot Failover mode, connections to all appliances you specify with APPLIANCE_SERVER_*n* are initiated at S-TAP startup and the connections are always kept active.

About this task

In Hot Failover mode, you need to configure and activate the policy only for the primary appliance you specify with parameter APPLIANCE_SERVER. If a connection outage occurs and connectivity is successfully established with a failover appliance specified by APPLIANCE_SERVER_n, the policy pushed by the primary appliance continues to be the active policy.

Note: In Hot Failover and Multistream, and Mirroring mode, you need to configure and activate the policy only for the primary appliance.

Procedure

1. Specify the IP address or hostname of the primary appliance server using keyword APPLIANCE_SERVER.
2. Set the value of parameter APPLIANCE_SERVER_LIST to HOT_FAILOVER.
3. Specify the number of failover appliances using keyword APPLIANCE_SERVER_*n* where *n*=1-5

4. To prevent data loss, define spill areas using keyword OUTAGE_SPILLAREA_SIZE().

Example

Example Hot Failover configuration:

```
APPLIANCE_SERVER(192.168.2.1)
APPLIANCE_SERVER_LIST(HOT_FAILOVER)
APPLIANCE_SERVER_1(192.168.2.101)
OUTAGE_SPILLAREA_SIZE(15)
```

Configuring Multistream mode

Multistream mode enables data streaming to the primary appliance and five additional multiple connected Guardium appliances.

About this task

In Multistream mode, you need to configure and activate the policy only for the primary appliance you specify with parameter APPLIANCE_SERVER. If a connection outage occurs and connectivity is successfully established with a failover appliance specified by APPLIANCE_SERVER_n, the policy pushed by the primary appliance continues to be the active policy.

Note: In Hot Failover and Multistream, and Mirroring mode, you need to configure and activate the policy only for the primary appliance.

Procedure

1. Specify the IP address or hostname of the primary appliance server using keyword APPLIANCE_SERVER.
2. Set the value of parameter APPLIANCE_SERVER_LIST to MULTI_STREAM.
3. Specify the number of failover appliances using keyword APPLIANCE_SERVER_*n* where *n*=1-5
4. To prevent data loss, define spill areas using keyword OUTAGE_SPILLAREA_SIZE().

Example

Example Multistream configuration:

```
APPLIANCE_SERVER(192.168.2.100)
APPLIANCE_SERVER_LIST(MULTI_STREAM)
APPLIANCE_SERVER_1(192.168.2.101)
APPLIANCE_SERVER_2(192.168.2.102)
OUTAGE_SPILLAREA_SIZE(15)
```

Configuring Mirroring mode

Mirroring mode enables you to stream the same event data to all connected appliances, known as mirroring. Mirroring mode supports ports 16022 and 16023.

About this task

Note: Do not enable Mirror mode if aggregation of appliances is occurring. Aggregation of appliances included in one or more S-TAPs operating in Mirror mode may result in duplicate events and alerts.

In Mirroring mode, you need to configure and activate the policy only for the primary appliance you specify with parameter APPLIANCE_SERVER. If a connection outage occurs, and connectivity continues to be successfully established with a failover appliance specified by APPLIANCE_SERVER_n, the policy pushed by the primary appliance continues to be the active policy.

Note: In Hot Failover, Multistream, and Mirroring mode, you need to configure and activate the policy only for the primary appliance.

Procedure

1. Specify the IP address or hostname of the primary appliance server using keyword APPLIANCE_SERVER.
2. Set the value of parameter APPLIANCE_SERVER_LIST to MIRROR.
3. Specify the number of failover appliances using keyword APPLIANCE_SERVER_*n* where *n*=1-5
4. To prevent data loss, define spill areas using keyword OUTAGE_SPILLAREA_SIZE().

Example

Example Mirroring configuration:

```
APPLIANCE_SERVER(192.168.2.100)
APPLIANCE_SERVER_LIST(MIRROR)
APPLIANCE_SERVER_1(192.168.2.101)
APPLIANCE_SERVER_2(192.168.2.102)
OUTAGE_SPILLAREA_SIZE(15)
```

Support Services Address Space overview

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

A Support Services Address Space, also referred to as a Primary Address Space, starts for each z/OS image after the first instance of IBM Security Guardium S-TAP 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 Primary Address Space is a Service Address Space for all instances of IBM Security Guardium S-TAP 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 Primary Address Space acts as a placeholder for shared collector resources, and is similar to other Primary Address Spaces that are used throughout MVS. For sample, MVS and Db2 both have Primary Address Spaces.

The Primary 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 Security Guardium S-TAP for Db2 or IBM Db2 Query Monitor for z/OS.
- Forcing the Primary Address Space to stop causes abnormal termination of all IBM Security Guardium S-TAP for Db2 and IBM Db2 Query Monitor for z/OS subsystems on the LPAR.

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

Usage considerations for the Primary Address Space

The following considerations apply to the use of the Support Services Address Space when you are using IBM Security 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 Security Guardium S-TAP for Db2 or IBM Db2 Query Monitor for z/OS) to monitor the same

If you use multiple collector products (such as IBM Security Guardium S-TAP 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 Security Guardium S-TAP 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 Primary Address Space

Do not stop the Primary 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 Primary Address Space should only be stopped by using the sample job that is provided in SADHSAMP, member ADHMSTR. This job verifies that no IBM Security Guardium S-TAP for Db2 or IBM Db2 Query Monitor for z/OS subsystems are using the Primary 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 for CICS. The capture of CICS transactions is limited to CICS versions TS 5.2 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. Managing data collection

IBM Security Guardium S-TAP for Db2 collects data from an audited Db2 subsystem, in accordance with the collection policies that you create through the IBM Security Guardium. 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 Security Guardium.

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

Data collection process

During the collection process, IBM Security 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 Security 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 criteria is present, or neither of the filtering criteria is 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 Security Guardium interface. This table lists the types of events that can be collected.

Table 6. Collected event types

Collected event types
All reads (SQL SELECT)
All changes (SQL UPDATE, INSERT, DELETE, TRUNCATE, MERGE)
SQL LOCK
Authorization
Audit data for Db2 utilities
Grant/Revoke
Access attempts
Binds/Rebinds
Commit/Rollbacks
Db2 commands
Db2 utilities
Failed logins
Create, Alter, Drop, Rename Table
Create, Alter, Drop, Rename Tablespace
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 Security Guardium interface.

Audit data for Db2 Utilities

You can collect table information for Db2 utility operations that are run against tablespaces. The IBM Security 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 16 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.

Including or excluding failed accesses and negative SQL code

IBM Security 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 of 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.
- 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.

Controlling host variable collection

IBM Security 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 Security 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 Security 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 / SET CURRENT SCHEMA events using the Audit SQL Collector

IBM Security Guardium S-TAP for Db2 enables you to collect SET CURRENT SQLID / SET CURRENT SCHEMA events using the Audit SQL Collector.

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

Filtering

IBM Security Guardium S-TAP for Db2 enables filtering to occur at the point of collection regardless of the field types 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 51.

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

Table 7. Event types and filtering

Event type	Subjected to filtering?
SELECT/MERGE/UPDATE/INSERT/DELETE/ TRUNCATE	Yes
LOCK	No
CREATE/ALTER/DROP/RENAME	No
GRANT/REVOKE	No
SET CURRENT SQLID/SET CURRENT SCHEMA	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/MERGE/TRUNCATE/SET CURRENT USERID/CREATE/ALTER/ DROP/RENAME/LOCK** 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/MERGE/TRUNCATE
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/MERGE events: SELECT, and either INSERT, UPDATE, DELETE, or MERGE. All nested INSERT/UPDATE/DELETE/MERGE 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/RENAME/LOCK
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/SET CURRENT SCHEMA
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.

Enable collection by adding the **DB2 Commands** event type to the COMMAND collection in a rule.

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.

To enable the collection of negative SQLCODE events, the pushed-down policy should contain negative SQLCODEs.

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

Filtering by database name

IBM Security 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 a 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 of 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 Security 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 (BLCKSIZE): 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* documentation on IBM Documentation.

For more information about using data sets, see z/OS DFSMS Using Data Sets: https://www.ibm.com/docs/en/zos/2.1.0?topic=dfsms-zos-using-data-sets.

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
   ```

Quarantining SQL activity

IBM Security 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 Security Guardium 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 Security Guardium interface, refer to the Security Guardium documentation on IBM Documentation.

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 16.

Chapter 4. Reference information

The following topics provide information about IBM Security Guardium S-TAP for Db2 sample library members, parameters, and variables.

Topics:

- "Sample library members" on page 55
- "Collector agent parameters" on page 16
- "Collector agent sample parameter file" on page 59
- "ADHEMAC1 edit macro variables" on page 60

Other resources

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

- IBM Ported Tools for z/OS
- 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 Security Guardium S-TAP for Db2 for installation and configuration.

Table 8. 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.
ADHCFGP	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 Security Guardium S-TAP for Db2 collector started task procedure. Runs an instance of the IBM Security 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 Security Guardium S-TAP for Db2 Primary Address Space.
ADHSJ000	JCL	Allocates VSAM product control file.

Table 8. Installation and configuration sample library members (continued)		
Member	**Type**	**Description**
ADHSJ001	JCL	Sets product configuration options.
ADHSJ003	JCL	Generates the product control file content report.
ADHSTAPD	JCL	Produces an IBM Security 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 ADHC*SSID* contains the sample JCL to set up the IBM Security 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-----------|
                          |      +-,STATUS-----------------|
```

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 the MUSTGATHER 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 filer 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

STATUS
Display the connection and policy status of the S-TAP

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_RRSAF (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 Security Guardium 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.

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 (ADHCFGP). 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(#APPSRVR)
```

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 9. 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 Security Guardium S-TAP for Db2 load modules.
#SADHDBRM	ADH.IBMTAPE. SADHDBRM	Change the default to the data set containing the IBM Security Guardium S-TAP for Db2 Dorms.
#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 DSNTEP2 module.
#DSNTEP2	DSNTEP2	Change the default to the DSNTEP2 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.
#SFECLOAD	None	Data set name of the required FEC load library.

Table 9. ADHEMAC1 Edit macro variables (continued)		
Variable	**Default**	**Instructions**
#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 Security Guardium S-TAP for Db2 VSAM Control file.
#APPSRVR	appliance.company.com	Host name or IP address of the IBM Security Guardium.
#ADHCFGDS	ADH.CF	Name of the customized ADHCFGP member

The following example shows the contents of the ADHEMAC1 member:

```
ISREDIT MACRO
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
ISREDIT CHANGE ALL '#ADHCFGDS'      ADH.CONFIG(SSIDCFGP)
```

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

These topics document the messages and error codes issued by IBM Security Guardium S-TAP for Db2. Messages are presented in ascending alphabetical and numerical order.

Error messages

IBM Security Guardium S-TAP for Db2 messages adhere to the following format: ADH*nnnx*

Where:

ADH
Indicates that the message was issued by IBM Security Guardium S-TAP for Db2.

nnn
Indicates the message identification number.

x
Indicates the severity of the message:

Table 10. 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 Security 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=*parameter-name***

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 *server-name***

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=*return-code* reason=*reason-code***

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 *reattempt-number* of *total-reattempts***

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-reattempts* 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: [*size*] 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 [*server*]**

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 **IBM Security Guardium S-TAP for Db2 Collector Agent is terminating**

Explanation:
The collector is terminating.

User response:
No action is required.

ADHG031I **IBM Security Guardium S-TAP for Db2 V11.3 [*component*] connection established**

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

User response:
No action is required.

ADHG033E **IP address is invalid for [*IP address*]**

Explanation:
The IP address or host name specified in the agent configuration is invalid.

User response:
Correct the IP address or host name and restart S-TAP.

ADHG034W **An error occurred resolving host name [*host name*]**

Explanation:
There is a problem resolving the host name [*host name*].

User response:
Ensure that the host name is valid and is registered.

ADHG035I **Host name [*host name*] is resolved to IP address [*IP address*]**

Explanation:
The S-TAP stream component successfully resolved an appliance host name to IP address.

User response:
No action is required.

ADHG036I **Registering server <*server*> as eligible for mirroring.**

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

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.

ADHG196I **Connection is active to server *server-address*.**

Explanation:
The status of the connection between S-TAP and appliance *server-address*.

User response:
No action is required.

ADHG197I **Connection is inactive to server *server-address*.**

Explanation:
The connection between S-TAP and appliance *server-address* is inactive.

User response:
Check with the network team and ensure that the *server-address* is up and running and is reachable by the S-TAP.

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

Explanation:
A **–CANCEL THREAD** command was issued by IBM Security Guardium S-TAP for Db2 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: *exception-count***

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=*length* rc=*returncode* rsn=*reasoncode***

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.

ADHG551I **High volume of data detected. Collecting rate is *<N>* events per second.**

Explanation:
A high volume of data is being collected or streamed by S-TAP. This could cause the appliance to be overwhelmed and unresponsive to the S-TAP agent.

User response:
Tune the policy to decrease the amount of data to be collected.

ADHG700I **Collection Manager stop requested.**

Explanation:
A collection stop request is detected. S-TAP is terminating.

User response:
No action is required.

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 **IBM Security Guardium S-TAP for Db2 V11.3 [component] connection established**

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

User response:
No action is required.

ADHI530E **DB2 connection failed [*function*] SQLCODE=[*sqlcode*] RSN=[*reason-code*]**

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 be 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:
his 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 IBM Security Guardium S-TAP for Db2 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 *reattempt-number* of *total-reattempts.***

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 *reattempt-number* reaches the *total-reattempts* 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 a 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 servers.

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 **IBM Security Guardium S-TAP for Db2 Policy component is terminating**

User response:
No action is required.

ADHP031I **IBM Security Guardium S-TAP for Db2 V11.3 *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.

ADHP032W **Contradictory value! Filter discarded: *<filter-value>***

Explanation:
A group contains both inclusive and exclusive filters, causing contradictory values in the filter compiler.

User response:
Update the policy and ensure that the group does not contain inclusive and exclusive filters. Then restart S-TAP.

ADHP033E **IP address is invalid for [*IP address*]**

Explanation:
The IP address or host name specified in the agent configuration is invalid.

User response:
Correct the IP address or host name and restart S-TAP.

ADHP034W **An error occurred resolving host name [*host name*]**

Explanation:
There is a problem resolving the host name [*host name*].

User response:
Ensure that the host name is valid and is registered.

ADHP035I **Host name [*host name*] is resolved to IP address [*IP address*]**

Explanation:
The S-TAP Policy component successfully resolved an appliance host name to IP address.

User response:
No action is required.

ADHP036I **Registering server <*server*> as eligible for mirroring.**

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

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, IBM Security Guardium S-TAP for Db2 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* on IBM Documentation.

ADHP103I **IBM Security Guardium S-TAP for Db2 on z/OS STOP requested.**

Explanation:
IBM Security Guardium S-TAP for Db2 on z/OS STOP requested. S-TAP will terminate.

User response:
No action is required.

ADHP110I **IBM Security Guardium S-TAP for Db2 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.

ADHP194I **[n] messages pushed from appliance detected.**

Explanation:
A policy pushed with [n] messages was detected, where [n] is the number of messages pushed from the Guardium appliance to the z/OS S-TAP task.

User response:
No action is required.

ADHP196I **Connection is active to server *server-address*.**

Explanation:
The status of the connection between S-TAP and appliance *server-address*.

User response:
No action is required.

ADHP197I **Connection is inactive to server *server-address*.**

Explanation:
The connection between S-TAP and appliance *server-address* is inactive.

User response:
Check with the network team and ensure that the *server-address* is up and running and is reachable by the S-TAP.

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.

ADHP700I **Collection Manager stop requested.**

Explanation:
A collection stop request is detected. S-TAP is terminating.

User response:
No action is required.

ADHP2020I **CURRENTLY ACTIVE POLICY RESULTS IN [*ENABLED* | *DISABLED*] COLLECTION.**

Explanation:
The status of the current policy.

User response:
No action is required.

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.

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.

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.

ADHQ1003E **SUBSYSTEM *ssid* ALREADY ACTIVE**

Explanation

The collector agent indicated in the message is already active and 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.

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

Explanation

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

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.

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.

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.

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 primary address space *address space*.**

Explanation:
A serious error has occurred in the primary address space specified.

User response:
Verify that the primary address space is available.

ADHQ1032I **Recreating primary address space.**

User response:
No action is required.

ADHQ1033E **UNABLE TO CREATE MASTER ADDRESS SPACE *additional_info*.**

Explanation

The explanation for this message depends on the variation of the message that is received.

UNABLE TO CREATE MASTER ADDRESS SPACE, MISMATCHED MASTER CODE LEVELS
S-TAP for Db2 is not able to create the main address space indicated in the message.

UNABLE TO CREATE MASTER ADDRESS SPACE, CSVDYLPA ERROR, RC=004
The CSVDYLPA service returns a return code indicating S-TAP for Db2 lacks the authorization to issue CSVDYLPA.

User response

The user response to this message depends on the variation of the message that is received.

UNABLE TO CREATE MASTER ADDRESS SPACE, MISMATCHED MASTER CODE LEVELS
The Support Services Address Space is unable to start or function properly.

- If this is an initial install, the problem is likely related to a security issue.
- If you are running two versions of S-TAP for Db2, you must specify different values for the MASTER_PROCNAME parameters for each version.
- If message IEE296I is issued, then the AUTHID for the Support Services Address Space assigned from the started task table may have been revoked or never initialized. The installation's security settings should be reviewed by your Security or z/OS® support areas to ensure that the settings are configured correctly before restarting S-TAP for Db2. You can use the ADHPROC userid as a model to create a similar entry for the Support Services Address Space. If the message is issued after applying S-TAP for Db2 maintenance, one of the fixes is likely to have affected the Support Services Address Space. You must cycle the S-TAP for Db2 started task and Support Services Address Space

after applying maintenance. Refer to SAMPLIB member ADHMSTR for example on how to cycle the main address space. If you are unable to diagnose or resolve the problem, send your console log to IBM® Software Support.

UNABLE TO CREATE MASTER ADDRESS SPACE, CSVDYLPA ERROR, RC=004

This is a RACF® definition issue. For more information, see Assessing RACF vulnerabilities.

ADHQ1034I **Primary address space has started.**

User response:
No action is required.

ADHQ1035E **Unable to restart primary (RS=rc).**

Explanation:
The primary address space could not be restarted.

User response:
Verify that the primary 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 11. Return code explanations

Service	Description
IWM4ECRE (WLM Enclave Create)	The return codes and reason codes are documented in *z/OS V1R10.0 MVS Programming Workload Management Services*.
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.
IEAVAPE (Z/OS Allocate Pause Element)	These return codes are described in *z/OS V1R10.0 MVS Programming Assembler Services References V2*. 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 (xxxxxxxx)

Explanation:
A policy is sent from the Guardium system to the IBM Security Guardium S-TAP for Db2 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 IBM Security Guardium S-TAP for Db2 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

An IBM Security Guardium S-TAP for Db2 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 IBM Security Guardium S-TAP for Db2 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

An IBM Security Guardium S-TAP for Db2 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

An IBM Security Guardium S-TAP for Db2 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

An IBM Security Guardium S-TAP for Db2 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

An IBM Security Guardium S-TAP for Db2 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 been produced to IBM Software Support.

ADHQ1213W SPACE IS FULL AND NO MORE EXTENTS CAN BE OBTAINED FOR SPACE – space

Explanation

An IBM Security Guardium S-TAP for Db2 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 IBM Security Guardium S-TAP for Db2. 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 IBM Security Guardium S-TAP for Db2, 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

An IBM Security Guardium S-TAP for Db2 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

An IBM Security Guardium S-TAP for Db2 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 IBM Security Guardium S-TAP for Db2. 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 IBM Security Guardium S-TAP for

Db2, 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:
An IBM Security Guardium S-TAP for Db2 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

An IBM Security Guardium S-TAP for Db2 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, IBM Security Guardium S-TAP for Db2 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 IBM Security Guardium S-TAP for Db2. 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 IBM Security Guardium S-TAP for Db2, 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 IBM Security Guardium S-TAP for Db2, 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 F0RCE(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.

ADHQ2058E IN-COLLECTOR ELAPSED TIME LIMIT EXCEEDED FOR THREAD *thread_id ssid plan_name*.

Explanation:
The monitoring agent has been detected to be consuming CPU for a period of time greater than specified in the HM_TIME_LIMIT parameter in ADHPARMS. The *thread_id* is the Db2 thread token for the thread consuming the CPU, *ssid* is the Db2 subsystem running the thread, and *plan_name* is the plan name the thread was executing.

User response:
Review the ADHPARMS parameters HM_DUMPS and HM_TIME_LIMIT (these set the thresholds for in-collector health monitoring). In environments with high CPU contention, the HM_TIME_LIMIT parameter value might need to be increased to avoid false positives. An SVCDUMP will be taken if the HM_DUMPS limit has not been met. If you encounter this message and receive a dump, contact IBM Software Support.

ADHQ2059E CALLRTM ISSUED FOR SRB *srb_address* IN ASID *asid*.

Explanation:
The SRB shown in the message has been canceled and will return to Db2 to resume execution.

User response:

Review the ADHPARMS parameters HM_DUMPS and HM_TIME_LIMIT (these set the thresholds for in-collector loop processing). In environments with high CPU contention, the HM_TIME_LIMIT parameter value might need to be increased to avoid false positives. An SVCDUMP will be taken if the HM_DUMPS limit has not been met. If you encounter this message and receive a dump, contact IBM Software Support.

ADHQ2060E CALLRTM ISSUED FOR TCB *tcb_address* IN ASID *asid*.

Explanation:
S-TAP collector has issued a CALLRTM service for the TCB or SRB identified by tcbaddr or srbid in the address space identified by ASID asidnum. This message is issued in conjunction with message ADH2058E.

User response:
Review the ADHPARMS parameters HM_DUMPS and HM_TIME_LIMIT (these set the thresholds for in-collector health monitoring). In environments with high CPU contention, the HM_TIME_LIMIT parameter value might need to be increased to avoid false positives. An SVCDUMP will be taken if the HM_DUMPS limit has not been met. If you encounter this message and receive a dump, contact IBM Software Support.

ADHQ2061E MONITORING OF THREADS DISABLED FOR SSID *ssid*.

Explanation:
S-TAP collector will no longer monitor SQL from threads from the named Db2 due to it detecting more high CPU conditions than were specified in the HM_DISABLE_AGENT parameter in ADHPARMS.

User response:
Review the SYSLOG for prior instances of ADH2058E and ADH2060E messages, which document units of work that were identified as consuming excessive collector elapsed time and were canceled as a result. The SVCDUMP associated with these entries would have been captured, provided that the HM_DUMPS parameter setting in effect permitted dumps to be captured. Monitoring will not be reactivated until the monitoring task is restarted. If you encounter this message and receive a dump, contact IBM Software Support.

ADHQ2062I SQL CALLS FOR THREAD *thread-token* ON *db2-ssid* WILL NO LONGER BE MONITORED.

Explanation:
S-TAP collector no longer will monitor SQL activity for the thread identified by *thread-token* on Db2 subsystem *db2-ssid* because it previously detected a high CPU condition within S-TAP collector within the thread. This message is issued in conjunction with message ADH2058E.

User response:
Restart S-TAP collector once the problem is identified. If you encounter this message and receive a dump, contact IBM Software Support.

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 *parameter*

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 *parameter*

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 *dsmgmt*

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 *z/OS V1R1.0 DFSMS/DFP Diagnosis Reference* (GY27-7618-01).

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

IBM Security Guardium S-TAP for Db2 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 IBM Security Guardium S-TAP for Db2 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 IBM Security Guardium S-TAP for Db2 maintenance applied.

ADHQ3192I LEVEL STATUS DB2(ssid) message

Explanation:
This message displays if a mismatch in code level exists between IBM Security Guardium S-TAP for Db2 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 SUBYSYSTEM *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 it 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 DATASPACES**.

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.

ADHQ3289I TRANSLATION EXCEPTION ADDRESS nnnnnnnn

Explanation:
This is an informational message that is put out as a result of the DDX modify 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 IBM Security Guardium S-TAP for Db2 and Query Monitor installations. The maintenance code levels for IBM Security Guardium S-TAP for Db2 and Query Monitor installations must match.

User response:
Ensure that the maintenance levels match between the IBM Security Guardium S-TAP for Db2 and Query Monitor installations. Apply maintenance as required to one or both environments to ensure that the maintenance levels match.

ADHQ3315E PRIMARY 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 audited by IBM Security Guardium S-TAP for Db2 must have a matching MASTER_PROCNAME parameter between the Query Monitor subsystem or the IBM Security Guardium S-TAP for Db2 ASC started task.

User response:
Update the MASTER_PROCNAME parameter for DB2 Query Monitor or IBM Security Guardium S-TAP for Db2 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 has 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

IBM Security Guardium S-TAP for Db2 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 Message*s (GC18-9602-01) and *DB2 Universal Database for z/OS V8 Code*s (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.

ADHQ4401I **DIAG THRESHOLD EXCEEDED ON DB2 SUBSYSTEM *ssid* FOR *info***

Explanation

An internal diagnostic trap has crossed the threshold on Db2 subsystem *ssid*. The dumps can be generated based on the DIAG_THRESHOLD_DUMPS parameter value. The dump number for the diagnostic trap is shown in the message (*info*).

User response

Provide IBM Software Support with the collected dump and job log.

ADHQ4402I **DIAGNOSTIC DUMP TAKEN ON *dataset_name***

Explanation

After reaching the DIAG_THRESHOLD threshold for an internal diagnostic, a dump is taken and is output to *dataset_name*.

User response

Provide IBM Software Support with the collected dump and job log.

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 **REQURESTING 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* R0=*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.

ADHQ8022I ***adh parameter value***

Explanation

This message is used to display the contents of the ADHPARMS file that was processed when IBM Security Guardium S-TAP for Db2 was started.

User response

No action is required.

ADHQ9899I ***adh modify command***

Explanation

This message is used to display the text of a modify command that was issued to IBM Security Guardium S-TAP for Db2.

User response

No action is required.

Error messages and codes: FECxxxx

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

FECA900E **Invalid Column Function value. Valid values: 1, 2, 3, 4**

Explanation:
An invalid character was entered in the Column Function field.

User response:
Specify a valid character (1, 2, 3, or 4).

FECA901E **Invalid Permanent View value. Valid values: Y, N**

Explanation:
An invalid value was entered in the Permanent View field.

User response:
Correct the value or cancel. Valid values are Y and N.

FECA902E **Invalid Reset View value. Valid values are Y, N**

Explanation:
An invalid character was entered in the Reset View field. Valid characters are Y and N.

User response

Specify a valid value or cancel. Valid values are:

- Y - resets all customizations.
- N - customizations are not reset.

FECA903E **Invalid Stop Sorting value. Valid values: Y, N**

Explanation

The specified stop sorting value is not valid. Valid values are:

- Y - Indicates that sorting will be stopped.
- N - Indicates that sorting will continue.

User response:
Specify a valid value or cancel.

FECA904E **Invalid command in FORM display**

Explanation:
The command you issued when viewing the FORM display was not valid.

User response:
Valid commands for FORM display include NROW and PROW.

FECA905E **FORM command not supported from CSETUP function**

Explanation:
The FORM command was issued from a CSETUP function. FORM is not supported while in a CSETUP function (CSETUP functions include CFIX, CORDER, CSIZE and CS).

User response:
No action is required.

FECA906E **Invalid parameter for NROW. Must be numeric.**

Explanation:
The parameter you specified was not numeric and is therefore invalid.

User response:
Specify a numeric value corresponding to the number of rows to advance. The default value for NROW is 1.

FECA907E **Invalid parameter for PROW. Must be numeric.**

Explanation:
The parameter you specified was not numeric and is therefore invalid.

User response:
Specify a numeric value corresponding to the number of rows to scroll back. The default value for PROW is 1.

FECA908E **Invalid parameter for NROW. Too many digits.**

Explanation:
An invalid parameter for the NROW keyword was specified. More than eight digits were specified. Parsing stops at eight digits.

User response:
A parameter of NROW must be between 1 and the number of rows in the current report display. If no parameter is specified, 1 is assumed.

FECA909E **Invalid parameter for PROW. Too many digits.**

Explanation:
Invalid parameter to PROW specified. More than eight digits were specified. Parsing stops at eight digits.

User response:
A parameter of PROW must be between 1 and the number of rows in the current report display. If no parameter is specified, 1 is assumed.

FECA910E **CSETUP command not supported from FORM function**

Explanation:
CSETUP functions are not supported while in the FORM display. CSETUP functions include CFIX, CORDER, CSIZE, CSORT, and CSETUP (CSET).

User response:
Exit the current FORM function before issuing a CSETUP function.

FECA911E **Invalid ICR command. Use RIGHT command.**

Explanation:
ICR is only valid with columns that are not their maximum size. You can see the column's current and maximum sizes by issuing CSIZE.

User response:
RIGHT and LEFT commands can be used to see all parts of this column.

FECA912E **Invalid ICL command. Use LEFT command.**

Explanation:
ICL is only allowed with columns that are not their maximum size. You can see the column's current and maximum sizes by issuing CSIZE.

User response:
RIGHT and LEFT commands can be used to see all parts of this column.

FECA913E **Format mix data element not updated.**

Explanation:
Format MIX data cannot be updated when only part of the data is displayed.

User response:
No action is required.

FECA914E **FORM command not supported from FORM function**

Explanation:

FORM was issued from within a FORM display. This is not supported.

User response:
No action is required.

FECA915E **FORM PF keys set; NROW = nrow PROW = prow**

Explanation

The NROW (next row) and PROW (previous row) commands are used to move the FORM display window to another row. The UP, DOWN, LEFT, and RIGHT commands move the FORM display window within the current row.

Row, as mentioned above, refers to the row from the original report display, not any reformatted FORM display row.

By default, NROW advances the FORM display to the next row. If NROW n is issued, the FORM display will advance n rows.

Similarly, PROW moves the FORM display window to the immediately prior row PROW n moves the current FORM display window to the nth prior row.

User response:
No action is required.

FECA916E **Invalid CNUM parm. Valid parms are ON, OFF, or blank.**

Explanation:
CNUM was issued with an invalid parameter. Issuing CNUM with no parameter acts as an ON/OFF toggle. ON and OFF are the only parameters accepted. ON turns the CNUM display on. OFF turns the CNUM display off.

User response:
Use a valid CNUM parameter (ON, OFF, or blank)

FECA917E **Report width for print too large.**

Explanation:
The report width exceeds the maximum print width.

User response:
The maximum report width that is currently supported is 32,760.

FECA918E ***string*** **not found. Press PF5 to continue from top.**

Explanation:
The indicated character string was not found.

User response:
To continue searching for the character string from the top of the dialog, press PF5.

FECA920I **Chars *chars* found *n* times**

Explanation:
Indicates the number of times the specified character was found.

User response:
No action is required.

FECA921I **Chars *chars* not found on any lines**

Explanation:
Indicates that the specified characters were not found on any of the lines.

User response:
No action is required.

FECA922I **Search for CHARS *chars* was successful.**

Explanation:
Indicates the search for the indicated characters produced matches.

User response:
No action is required.

FECA923E **Check for misspelled keywords or embedded blanks in search string.**

Explanation:
Indicates there may be invalid keywords or blanks embedded within the search string.

User response:
Verify and correct the search string to remove embedded blanks or to correct keywords.

FECA924E ***string*** **and *string* cannot both be specified for FIND command.**

Explanation:
You specified two strings for the FIND command.

User response:
You must specify one FIND string at a time.

FECA925E **Put quotes (" ") around the string of characters to be displayed.**

Explanation:
The string of characters is not enclosed in quotes.

User response:
Place the string of characters inside quotes.

FECA926E **Maximum parameter length is 80**

Explanation:
The parameter you specified is too long.

User response:
Specify a parameter that is 80 characters or less.

FECA927E **Invalid COLS parm. Valid parms are ON, OFF, or blank**

Explanation:

COLS was issued with an invalid parameter. Issuing COLS with no parameters acts as an ON/OFF toggle. ON and OFF are the only parameters accepted.

User response:
Enter COLS ON or COLS OFF. COLS ON turns the COLS display on; COLS OFF turns the COLS display off.

FECA930I No columns eligible for resizing.

Explanation:
You cannot resize any columns.

User response:
No action is required.

FECA931I No columns eligible for sorting

Explanation:
You cannot sort any columns.

User response:
No action is required.

FECA932I TBMOD failed. RC=*rc*

Explanation:
An unexpected return code occurred during TBMOD.

User response

Suggested diagnostics:

- See z/OS ISPF Services Guide under TBMOD.
- Review ISPTLIB allocation.
- Review security-controlled access to ISPTLIB data sets.

FECA933E Invalid column name: missing quote

Explanation:
SORT or CSORT was issued with a parameter that had an initial quotation character, but not a second closing quotation character.

User response:
Either clear the command line and select the desired sort column(s) from the displayed selection list or correct the command on the command line.

FECA934E More than 9 columns specified

Explanation:
SORT or CSORT was issued with too many columns specified as sort columns. A maximum of 9 sort columns can be specified.

User response:
Either clear the command line and select the desired sort column(s) from the displayed selection list or correct the command on the command line.

FECA935E Invalid column name

Explanation:
SORT or CSORT was issued with a column parameter that does not match any column name. A list of the correct column names is seen in the SORT selection panel.

User response:
Either clear the command line and select the desired sort column(s) from the displayed selection list or correct the command on the command line.

FECA936E Invalid row selection character

Explanation:
An invalid selection character was entered in the SSID selection list. The only valid selection character is S. Alternatively, place the cursor on the desired line and press ENTER (without a line selection character).

User response:
Clear the invalid character.

FECA937E Only one row selection allowed

Explanation:
More than one SSID was selected from the SSID selection list. A maximum of one SSID can be selected.

User response:
Clear all, or all but one row selection character.

FECA938E Invalid command

Explanation:
An invalid command was entered on the SSID selection list panel.

User response:
Clear the command.

FECA939E Read of control file failed

Explanation:
Reading the control data set failed.

User response:
Check the product setup (accessed from the main menu) to view the control data set currently in use. Verify that the data set name is correct.

FECA940E Invalid DB2 Control data set

Explanation:
Allocation of the control data set failed.

User response:
Check the product setup (accessed from the main menu) to view the control data set currently in use. Verify that the data set name is correct.

FECA942E IFCARC1=*return code* IFCARC2=*reason code*

Explanation:
The Db2 command issued failed. The return code and reason code received from Db2 are in the error message. If there is any command output, it is displayed.

User response:
Check the command for possible mistyping, invalid syntax, or other errors. Refer to https://www.ibm.com/support/knowledgecenter/en/SSEPEK for information about the messages and codes for your version of Db2.

FECA943E Invalid command

Explanation:
An invalid command was issued. It is not supported on the current panel.

User response:
Check the command for typographical error. Clear or correct the command.

FECA944I Empty History

Explanation:
This is an informational message. The history database is empty. If commands were previously entered, then either HCLEAR was issued or the size of the history database was set to 0. If ISPTABL and ISPTLIB are not allocated, history is not remembered across sessions, and each new session has an empty history database.

User response:
No action is required. To verify allocation of ISPTLIB and ISPTABL, ISRDDN and ISPLIBD can be useful. Refer to https://www.ibm.com/support/knowledgecenter/en/SSLTBW to access the ISPF services guide for your version of z/OS.

FECA945E Invalid history size limit

Explanation:
An invalid character was found in the History Size Limit field. Only numeric values from 0-999 are valid.

User response:
Enter a valid value in the History Size Limit field.

FECA946I No DB2 command history output library allocated

Explanation:
This is an informational message. ISPTABL is not allocated. The history database cannot be saved across sessions when ISPTABL is not allocated.

User response:
No action is required. If saving history across sessions is desired, see product installation instructions for allocating ISPTABL (and ISPTLIB).

FECA947I No DB2 command history input library allocated

Explanation:
This is an informational message. ISPTLIB is not allocated. If a history database is saved across sessions (using ISPTABL DD), the ISPTLIB DD is used to initialize a new Db2 Command Processor session. If ISPTLIB is not allocated, this cannot occur and the history starts out empty.

User response:
No action is required. If saving history across sessions is desired, see product installation instructions for allocating ISPTLIB (and ISPTABL).

FECA948E TBOPEN failed. RC=*return code*

Explanation:
TBOPEN for the history table failed. *return code* is the return code from the TBOPEN service.

User response:
Check ISPTLIB allocation. Verify the data sets in ISPTLIB. Verify it is a valid PDS. See ISPF manuals for ISPTLIB requirements.

FECA949E Invalid command

Explanation:
An invalid command was entered.

User response:
Check for typographical error. Clear or correct the command. Issue **HELP** for the Db2 Command Processor tutorial to see what commands are valid. **KEYS** might also be a useful command, since some PF keys are set to valid Db2 Command Processor commands.

FECA950E No SSIDs in control file

Explanation:
There are no valid SSIDs found in the Db2 control file specified.

User response:
A control file with no SSIDs is not useful. It is probably not the control file desired. See product installation instructions for information about creating and building a control file.

FECA951I History cleared

Explanation:
History was cleared either by issuing the HCLEAR command or by setting the History Size Limit to 0.

User response:
No action is required.

FECA952E Unable to list data sharing members. Display failed

Explanation:
Command failed attempting to get a list of data sharing members. The reason code and return code are listed in the message.

User response:
Refer to https://www.ibm.com/support/knowledgecenter/en/SSEPEK for information about the messages and codes for your version of Db2.

FECA953I Zero data sharing members found

Explanation:

Zero data sharing members found. The current SSID is not a member of a data sharing group.

User response:
The Datasharing Member field should be left blank.

FECA954E Invalid command

Explanation:
An invalid command was issued from the datasharing members list/selection panel.

User response:
Clear the command.

FECA955I No member selected

Explanation:
You exited the datasharing member selection panel without selecting a datasharing member.

User response:
No action is required.

FECA956E Invalid row selection character

Explanation
An invalid selection character was entered in the History output display. A command listed in the History display can be selected for execution either by selecting it with an "S" selection character, or by placing the cursor anywhere on a line within the command and pressing Enter.

When selecting by cursor placement, the cursor can be on the line selection input line, which also has a command number, or on a line with some command text.

User response:
Clear the invalid character.

FECA957E Only one row selection allowed

Explanation:
More than one command was selected from the History display. Only one History command can be selected.

User response:
Clear all, or all but one row selection character.

FECA958E Invalid row selection character

Explanation:
An invalid selection character was entered in the displayed list of datasharing members. A datasharing member in this display can be selected by selecting it with an S selection character, or by placing the cursor anywhere on the desired row and pressing Enter.

User response:
Clear the invalid character.

FECA959E Only one row selection allowed

Explanation:
More than one datasharing member was selected from the list of displayed datasharing members.

User response:
Clear all, or all but one row selection character.

FECA960E Cannot list commands without SSID

Explanation:
A command was issued to select a command syntax diagram, but no SSID has been selected. Syntax diagrams cannot be displayed until an SSID has been selected.

User response:
Select an SSID. You can generate a list of SSIDs by clearing the SSID field, or entering a ? (question mark).

FECA961E Invalid row selection character

Explanation:
An invalid selection character was entered in the displayed list of Db2 commands. A Db2 command in this display can be selected by selecting it with an S selection character, or by placing the cursor anywhere on the desired row and pressing Enter.

User response:
Clear the invalid character.

FECA962E Only one row selection allowed

Explanation:
More than one Db2 command was selected from the list of displayed Db2 commands.

User response:
Clear all, or all but one row selection character.

FECA963E Invalid command

Explanation:
An invalid command was issued from the Db2 command list/selection panel.

User response:
Clear the command.

FEC801E Pgm: *program name* Stmt: *statement* Type: *type*

Explanation:
This message is used to convert SQL return code information into a text message. The data from the SQLCA is called using DSNTIAR and formatted into this message.

User response:
Refer to https://www.ibm.com/support/knowledgecenter/en/SSEPEK for information about Db2 SQL for your version of Db2.

FEC802E An invalid return code of *code* was encountered on *function* function.

The error message text follows: *text*

Explanation:
An invalid return code was encountered for the specified function. The supporting diagnostic data are returned in the error message.

User response:
Refer to https://www.ibm.com/support/knowledgecenter/en/SSEPEK for information about the messages and codes for your version of Db2.

FEC803E **The first character of the command is not a dash. Correct the syntax of the DB2 command and resubmit.**

Explanation:
The first character of the command is not a dash. Correct syntax for a Db2 command dictates that the command be preceded by a dash.

User response:
Precede the command with a dash ('-') and reenter.

FEC804E ***message_text***

Explanation:
An error occurred during call attach initialization.

User response:
Refer to the message text for details. If a reason code accompanies the message, use the reason code to help you determine the appropriate corrective action. If you need assistance, contact IBM Software Support.

FEC901E **The default load library could not be located.**

Explanation:
The data set name entered for Db2 Tools Load Library was not found.

User response:
Enter a valid loadlib data set name and continue.

FEC902E **A DB2 subsystem ID has to be entered for processing.**

Explanation:
There was no valid value entered for Db2 subsystem ID.

User response:
Enter a valid Db2 subsystem name.

FEC903E **The default GDG base data set name could not be located.**

Explanation:
The data set name entered for GDG Base model was not found.

User response:
Enter a valid model data set name and continue.

FEC904E **The specified data set could not be opened for I/O.**

Explanation:
A VSAM open error occurred while attempting to open the data set specified for the Db2 Control File.

User response:
Verify that the VSAM data set is accessible.

FEC905E **An unexpected return code from VSAM was encountered while doing a read of the control file. RC1=*rc* RC2=*rc***

Explanation:
A VSAM READ error occurred while attempting to access the data set specified for the Db2 Control File. The VSAM return code is provided for diagnostic purposes.

User response:
Refer to https://www.ibm.com/support/knowledgecenter/en/SSEPEK for information about the messages and codes for your version of Db2.

FEC906I **The control file record for DB2 subsystem *ssid* has been successfully updated.**

Explanation:
The Db2 Control File record has been successfully updated based on the definitions for the specified Db2 subsystem.

User response:
No action is required.

FEC907E **An unexpected return code from VSAM was encountered while doing an update operation of the control file. RC1=*rc* RC2=*rc***

Explanation:
A VSAM update error occurred while attempting to update the data set specified for the Db2 Control File. The RC1 and RC2 (VSAM return cards) are provided for diagnostic purposes.

User response:
Refer to https://www.ibm.com/support/knowledgecenter/en/SSEPEK for information about the messages and codes for your version of Db2.

FEC908I **The control file record for DB2 subsystem *sys* has been successfully added.**

Explanation:
The Db2 Control File record has been successfully updated based on the definitions for the specified Db2 subsystem.

User response:

No action is required.

FEC909E **Invalid value. Valid options are 1 and 2.**

Explanation:
The value you specified is not valid. valid values are 1 and 2.

User response:
Enter a valid value.

FEC910E **An unexpected return code from VSAM was encountered while doing an add operation to the control file. RC1=*rc* RC2=*rc***

Explanation:
A VSAM error occurred while attempting to perform an add operation to the specified Db2 Control File. The RC1 and RC2 (VSAM return codes) are provided for diagnostic purposes.

User response:
Refer to https://www.ibm.com/support/knowledgecenter/en/SSEPEK for information about the messages and codes for your version of Db2.

FEC911E **The (F)IND command was entered but no parameters were specified.**

Explanation:
No parameters were specified with the (F)IND command. No match can be made unless you specify a string to find.

User response:
Enter a FIND parameter.

FEC912I **The requested find string was not found.**

Explanation:
No matches were found for the string you specified with the FIND command.

User response:
No action is required.

FEC913I **The control file record has been successfully updated.**

Explanation:
The control file was updated successfully.

User response:
No action is required.

FEC914E **An unknown column was specified using the SORT command.**

Explanation:
The column you specified with the SORT command is not known.

User response:
Verify that you correctly typed the name of the column or select another column.

FEC915E **SORT is not supported for the specified column.**

Explanation:
The column you attempted to SORT is not supported as a column on which to sort.

User response:
Refer to the sort columns listed on the Define Sort Columns panel for a list of valid columns on which the sort can be based and redefine the sort.

FEC916E **Sort column not entered. Column name or number must be specified.**

Explanation:
A column was not specified with the SORT. A column name or number must be specified for the SORT command.

User response:
Ensure that if the column name is used, that all spaces in the name are replaced with an underscore.

FEC917E **Put an ending quote at the end of the string.**

Explanation:
You must place a quote at the end of the string.

User response:
Place a quote at the end of the string.

FEC918 **CHARS *string* not found. Press PF5 to continue from top.**

Explanation:
The indicated character string was not found.

User response:
To continue searching for the character string from the top of the dialog, press PF5.

FEC919 ***chars foundstr* not found. Press PF5 to continue from bottom.**

Explanation:
The indicated character string was not found.

User response:
To continue searching for the character string from the bottom of the dialog, press PF5.

FEC920E **File tailoring open returned a file tailoring already in progress condition**

Explanation:
An attempt to perform file tailoring for utility customization failed. There was a file tailoring session already in progress. File tailoring sessions cannot be performed concurrently.

User response:
No action is required.

FEC921E **File tailoring open returned the output file already in use condition -- ENQ failed**

Explanation:
An attempt to open the Db2 Control File failed with an ENQ error. The data set is already open for output.

User response:
Verify that you are the only user attempting to access this file.

FEC922E **File tailoring open returned the skeletal file or output file not allocated condition**

Explanation:
An attempt to perform file tailoring failed because either the tailoring skeleton file or output file is not allocated.

User response:
Verify that all required files are allocated prior to performing file tailoring.

FEC923E **File tailoring open returned a severe error condition**

Explanation:
An attempt to perform file tailoring failed because a severe error condition was encountered on open.

User response:
Verify that all required files are allocated and accessible prior to performing file tailoring.

FEC924E **File tailoring open returned an unknown code -- severe error**

Explanation:
An attempt to perform file tailoring failed because a severe error condition was encountered on open.

User response:
Verify that all required files are allocated and accessible prior to performing file tailoring.

FEC925E **File tailoring close returned a file not open condition -- severe error**

Explanation:
An attempt to perform file tailoring failed because a File-Not-Open condition was encountered on close.

User response:
Verify that all required files are allocated and accessible and that there are no other tailoring sessions running concurrently with your session.

FEC926E **File tailoring close returned an output file in use condition**

Explanation:
An attempt to perform file tailoring failed because an Output-File-In-Use condition was encountered on close.

User response:
Verify that all required files are allocated and accessible and that there are no other tailoring sessions running concurrently with your session.

FEC927E **File tailoring close returned a skeletal file or output file not allocated condition**

Explanation:
An attempt to close file tailoring failed because either a tailoring skeleton file or output file was not allocated.

User response:
Verify that all required files are allocated and accessible and that there are no other tailoring sessions running concurrently with your session.

FEC928E **File tailoring close returned a severe error**

Explanation:
An attempt to perform file tailoring failed because a severe error condition was encountered on close.

User response:
Verify that all required files are allocated and accessible prior to performing file tailoring.

FEC929E **File tailoring close returned an unknown code -- severe error**

Explanation:
An attempt to perform file tailoring failed because a severe error condition was encountered on close.

User response:
Verify that all required files are allocated and accessible prior to performing file tailoring.

FEC930E **File tailoring close returned an output member exists in the output library and NOREPL was specified**

Explanation:
An attempt to perform file tailoring failed because the close process could not replace the pre-existing tailored member in the output file.

User response:
Change the output member name to a new name or ensure that the output library allows for member replacement.

FEC931E **File tailoring include returned a skeleton does not exist condition**

Explanation:

An attempt to perform file tailoring failed because the tailoring process could not locate a required tailoring skeleton.

User response:
Assure that all required files are allocated to perform file tailoring.

FEC932E **File tailoring include returned a skeleton in use -- ENQ failed condition**

Explanation:
An attempt to access a tailoring skeleton failed with an ENQ error (member-in-use).

User response:
Verify that all required tailoring files are allocated and that there are no other tailoring sessions running concurrently.

FEC933E **File tailoring include returned a data truncation or skeleton library or output file not allocated condition**

Explanation:
An attempt to perform file tailoring failed because either the tailoring skeleton file or output file is not allocated.

User response:
Verify that all required files are allocated prior to performing file tailoring.

FEC934E **File tailoring include returned a severe error condition**

Explanation:
An attempt to perform file tailoring failed because a severe error condition was encountered on an include operation.

User response:
Verify that all required files are allocated and accessible prior to performing file tailoring.

FEC935E **File tailoring include returned an unknown condition -- severe error**

Explanation:
An attempt to perform file tailoring failed because a severe error condition was encountered on an include operation.

User response:
Verify that all required files are allocated and accessible prior to performing file tailoring.

FEC936E **Allocation error - The ISPFILE DD is already allocated and cannot be deallocated - Process not completed**

Explanation:
The ISPFILE DD allocation failed. The DD is already allocated and cannot be deallocated for this TSO session. The process did not complete successfully.

User response:
No action is required.

FEC937E **Allocation Error - An error was encountered allocating the ISPWRK1 or ISPWRK2 DD - Process not completed**

Explanation:
The ISPWRK1 or ISPWRK2 DD allocation failed.

User response:
Verify TSO session parameters are set correctly for your site prior to allocation of these DD statements. The process did not complete successfully.

FEC938E **Field Required - The data set entered is a partitioned data set and the member name is required**

Explanation:
A required field was not specified. The data set entered is a PDS (partitioned data set) and a member in this PDS must be referenced.

User response:
Enter a valid member name for PDS access.

FEC939E **The only valid values are "T" for tracks and "C" for cylinders**

Explanation:
You specified an invalid value. The only valid values are "T" for tracks and "C" for cylinders

User response:
Specify a valid value.

FEC940E **The specified data set could not be found in the MVS catalog.**

Explanation:
The specified data set could not be found in the MVS catalog.

User response:
Ensure that the data set name is correct.

FEC941E **The RFIND key works only after a FIND character string is entered.**

Explanation:
A repeat FIND (RFIND) was issued before a FIND command was issued. You must issue FIND before RFIND will work.

User response:
Issue FIND prior to attempting to issue RFIND.

FEC942E **Invalid Sort number. Enter a valid digit.**

Explanation:

An invalid character was entered in the Srt column. Valid characters are the digits 1, 2, 3,... up to 9, or the number of sortable columns, whichever is less.

User response:
Specify a valid sort number.

FEC943E Same Sort number entered twice

Explanation:
The same sort number was entered for more than one column. The screen is positioned to the second instance. Sort sequence numbers must be unique.

User response:
Specify a valid sort number.

FEC944E Sort sequence skips a number.

Explanation:
The selected sorting sequence skips a number. This is not allowed. The screen is positioned to a selection whose number is lacking an immediate predecessor. The sort sequence is completely rebuilt from the Cmd (and Dir) information. Any previously existing sort sequence is entirely replaced. It is not added to or extended by the new entries.

User response:
Specify a valid sort sequence that does not skip a number.

FEC945E Invalid Dir entered. Must be A or D (ascending/descending).

Explanation:
The selected sorting direction is invalid. Only A (ascending) or D (descending) can be specified. A blank indicates ascending (default).

User response:
Specify a valid sorting direction.

FEC946E Dir not valid without Ord.

Explanation:
A sorting direction was selected for a column that was not selected to be sorted. Sorting direction is only a valid choice for selected columns.

User response:
Select a sorting direction and order.

FEC947E Max Sort Columns exceeded. Sorting first 10 columns.

Explanation:
More columns were selected for sorting than are supported. Nine columns can be selected. Under certain circumstances the limit is less than nine, due to internal constraints. For example, sorting a date field can be implemented by three sorts of partial column fields. In that case, the column would count as three toward the maximum of nine, not one.

User response:
Specify the appropriate allowable maximum number of sort columns.

FEC948E Fix Columns cannot exceed screen size.

Explanation:
More columns were selected to be fixed than will fit on the screen.

User response:
Remove the (F) selection character from one or more columns.

FEC950E Invalid selection character. "F" and "U" are valid.

Explanation:
An invalid Cmd character was entered. Valid characters are F (fix) and U (unfix). Fix causes the column to move to the fixed area on the left side of the screen. Fixed columns do not scroll horizontally when LEFT or RIGHT scrolling commands are issued. Unfix moves the column out of the fixed area, and allows it to scroll horizontally when LEFT and RIGHT scroll commands are issued.

User response:
Either remove the invalid character or enter a valid one.

FEC951E Invalid entry. Must be numeric.

Explanation:
An invalid Cmd value was entered. Cmd values must be numeric. If the column is fixed, the number must be in the fixed range. If the column is not fixed, the number must be in the unfixed range.

User response:
Either remove the invalid number or enter a valid one.

FEC952E Invalid entry for fixed column.

Explanation:
An invalid Cmd value was entered for a fixed column. Valid selections for fixed column are up to the number of fixed columns.

User response:
Either remove the invalid number or enter a valid one.

FEC953E Invalid entry for unfixed column.

Explanation:
An invalid Cmd value was entered for an unfixed column. The number must be less than the number of columns, and greater than the number of fixed columns.

User response:
Either remove the invalid number or enter a valid one.

FEC954E Invalid value entered for column size: non-numeric data.

Explanation:
An invalid Cmd value was entered. This must be a number between the values in the MIN and MAX fields.

User response:
Either remove the invalid number or enter a valid one.

FEC955E **Invalid value entered for column size: out of range.**

Explanation:
An invalid Cmd value was entered. This must be a number between the values in the MIN and MAX fields. MIN is the smallest acceptable value. MAX is the largest acceptable value.

User response:
Either remove the invalid number or enter a valid one.

FEC956E **Total fixed column sizes cannot exceed screen size.**

Explanation:
The Cmd values entered would result in the sum of the fixed column sizes to exceed the screen size. This is not allowed. The fixed columns are those with an or in the Fix column. Fixed columns are always displayed, and so must fit on the screen.

User response:
Either change the fixed column sizes so that the total is less than the screen size or cancel to return to the previous panel.

FEC957E **New configuration makes this column size invalid.**

Explanation:
The requested column sizes make at least one unfixed column unable to be displayed. The cursor is positioned on the value where the problem was detected. The unfixed area on the screen would be too small to show the column where the cursor is placed.

User response

Do one of the following:

- Make the column where the cursor is smaller so that it can fit in the available unfixed area.
- Set it to its maximum size (width).
- Make the fixed area smaller.
- Cancel to return to the previous panel.

FEC958E **Column does not fit in unfixed area in new configuration.**

Explanation:
The requested column sizes would make the unfixed column where the cursor is positioned undisplayable. The unfixed area on the screen would be too small to show this column.

User response:
Shrink the fixed area by either unfixing columns or making fixed columns smaller. The column where the cursor cannot be partially displayed (min-max) so its size cannot be changed.

FEC959E **New configuration makes this column size invalid.**

Explanation:
Fixing the requested columns would shrink the available area for unfixed columns unacceptably. One or more unfixed columns would not fit in the remaining unfixed area of the screen. The cursor is placed on a row that represents one such column. Therefore, the requested configuration is not allowed.

User response:
To change column sizes, cancel out of the CFIX function and invoke the CSIZE function. Either cancel to exit CFIX with no change or blank out one or more FIX selections until an allowable fixed size is reached.

FEC960E **Invalid fixed selections. Would not leave enough space for this column.**

Explanation:
Fixing the columns requested would make at least one unfixed column undisplayable. The cursor is positioned on the row that represents one such unfixed column, whose minimum displayable size would not fit in the available screen area.

User response

Shrink the requested fixed area by either:

- Requesting fewer fixed columns.
- Unfixing one or more fixed columns.
- Cancel out of CFIX and invoke CSIZE in order to shrink one or more fixed columns enough so that all unfixed columns have the space they require.

FEC962E **Duplicate Cmd values entered.**

Explanation:
Duplicate Cmd numbers were entered. The cursor points to the second instance of a Cmd value.

User response:
Either change this value, clear it, or exit the CORDER function.

FEC963E **Cursor not on data element.**

Explanation:
CEXPAND was issued and the cursor was not located on a valid (expandable) area. CEXPAND requires the cursor to be positioned on a data element (non-heading area) in the dynamic area of the display. Or CEXPAND can be issued specifying the row and column of the data element to expand.

User response:
Ensure the cursor is located on a valid (expandable) area prior to issuing the CEXPAND command.

FEC964E **Invalid scroll amount for CRIGHT. Must be numeric.**

Explanation:
Invalid (non-numeric) parameter to CRIGHT specified. CRIGHT accepts one numeric parameter: the number of columns to scroll right. If no parameter is entered a value of 1 is assumed.

User response:
Specify a numeric parameter to the CRIGHT command.

FEC965E **Invalid scroll amount for CLEFT. Must be numeric.**

Explanation:
Invalid (non-numeric) parameter to CLEFT specified. CLEFT accepts one numeric parameter: the number of columns to scroll left. If no parameter is entered, a value of 1 is assumed.

User response:
Specify a numeric parameter to the CLEFT command.

FEC966E **Invalid parameter to ICRIGHT; must be numeric.**

Explanation:
A parameter to ICRIGHT is not numeric. ICRIGHT (inner column scroll right) accepts either zero, one, or two numeric parameters. ICRIGHT can be abbreviated as ICR.

User response:
Specify a valid, numeric parameter for ICRIGHT.

FEC967E **Parameter to ICRIGHT too long. Invalid.**

Explanation:
A parameter to ICRIGHT is too long. ICRIGHT does not process more than eight digits in a parameter, which is more than double any reasonable value.

User response:
Specify a valid parameter for ICRIGHT.

FEC968E **Parameter to ICRIGHT is zero. Invalid.**

Explanation:
A parameter to ICRIGHT has the value zero. This is not supported.

User response:
Specify non-zero parameters to ICRIGHT.

FEC969E **ICRIGHT: unspecified column.**

Explanation:
ICRIGHT was invoked with no parameters and the cursor is not positioned in the dynamic panel area.

User response:
Either put the cursor in the column that should be scrolled or specify the column by number. Column numbers can refer to visible columns (in the current display window) only. Number starts at 1, on the left side.

FEC971E **ICRIGHT: Column number specified is too big.**

Explanation:
A column number parameter to ICRIGHT must be between 1 and the number of columns currently on the display screen.

User response:
To refer to a column by number you must first position the display window so that the desired column is visible.

FEC972E **Invalid parameter to ICLEFT; must be numeric.**

Explanation:
A parameter to ICLEFT is not numeric. ICLEFT (inner column scroll left) accepts either zero, one, or two numeric parameters. ICLEFT can be abbreviated as ICL.

User response:
Specify a valid parameter for ICLEFT.

FEC973E **Parameter to ICLEFT too long. Invalid.**

Explanation:
A parameter to ICLEFT is too long. ICLEFT does not process more than eight digits in a parameter which is more than double reasonable value.

User response:
Specify a parameter less than or equal to eight digits for ICLEFT.

FEC974E **Parameter to ICLEFT is zero. Invalid.**

Explanation:
A parameter to ICLEFT has the value zero. This is not supported.

User response:
Specify a non-zero number for ICLEFT.

FEC975E **ICLEFT: unspecified column.**

Explanation:
ICLEFT was invoked with no parameters and the cursor is not positioned in the dynamic panel area.

User response:
Either put the cursor in the column that should be scrolled or specify the column by number. Column

numbers can refer to visible columns (in the current display window) only. Numbering starts at 1 on the left side.

FEC976E **Column selected not sortable. Sort selection list presented.**

Explanation:
You cannot perform a SORT on the column you selected. Valid sort columns are displayed in the sort selection list.

User response:
Sort on one of the valid columns displayed in the selection list.

FEC977E **ICLEFT: Column number specified is too big.**

Explanation:
A column number parameter to ICLEFT must be between 1 and the number of columns currently on the display screen.

User response:
To refer to a column by number, you must first position the display window so that the desired column is visible.

FEC978E **Invalid column number specified for SORT (not numeric).**

Explanation:
Invalid column number parameter to CSORT specified (non-numeric).

User response:
Specify a column number parameter to CSORT that is between 1 and the number of columns currently on the display screen. This can be followed by a direction value A or D (ascending/descending).

FEC979E **Invalid column number specified. Too many digits.**

Explanation:
Invalid parameter to CSORT specified. More than eight digits were specified. Parsing stops at eight digits.

User response:
Specify a column number parameter between 1 and the number of columns currently on the display screen. This can be followed by a direction value A or D (ascending/descending).

FEC980E **Invalid column number specified: zero.**

Explanation:
Invalid parameter to CSORT was specified (zero).

User response:
Specify a column number parameter to CSORT that is between 1 and the number of columns currently on the display screen. This can be followed by a direction value A or D (ascending/descending).

FEC981E **Invalid column number specified: out of range.**

Explanation:
Invalid parameter to CSORT was specified (zero).

User response:
Specify a column number parameter to CSORT that is between 1 and the number of columns currently on the display screen. This can be followed by a direction value A or D (ascending/descending)

FEC982E **Invalid view. View adjusted.**

Explanation:
The current view was adjusted but not deleted. The saved view did not match the report requirements. This could be caused by the report changing or the view file getting corrupted.

User response:
The adjusted view will be used. You can issue CSET to modify the view.

FEC983E **Invalid view. View deleted.**

Explanation:
Invalid data was found in a view for this report. The view was deleted and contents ignored. This could be caused by the report changing or the view file getting corrupted.

User response:
You can issue CSET to create a view that will match current report.

FEC984E **Unexpected return code from TBSTATS: *rc***

Explanation:
An unexpected failure issuing TBSTATS was received.

User response:
Refer to https://www.ibm.com/support/knowledgecenter/en/SSLTBW to access the ISPF services guide for your version of z/OS.

FEC985E **View Library not allocated.**

Explanation:
A view input library has not been allocated. In order for a user to save and use report customizations that are created via the CSET command, ISPTABL and ISPTLIB must be allocated.

User response:
Refer to https://www.ibm.com/support/knowledgecenter/en/SSLTBW to access the ISPF services guide for your version of z/OS.

FEC986E **TBCREATE failed. RC=*rc***

Explanation:

TBCREATE was issued to create a view. It failed with a (hex) return cod as indicated in the message.

User response:
Review ISPTLIB allocation and data set characteristics. Refer to https://www.ibm.com/support/knowledgecenter/en/SSLTBW for information about ISPF messages and codes for your version of z/OS.

FEC987E TBOPEN failed. RC=*rc*

Explanation:
TBOPEN was issued to open a view. It failed with a (hex) return code as indicated in the message.

User response:
Review ISPTLIB allocation and data set characteristics. Refer to https://www.ibm.com/support/knowledgecenter/en/SSLTBW for information about ISPF messages and codes for your version of z/OS.

FEC988E TBGET failed. RC=*rc*

Explanation:
A TBGET produced a return code (as indicated in the message).

User response:
Review ISPTLIB allocation and data set characteristics. Refer to https://www.ibm.com/support/knowledgecenter/en/SSLTBW for information about ISPF messages and codes for your version of z/OS.

FEC989E TBMOD failed. RC=*rc*

Explanation:
A TBMOD produced an error and return code (as indicated in the message).

User response:
Review ISPTLIB allocation and data set characteristics. Refer to https://www.ibm.com/support/knowledgecenter/en/SSLTBW for information about ISPF messages and codes for your version of z/OS.

FEC990E TBCLOSE failed. RC=*rc*

Explanation:
TBCLOSE failed with a (hex) return code as indicated in the message.

User response:
Review ISPTLIB allocation and data set characteristics. Refer to https://www.ibm.com/support/knowledgecenter/en/SSLTBW for information about ISPF messages and codes for your version of z/OS.

FEC991E TBDELETE failed. RC=*rc*

Explanation:
TBDELETE failed with a (hex) return code as indicated in the message.

User response:
Review ISPTLIB allocation and data set characteristics. Refer to https://www.ibm.com/support/knowledgecenter/en/SSLTBW for information about ISPF messages and codes for your version of z/OS.

FEC992E Invalid selection.

Explanation:
A command that is not supported on this panel was selected.

User response:
Issue a valid command for the panel.

FEC993I Permanent view not supported.

Explanation:
Db2 Query Monitor detected something that prevents views from being saved. The permanent view flag cannot be set to Y. The most likely cause of this is that either ISPTLIB or ISPTABL (or both) have not been properly allocated.

User response:
Review ISPTLIB allocation and data set characteristics. Refer to https://www.ibm.com/support/knowledgecenter/en/SSLTBW for information about ISPF messages and codes for your version of z/OS.

FEC994E Invalid row number.

Explanation:
CEXPAND was issued with an invalid parameter of zero. CEXPAND can be issued with no parameters and the cursor on a data field, or with two parameters. The two parameters are the row number, followed by the column number of the data element to be expanded. The row number is counted down from the top, starting with the first scrollable row (heading not counted) The column number is counted from left to right, starting with the left column in the current display window.

User response:
Specify a valid parameter count for use with CEXPAND.

FEC995E Invalid column number.

Explanation:
CEXPAND was issued with an invalid parameter of zero. CEXPAND can be issued with no parameters and the cursor on a data field, or with two parameters. The two parameters are the row number, followed by the column number of the data element to be expanded. The row number is counted down from the top, starting with the first scrollable row (heading not counted) The column number is counted from left

to right, starting with the left column in the current display window.

User response:
Specify a valid parameter count for use with CEXPAND.

FEC996E Invalid digits.

Explanation:
CEXPAND was issued with an invalid parameter of zero. CEXPAND can be issued with no parameters and the cursor on a data field, or with two parameters. The two parameters are the row number, followed by the column number of the data element to be expanded. The row number is counted down from the top, starting with the first scrollable row (heading not counted) The column number is counted from left to right, starting with the left column in the current display window.

User response:
Specify a valid parameter count for use with CEXPAND.

FEC997E Too many digits.

Explanation:
CEXPAND was issued with an invalid parameter of zero. CEXPAND can be issued with no parameters and the cursor on a data field, or with two parameters. The two parameters are the row number, followed by the column number of the data element to be expanded. The row number is counted down from the top, starting with the first scrollable row (heading not counted) The column number is counted from left to right, starting with the left column in the current display window.

User response:
Specify a valid parameter count for use with CEXPAND.

FEC998E Zero parameter invalid.

Explanation:
CEXPAND was issued with an invalid parameter of zero. CEXPAND can be issued with no parameters and the cursor on a data field, or with two parameters. The two parameters are the row number, followed by the column number of the data element to be expanded. The row number is counted down from the top, starting with the first scrollable row (heading not counted) The column number is counted from left to right, starting with the left column in the current display window.

User response:
Specify a non-zero parameter.

FEC999E Invalid parameter count: must be either two or zero parms.

Explanation:
CEXPAND was issued with an invalid number of parameters. CEXPAND can be issued with no parameters and the cursor on a data field, or with two parameters. The two parameters are the row number, followed by the column number of the data element to be expanded. The row number is counted down from the top, starting with the first scrollable row (heading not counted) The column number is counted from left to right, starting with the left column in the current display window.

User response:
Specify a valid parameter count for use with CEXPAND.

Notices

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

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

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

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

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered marks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at: http://www.ibm.com/legal/copytrade.shtml.

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

Terms and conditions for product documentation

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

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

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

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

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

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

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

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

Privacy policy considerations

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

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

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

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

Index

Special Characters

/f cqmstc, ISMERROR_DETAIL 26

A

About this information vii
accessibility
  overview 9
additional documentation 55
ADHEMAC1 edit macro variables 60
APPLIANCE_CONNECT_RETRY_COUNT 16
APPLIANCE_NETWORK_REQUEST_TIMEOUT 17
APPLIANCE_PING_RATE 17
APPLIANCE_PORT 18
APPLIANCE_RETRY_INTERVAL 18
APPLIANCE_SERVER 19
APPLIANCE_SERVER_LIST 19
AUDIT 21
AUTHID 21

C

CICS Login User ID reporting 44
CICS_USERID 22
COLLECT_COMMIT_ROLLBACK 22
collector agent
  configuration 14
collector agent parameters
  AUTHID 21
collector agent started task 15
comments 8
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 14
  collector agent started task 15
configuring
  additional Db2 collections 38
  Configuring data streaming modes 39
  failover 41
  hot failover 41
  mirroring 42
  multistream 42
  single appliance 40
control file
  creating 12
  required statements 13
cookie policy 115
customizing
  JCL members 12

D

data collection
  DB2 utilities 46
  process 45
  source of collected event types 46
Db2 function level support 4
Db2 Query Monitor
  compatibility with collector agent 3
DEBUG 22
DIAG_THRESHOLD 23
DIAG_THRESHOLD_DUMPS 23
documentation
  accessing 8
  feedback 8
dynamic LPA facility service CSVDYLPA 12

E

error messages
  codes 63
  collector agent messages 80

F

failover
  configuring 41
filtering
  combined filters 48
  efficiency 48
  event types 48, 49
  process 48
  Stage 1 48
  Stage 2 48
  wildcarding (%) 51
FORCE 24

G

Guardium system
  connection 16

H

HOSTVAR_LIMIT 24
hot failover
  configuring 41

I

ISM_CONSTRAINT_AGE 25
ISM_ERROR_BLOCKS 26
ISM_ERROR_DETAIL 25
ISM_ERROR_MSG_BLOCKS 27

J

JCL
    ADHBIND 14

L

legal notices
    cookie policy 115
    notices 115
    programming interface information 115
    trademarks 115
links
    non-IBM Web sites
    116
LOAD library
    APF authorizing 6

M

MASTER_PROCNAME 27
MAXIMUM_ALLOCATIONS 28
MESSAGE_LOG_LEVEL 28
messages 63
mirroring
    configuring 42
MODIFY command 56
multistream
    configuring 42

N

notices 115

O

OUTAGE_SPILLAREA_SIZE 29

P

parameters 16
policy pushdown 51
PREFER_IPV4_STACK 30
Primary Address Space
    considerations for stopping 44
    usage considerations 43
programming interface information 115

R

reference information 55
reporting
    CICS Login User ID 44

S

S-TAP logging
    requesting 59
    viewing 59
sample library members 55
sample parameter file 59
screen readers and magnifiers 9
SEND_FAIL_EVENT_COUNT 30
service information 8
SHUTDOWN_DIAGNOSTICS 36
single appliance
    configuring 40
SMEM_SIZE 31
SQL Blocking 53
SQL event filtering
    Stage 1 filtering 48, 49
    Stage 2 filtering
        improving efficiency 48
STAP_BLOCKING 32
STAP_MEGABUFFER 32
STAP_STREAM_EVENTS 33
STAP_STREAM_GTT_EVENTS 33
STAP_TERMINATE_OPTIMIZE 34
STAP_UTILITY_TS_TO_TABLE 35
STARTUP_DIAGNOSTICS 35
SUBSYS 36
support information 8

T

TAP_UTILITY_MULTITABLE 34
tech notes 8
trademarks 115
TS_OFFSET 37

U

user IDs
    required user ID authorizations 7

Z

ZIIP_FILTER 37
ZIIP_TCP 38

Product Number: 5656-STQ