

IBM InfoSphere Guardium S-TAP for DB2 on z/OS

Collection Policy Pushdown Reference

Barry Davis, Brandon Wilkie

5/18/2012

This document is intended to assist IBM Technical Sales Engineers tasked with support of Guardium customers in the definition of Guardium Collection Policy used by S-TAP for DB2 on z/OS . Policy Pushdown Mode became available for use 9/27/2011 via UK72285.

IBM InfoSphere Guardium S-TAP for DB2 on z/OS

Collection Policy Rule Reference

OVERVIEW of Policy Pushdown flow on z/OS platform

At startup/connection of S-TAP Agent on z/OS receives the policy information from the Guardium Z Appliance and process/compiles the policy information into a format used by the S-TAP. If policy is acceptable (free of errors) the S-TAP Agent will start the ASC started task if it was not previously running. If ASC started task was previously running the ASC started task will be shut down by the S-TAP Agent and restarted using the new policy.

If the S-TAP Agent encounters errors within the policy information the following types of messages will be displayed in the S-TAP Agent log and the policy will not be activated (no collection starts). *rule error:* messages are currently not displayed in the Guardium Z Appliance.

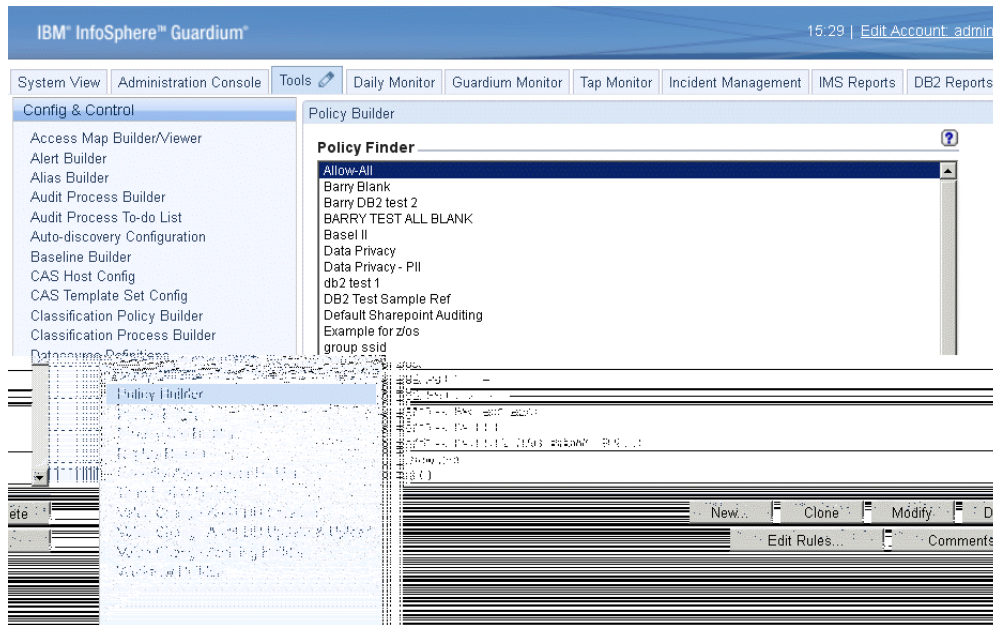
rule error: unrecognized type for OBJECT_NAME=. Valid types are: read, change, %*
rule error: invalid syntax for OBJECT_NAME. Correct syntax is: read, change/schema.name
rule error: invalid syntax encountered at position 0. Syntax starting: ""%acctg_rpt
error: rule discarded due to error

If the ASC started task was previously running and errors are encountered in the newly installed Policy, the policy in error is ignored and the S-TAP collectors continue to use the last known error free policy.

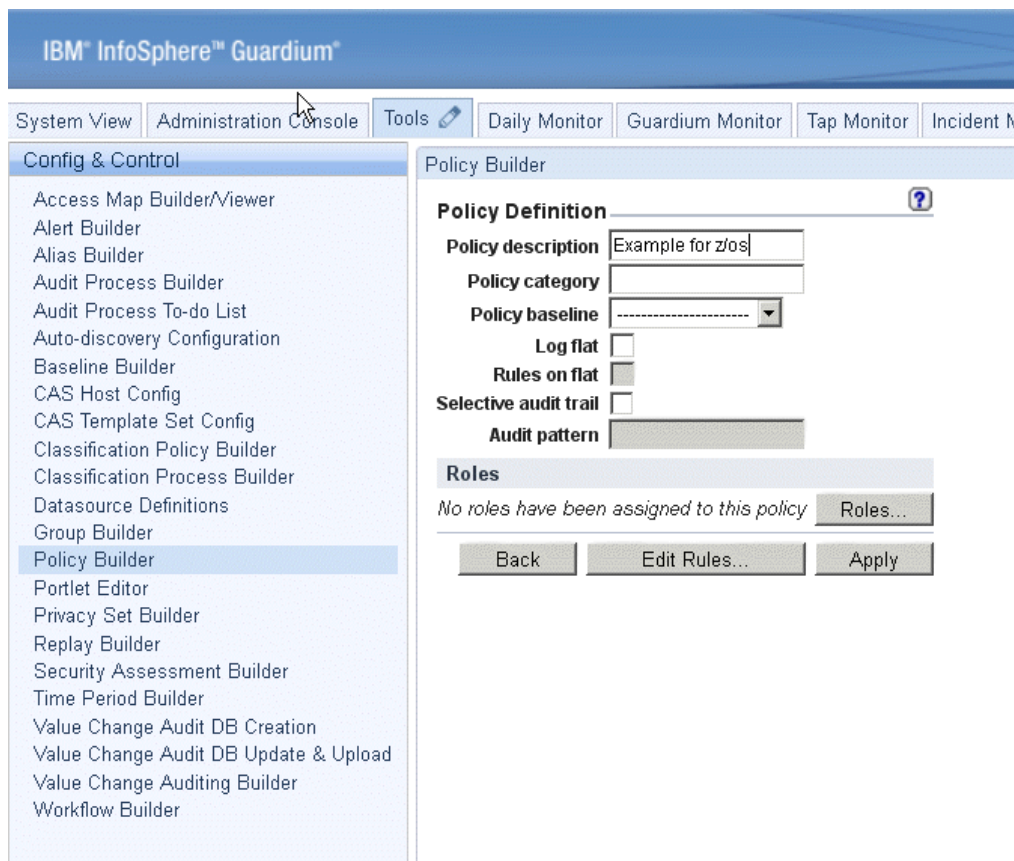
IBM InfoSphere Guardium S-TAP for DB2 on z/OS Collection Policy Rule Reference

Setting up a new policy (4 steps to get us to Policy Rule Definition)

- 1) Start with creation of new Policy via TOOLS > Policy Builder and click on NEW



- 2) Enter Policy description and save by clicking on Apply



IBM InfoSphere Guardium S-TAP for DB2 on z/OS Collection Policy Rule Reference

3) Select Edit Rules

Policy Builder

Policy Definition ?

Policy description Example z/os

Policy category

Policy baseline

Log flat

Rules on flat

Selective audit trail

Audit pattern

Roles

No roles have been assigned to this policy

4) Select Add Access Rule

Policy Builder

Policy Rules ?

Example z/os Filter:

Rule Suggestion

Rule min. ct. Object Group min. ct.

IBM InfoSphere Guardium S-TAP for DB2 on z/OS

Collection Policy Rule Reference

You will be presented a common Rule Definition screen and now must select DB Type.

Field - DB Type Required

For DB2 on z/OS rules, select "DB2 COLLECTION PROFILE" from the drop-down box.

*Selecting this first when creating a new Policy Definition will change display so screen only presents fields used in DB2 on z/OS.

Policy Builder ?

Access Rule Definition ?

Rule #1 of policy **Example for z/os**

Description

Category Classification Severity

<input type="checkbox"/>	Not Server IP	<input type="text"/>	/	<input type="text"/>	and/or Group	<input type="text"/>	
<input type="checkbox"/>	Client IP	<input type="text"/>	/	<input type="text"/>	and/or Group	<input type="text"/>	
<input type="checkbox"/>	Client MAC	<input type="text"/>					
<input type="checkbox"/>	Net Prtcl.	<input type="text"/>	and/or Group	<input type="text"/>			
DB Type <input type="text"/>							
<input type="checkbox"/>	Not Svc. Name	<input type="text"/>	and/or Group	<input type="text"/>			
<input type="checkbox"/>	Not DB Name	<input type="text"/>	and/or Group	<input type="text"/>			
<input type="checkbox"/>	Not DB User	<input type="text"/>	and/or Group	<input type="text"/>			
Client IP/Src App./DB User/Server IP/Svc. Name <input type="text"/>							
<input type="checkbox"/>	Not App. User	<input type="text"/>	and/or Group	<input type="text"/>			
<input type="checkbox"/>	Not OS User	<input type="text"/>	and/or Group	<input type="text"/>			
<input type="checkbox"/>	Not Src App.	<input type="text"/>	and/or Group	<input type="text"/>			
<input type="checkbox"/>	Not Field	<input type="text"/>	and/or Group	<input type="text"/>			
<input type="checkbox"/>	Not Object	<input type="text"/>	and/or Group	<input type="text"/>			
<input type="checkbox"/>	Not Command	<input type="text"/>	and/or Group	<input type="text"/>			

Pattern RE

XMI Pattern RE

App Event Exists Event Type Event User Name

App Event Values Text and/or Group

Numeric Date

Masking Pattern RE Replacement Character

Time Period

Minimum Count Reset Interval minutes

Quarantine for minutes Records Affected Threshold Rec. Vals. Cont. to next rule

Actions

IBM InfoSphere Guardium S-TAP for DB2 on z/OS Collection Policy Rule Reference

Field - DB Type "DB2 COLLECTION PROFILE" results in rule definition just for fields used in DB2 on z/OS.

Policy Builder

Access Rule Definition ?

Rule #1 of policy **Example for z/os**

Description

Category Classification Severity **INFO** ▼

<input type="checkbox"/> Net Prtcl.	<input type="text"/>	and/or Group	<input type="text"/>	<input type="checkbox"/>
<input type="checkbox"/> DB Type	DB2 COLLECTION PROFILE			
<input type="checkbox"/> Svc. Name	<input type="text"/>	and/or Group	<input type="text"/>	<input type="checkbox"/>
<input type="checkbox"/> DB User	<input type="text"/>	and/or Group	<input type="text"/>	<input type="checkbox"/>
<input type="checkbox"/> Client IP/Src App./DB User/Server IP/Svc. Name	<input type="text"/>			<input type="checkbox"/>
<input type="checkbox"/> App. User	<input type="text"/>	and/or Group	<input type="text"/>	<input type="checkbox"/>
<input type="checkbox"/> OS User	<input type="text"/>	and/or Group	<input type="text"/>	<input type="checkbox"/>
<input type="checkbox"/> Object	<input type="text"/>	and/or Group	<input type="text"/>	<input type="checkbox"/>
<input type="checkbox"/> Command	<input type="text"/>	and/or Group	<input type="text"/>	<input type="checkbox"/>
<input type="checkbox"/> Client Info	<input type="text"/>	and/or Group	<input type="text"/>	<input type="checkbox"/>
<input type="checkbox"/> Object/Cmd. Group	<input type="text"/>			<input type="checkbox"/>
<input type="checkbox"/> Masking Pattern	<input type="text"/>	<input type="checkbox"/> RE	Replacement Character	<input type="text"/>
<input type="checkbox"/> Time Period	<input type="text"/>			<input type="checkbox"/>

Actions

Now we can start looking at what the other fields do and the syntax for each of the fields.

IBM InfoSphere Guardium S-TAP for DB2 on z/OS Collection Policy Rule Reference

Field - Svc. Name

Specifies the DB2 subsystem ID(s) that this rule applies to.

Wildcards supported: yes (as of PM55802/UK75726)

Value groups supported: yes

Excludes supported: **NO** Exclude currently not supported even though NOT box is presented on screen.

Case sensitive: yes (DB2 SSIDs are upper case)

Blank means: This policy rule applies to all DB2 subsystems IDs

IBM® InfoSphere™ Guardium®

Manage Members for Selected Group ?

Group Name all DB2s

Group Type

Category

Group Members

Filter



IB1A
I9?2
IA1A

Please select one of the following options

Create & add a new Member named

Add an existing Member to Group

Rename selected Member to

Delete selected Member

[Close this window](#)

IBM InfoSphere Guardium S-TAP for DB2 on z/OS Collection Policy Rule Reference

Field - DB User

Specifies the AuthID filter.

Wildcards supported: yes

Value groups supported: yes

Excludes supported: yes, with NOT keyword (i.e. "NOT CSUSER") or "NOT" checkbox

Case sensitive: yes (most z/OS DB user IDs are upper case)

Blank means: No AuthID filtering

Description: DB User is often the authorisation ID that executes the SQL, can be the BINDER of the plan or package or value of SET CURRENT SQLID. DB User filters on ASC data field ADH_AUTHORIZATION_ID and ADH_CURRENT_SQL_ID

DB User is a stage 1 eligible filter.

IBM® InfoSphere™ Guardium®

Manage Members for Selected Group ?

Group Name PRE SALES USERS PUBLIC

Group Type

Modify Group Type

Category

Modify Category

Group Members

Filter



CSTHUB%
PDDAVI%
PRODDBA
TSSXS%

Please select one of the following options

Create & add a new Member named

Add

Add an existing Member to Group

Add

Rename selected Member to

Update

Delete selected Member

Delete

Add Comments

Aliases...

LDAP

Back

[Close this window](#)

IBM InfoSphere Guardium S-TAP for DB2 on z/OS Collection Policy Rule Reference

Field - OS User

Specifies the Original OpID filter.

Wildcards supported: yes

Value groups supported: yes

Excludes supported: yes, with NOT keyword (i.e. "NOT CSUSER") or "NOT" checkbox

Case sensitive: yes (most z/OS user IDs are upper case)

Blank means: No Original OpID filtering

Description: AUTHID that connects to DB2, Similar to DB User but filters on the ASC data field

ADH_ORIGINAL_OP_ID.

OS User is a stage 1 eligible filter.

DB2 threads AUTHID is often the OS User.

NAME ST A REQ ID AUTHID PLAN ASID TOKEN

00

)

IBM® InfoSphere™ Guardium®



Manage Members for Selected Group

Group Name Primary Connection USERIDs

Group Type OS User

Modify Group Type

Category

Modify Category

Group Members

Filter



NOT %STC
PDDAVI%
TSSXS%

Please select one of the following options

Create & add a new Member named

Add

Add an existing Member to Group

Add

Rename selected Member to

Update

Delete selected Member

Delete

Add Comments

Aliases...

LDAP

Back

Close this window

IBM InfoSphere Guardium S-TAP for DB2 on z/OS

Collection Policy Rule Reference

Field - Net Prtcl.

Specifies the connection type filter.

ACCEPTED VALUES	DESCRIPTION	ADH_SYSTEM_CON_TYPE value
TSO	TSO FOREGROUND AND BACKGROUND	1
CALL	DB2 CALL ATTACH	2
BATCH	DL/I BATCH	3
CICS	CICS ATTACH	4
BMP	IMS ATTACH BMP	5
MPP	IMS ATTACH MPP	6
PRIV	DB2 PRIVATE PROTOCOL	7
DRDA	DRDA PROTOCOL	8
CTL	IMS CONTROL REGION	9
TRAN	IMS TRANSACTION BMP	10
UTIL	DB2 UTILITIES	11
RRSAF	RRSAF	12

Wildcards supported: no

Value groups supported: yes

Excludes supported: yes, with NOT keyword (i.e. "NOT TSO") or "NOT" checkbox

Case sensitive: yes (most values are upper case)

Blank means: No connection type filtering

Net Prtcl is a stage 0 eligible filter. Excluding some connection types from audit can greatly reduces overhead.



IBM® InfoSphere™ Guardium®

Manage Members for Selected Group

Group Name DB2/Z Connection Types

Group Type NET PROTOCOL

Category

Group Members Filter  

- BATCH
- BMP
- CALL
- CICS
- CTL
- DRDA
- MPP
- PRIV
- RRSAF
- TRAN
- TSO
- UTIL

Please select one of the following options

Create & add a new Member named

Add an existing Member to Group

Rename selected Member to

Delete selected Member

[Close this window](#)

IBM InfoSphere Guardium S-TAP for DB2 on z/OS Collection Policy Rule Reference

Field - App. User

Specifies the plan and/or program filter(s). This field requires the use of PLAN and/or PROG labels to denote which filter the values applies.

It is in the format of "PLAN=x; PROG=z". In this example "PLAN" and "PROG" are labels and "x" and "z" are values.

Wildcards supported: yes

Value groups supported: yes

Excludes supported: yes, with NOT keyword (i.e. PLAN=NOT x; PROG=NOT y) or "NOT" checkbox

Case sensitive: Labels are not case-sensitive. Values are case-sensitive. (most values are upper case)

Blank means: No plan/program filtering

Additional examples:

Example 1: PLAN=XXXPLAN1; PLAN=XXXPLAN2; PLAN=XXXPLAN3

Example 2: PROG=XXXPRG1; PROG=XXXPRG2; PROG=XXXPRG3

Example 3: PLAN=XXXPLAN1

Example 4: PROG=XXXPRG1

Note: Multiple values can be specified by either:

- semicolon-delimited values (as in Examples 1 & 2), or
- single entries in values groups (as in Examples 3 & 4)

Plan value is a stage 0 eligible filter. Excluding some plans from audit can reduce overhead.

IBM® InfoSphere™ Guardium®

Manage Members for Selected Group ?

Group Name Copy of DB2/Z Exclude Plan Example

Group Type APPLICATION USER

Modify Group Type

Category

Modify Category

Group Members

Filter

PLAN = DSN%
PLAN = NOT DSNREXX
PROG = NOT XX1100

Please select one of the following options

Create & add a new Member named

Add

Rename selected Member to

Update

Delete selected Member

Delete

Add Comments

Aliases...

LDAP

Back

[Close this window](#)

IBM InfoSphere Guardium S-TAP for DB2 on z/OS Collection Policy Rule Reference

Field - Client Info

Specifies any or all of the workstation fields (wsuser, wsname, wstran). This field requires the use of USER, WKSTN, and/or APPL labels to denote which filter the values applies. The format is "USER=x; WKSTN=y; APPL=z". In this example "USER", "WKSTN", and "APPL" are labels and "x", "y", and "z" are values.

Wildcards supported: yes

Value groups supported: yes

Excludes supported: yes, with NOT keyword (i.e. USER=NOT x; WKSTN=NOT y; APPL=NOT z) or "NOT" checkbox

Case sensitive: Labels are not case-sensitive. Values are case-sensitive. (most WS values are lower case)

Blank means: No workstation filtering

Additional examples:

Example 1: USER=usera; USER=userb; USER=userc

Example 2: WKSTN=ws001; WKSTN=ws002; WKSTN=ws003

Example 3: USER=usera;

Example 4: APPL=appl001;

Note: Multiple values can be specified by either:

- semicolon-delimited values (as in Examples 1 & 2), or
- single entries in values groups (as in Examples 3 & 4)

WKSTN and APPL values are stage 1 eligible filters.

IBM® InfoSphere™ Guardium®

Manage Members for Selected Group

Group Name DB2/Z Exclude Workstation Example

Group Type Client Info

Category

Modify Category

Group Members

Filter

APPL = db2jcc_application
USER = NOT pddavia
USER = pddavi%
WKSTN = us-l-db01

Please select one of the following options

Create & add a new Member named

Add

Rename selected Member to

Update

Delete selected Member

Delete

Reset to Predefined

Add Comments

Aliases...

LDAP

Back

Close this window

IBM InfoSphere Guardium S-TAP for DB2 on z/OS Collection Policy Rule Reference

Field - Object

All Rules in policy must have a value in this field or group (%%.% or greater restriction).

Specifies the DB2 table filters. This field requires the use of 2-part syntax in the form of "read/schema.table". The first part of the syntax ("read" in the example) specifies the context--reads, changes, or both (%) will be collected for the specified table. A slash separates the two parts. The second part of syntax is schema.table name.

Wildcards supported: yes

Value groups supported: yes

Excludes supported: no

Blank is invalid for Object: If no table filtering is desired a value of %/.% should be specified.

Case sensitive: Context is not case-sensitive. Values are case-sensitive. (Most values in DB2 are upper case)

Additional examples:

Example 1: read/SCHEMA.%

Example 2: change/%.CUSTOMER

Example 3: read/SCHEMA.%; change/%.CUSTOMER

Example 4: %/.%

Note: Multiple values can be specified by either:

- semicolon-delimited values (as in Examples 3), or
- single entries in values groups (as in the other examples)

%%.% - value is used to audit all tables (read/update). The value %/.% makes policy eligible for stage 0 or stage 1 filtering. Explicit values like %/CUSTOMER.CREDIT will cause Stage 2 filtering.

IBM® InfoSphere™ Guardium®

Manage Members for Selected Group



Group Name Cardholder Objects

Group Type OBJECTS

Category

Modify Category

Group Members

Filter



%/CUSTOMER.A%
change/CUSTOMER.CREDIT
read/CARD.ADDRESS

Please select one of the following options

Create & add a new Member named

Add

Rename selected Member to

Update

Delete selected Member

Delete

Reset to Predefined

Add Comments

Aliases...

LDAP

Back

[Close this window](#)

IBM InfoSphere Guardium S-TAP for DB2 on z/OS Collection Policy Rule Reference

Command

Specifies the "General" (IFI) audit types to be collected

Accepted values:

- Grant and Revokes
- DB2 Commands
- IBM DB2 Utilities
- All Failed Authorizations
- Set Current SQLID
- Failed AuthId Changes

Wildcards supported: no

Value groups supported: yes

Excludes supported: no

Case sensitive: no

Blank means: No general audit types will be collected

IBM® InfoSphere™ Guardium®

Manage Members for Selected Group

Group Name DB2/Z General Audit Types

Group Type COMMANDS

Category

Group Members

Filter



All Failed Authorizations
DB2 Commands
Failed AuthId Changes
Grant and Revokes
IBM DB2 Utilities
Set Current Sqlid

Please select one of the following options

Create & add a new Member named

Rename selected Member to

Delete selected Member

Close this window

IBM InfoSphere Guardium S-TAP for DB2 on z/OS Collection Policy Rule Reference

ACTIONS

ACTIONS does NOT have an effect on S-TAP for DB2 on z/OS collection/filtering process on the z/OS platform.

Actions has no effect at all in a DB2 Collection Profile rule!!!

ACTIONS is a required field for policy rule syntax, any value is acceptable.

Setting up a policy with only DB2 Collection Profile rules will cause the Guardium Collector to perform the exact same actions with the packets received as a blank Policy. In other words the Guardium Collector will perform the default action of simple logging of all activity (no full details).

It is essential to recognize that "xxx Collection Profile" rules only act on the z/OS S-TAP and non "xxx Collection Profile" only act on the Guardium Collector.

In order to have filtering and ACTIONS applied on traffic at Guardium Appliance that comes from S-TAP you need to have separate policy or rule without "DB2 (IMS/VSAM) COLLECTION PROFILE " as DB TYPE.

IBM InfoSphere Guardium S-TAP for DB2 on z/OS

Collection Policy Rule Reference

Key Performance Considerations

The S-TAP is responsible for gathering the DB2 SQL requests and filtering those requests against policies that have been established by the S-TAP administrator. If the policy matches the content of the SQL, it is passed to the Guardium appliance for processing, collection, analysis and reporting. Great effort has been made to offload as much processing as possible to the appliance from the S-TAP to reduce the overhead incurred on the mainframe. The functions that are performed by the S-TAP and which contribute to the performance overhead are:

Data Gathering:

As an SQL statement is processed by DB2, the S-TAP ASC intercept captures the SQL and a variety of additional fields to characterize the event for downstream processing. It is important to consider that all SQL statements must be minimally inspected by the S-TAP to see if they are events that are of interest (i.e. are part of the collection profile as defined by the administrator). Thus, even if the requirement is to capture very few events for downstream processing (e.g. only SQL from a single user), all SQL processed by DB2 will need to be minimally inspected to be able to identify those SQL events of interest (those of that user). The performance overhead of the data gathering is therefore correlated to the rate of all SQL that passes through DB2. For this reason, many optimizations have been made to ensure that the overhead per request of this phase is kept very low, and flexibility is provided to manage the overhead through the design of the collection profiles and the resulting filtering of the events.

Data Filtering:

Once an SQL event is gathered by the S-TAP intercept, it needs to be inspected and filtered against the configuration policies that have been established in the collection profiles. Only those events of interest will be sent on -TAP will perform
filtering very efficiently in the DB2 address space at the point of inspection, using S-TAP stage 0 and/or stage 1 compiled filtering, whenever possible.

Stage 0 filtering is the most basic and efficient form of filtering where the user can filter based on connection type or plan. This filtering is done in the DB2 address space at the point of inspection. This is most commonly used to filter out

filtering on connection type or plan a vast majority of events can be filtered out of further evaluation thus limiting the overhead of any further downstream evaluation and collection.

Stage 1 filtering is by userid. This filtering is done in the DB2 address space at the point of inspection. The most common use of stage 1 filtering is to limit collection to only privileged users.

Any filtering that cannot be done by a stage 0 or stage 1 filters is performed in a stage 2 filter in the S-TAP address space outside of DB2. Examples of stage 2 filters are those that operate on an object (such as a table). An event that cannot be completely evaluated at stage 0 or stage 1 will need to be moved from the DB2 address space to the S-TAP address space for stage 2 evaluation.

To minimize overall overhead on the LPAR, the filtering policies should, whenever possible, be targeted at use of stage 0 and stage 1 filtering criteria. Stage 0 and stage 1 filters are performed in the intercept running in the DB2 address space, so stage 0 and stage 1 filtering will be charged as in-DB2 processing.

The conditions to allow an event to be handled by stage 0 filtering:

- A PLAN or CONNTYPE filter value is provided (APP.USER, PLAN= or NET PRCL)
- The same PLAN or CONNTYPE filter value is in every rule
- Stage1 filtering is enabled To enable, ASC configuration parm STAGE1_FILTER(Y) is required.

IBM InfoSphere Guardium S-TAP for DB2 on z/OS Collection Policy Rule Reference

The conditions to allow an event to be handled by stage 1 filtering:

- The following fields would be identified as filtering criteria. These fields may be fully or partially qualified (wild carded). At least one of these fields must be specified for the rule to be eligible for Stage 1 filtering. However, if all of the Stage 1 fields specified in the rule only contain the wildcard character, then the rule is not eligible for Stage 1 filtering.

Plan Name	(APP.USER, PLAN=)
Primary AUTHID	(OS USER)
Current SQLID	(DB USER)
WSNAME	(CLIENT INFO, WKSTN=)
WSTRAN	(CLIENT INFO, APPL=)

The conditions to allow an event to be handled by stage 2 filtering:

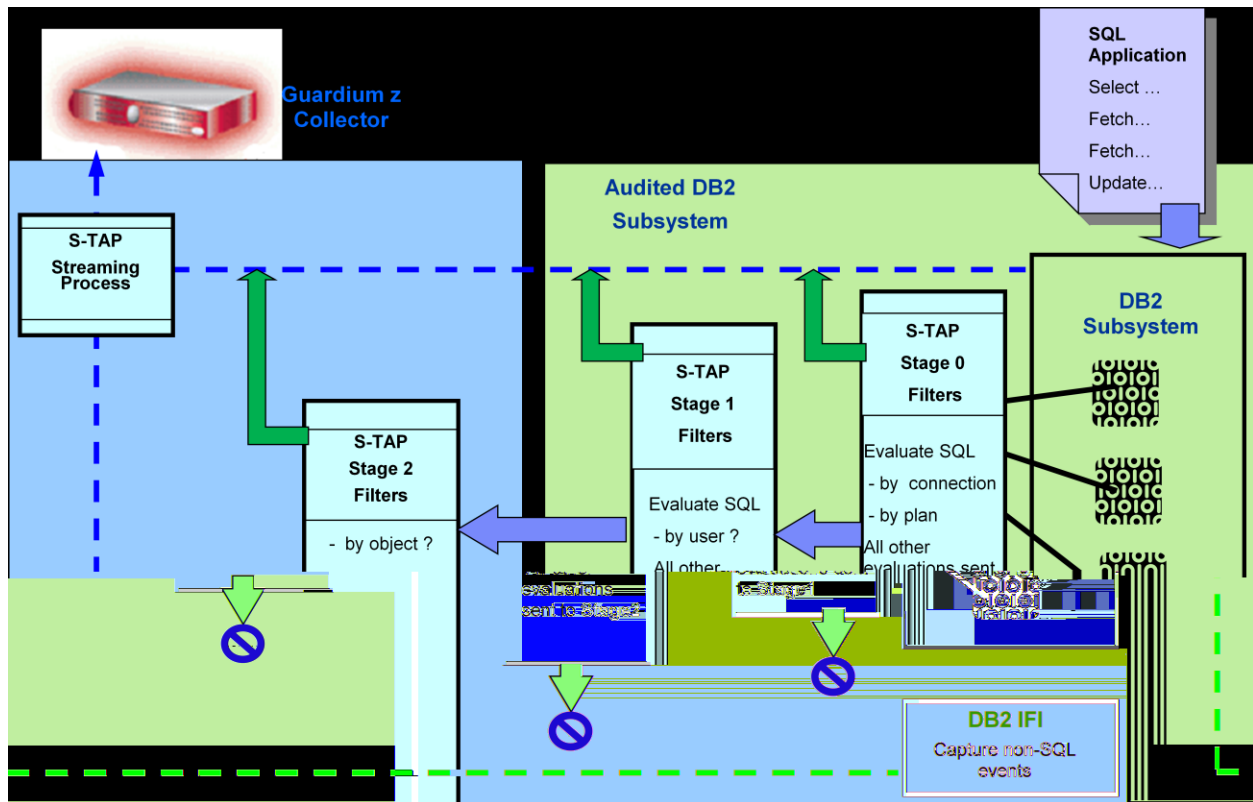
- Stage 2 filtering is required for any other fields, and for objects. If all rules in the active collection profile are able to be filtered in Stage 0 or 1, then no Stage 2 filtering will occur. This will result in CPU reduction for the collection and filtering process.

Further discussion of how to configure the filtering effects of the collection profiles is available in the Guardium S-TAP product documentation.

IBM InfoSphere Guardium S-TAP for DB2 on z/OS Collection Policy Rule Reference

Data Movement

As the events are gathered and filtered, if any events have not been handled by Stage 0 or Stage 1 they will need to be moved out of the DB2 address space to the S-TAP address space. This involves a memory move from the DB2 address space, to memory that can be addressed by the S-TAP address space. One benefit of stage 0/1 filtering is the reduction in the number of events that might qualify to move to the S-TAP address space and the resulting reduction in memory moves of the data. In the worst case, with no stage 0/1 filtering, all the captured events will need to be moved in memory. Once available to the the S-TAP address space, stage 2 filtering will be applied where necessary and the resulting events are streamed to the Guardium collector over TCP/IP. If the filtering is extensive, potentially few events will be streamed, limiting the overhead of the TCP/IP transfers. Note that if there is no filtering (stage 0/1 nor stage 2), the effect is to stream all the events processed through DB2 over the network to the Guardium collector. This can result in significant TCP/IP processing and resulting CPU overhead. Stage 2 filtering cost and preparing the data for streaming will be borne by the S-TAP task (not DB2). Note that stage 2 filtering is eligible for zIIP processing should a zIIP processor be available and have capacity to have this work dispatched to the zIIP subject to the workload manager policies. TCP/IP cost to do the transfer is borne by the TCP/IP task.



IBM InfoSphere Guardium S-TAP for DB2 on z/OS Collection Policy Rule Reference

express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to

IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole