



IBM Security Guardium Data Protection Usage and Reporting

Version 12.0

PURPOSE	2
GUARDIUM DATA PROTECTION PARTS	2
PID 5725-I12 - IBM Security Guardium Data Security and Compliance - IBM Security Guardium Data Protection	3
IBM Security Guardium Data Protection	11
CC - IBM Security Guardium Data Protection for Databases	11
CC - IBM Security Guardium Data Protection for Data Warehouses	11
CC- IBM Security Guardium Data Protection for Big Data	11
CC- IBM Security Guardium Data Protection for SAP HANA	11
CC- IBM Security Guardium Data Protection for Database Services	11
CC - IBM Security Guardium Data Protection for Data Warehouses	15
CC- IBM Security Guardium Data Protection for Big Data	16
CC- IBM Security Guardium Data Protection for SAP HANA	16
CC- IBM Security Guardium Data Protection for Database Services	16
CC - IBM Security Guardium Vulnerability Assessment for Databases	17
PID 5725-V56 - IBM Security Guardium for Files - IBM Security Guardium Data Protection for Files	17
cc - IBM Security Guardium Data Protection for Files	17
PID 5737-H31- IBM Security Guardium for SharePoint - IBM Security Guardium Data Protection for SharePoint	20
cc - IBM Security Guardium Data Protection for SharePoint	20
PID 5737-H30- IBM Security Guardium for NAS - IBM Security Guardium Data Protection for NAS	22
cc - IBM Security Guardium Data Protection for NAS	22
PID 5725-I12 - IBM Security Guardium Data Security and Compliance - IBM Security Guardium Database Vulnerability Assessment Solution	24
CC - IBM Security Guardium Vulnerability Assessment for Databases	24
PID 5725-I12 - IBM Security Guardium Data Security and Compliance - IBM Security Guardium Database Activity Monitor Group	24

Standard Data Activity Monitoring:	24
CC - IBM Security Guardium Standard Activity Monitor for Databases	24
CC - IBM Security Guardium Standard Activity Monitor for Data Warehouses	24
CC- IBM Security Guardium Standard Activity Monitor for Big Data	24
CC - IBM Security Guardium Standard Activity Monitor for Data Warehouses	26
CC- IBM Security Guardium Standard Activity Monitor for Big Data	26
Advanced Data Activity Monitoring:	27
CC- IBM Security Guardium Advanced Activity Monitor for Databases	27
CC- IBM Security Guardium Advanced Activity Monitor for Data Warehouses	27
CC- IBM Security Guardium Advanced Activity Monitor for BigData	27
CC- IBM Security Guardium Advanced Activity Monitor for Databases	27
CC- IBM Security Guardium Advanced Activity Monitor for Data Warehouses	27
CC- IBM Security Guardium Advanced Activity Monitor for BigData	27
PID 5725-V56 - IBM Security Guardium for Files - IBM Security Guardium Activity Monitor for Files	
Group	28
cc - IBM Security Guardium Standard Activity Monitor for Files	28
CC- IBM Security Guardium Advanced Activity Monitor for Files	29
PID 5725-I12 - IBM Security Guardium Data Security and Compliance - IBM Security Guardium	
Central Management and Aggregation Group	29
CC - IBM Security Guardium Central Management and Aggregation for Databases Pack	29
CC - IBM Security Guardium Central Management and Aggregation for Data Warehouses Pack	30
CC - IBM Security Guardium Central Management and Aggregation for Big Data Pack	30

Purpose

This document is intended to help Guardium administrators and users to understand and report usage of Guardium Data Protection instead of using the IBM License Metric Tool (ILMT). It provides an overview of how to map Server IPs within IBM Security Guardium Data Protection v12.0

Guardium Data Protection Parts

The following provides an index of the various PIDs associated with IBM Security Guardium Data Protection v12.0 and how to get the Server IP list for each Guardium chargeable component (CC).

PID 5725-I12 - IBM Security Cloud Pak for Security (CP4S) Guardium Domain Package

The following chargeable components can be classified as belonging to an activity monitoring group that possesses identical criteria for mapping server IPs.

IBM Security Cloud Pak for Security (CP4S) Guardium Domain Package

CC - IBM Security Cloud Pak for Security (CP4S) Guardium Domain Package

Under CP4S Guardium Domain Package, the CC are related

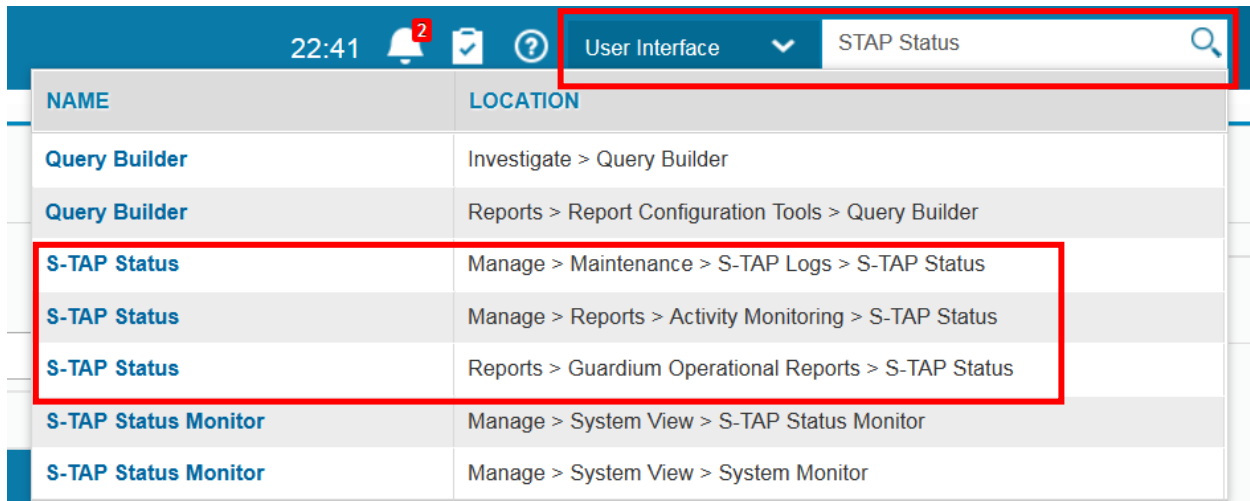
Capabilities	Enterprise-wide pricing:	Usage based pricing:
Single Resource Unit part - D0A2GZX		
Data Protection	1 MVS : 360 RU	1 VPC : 36 RU
Vulnerability Assessment	1 MVS : 40 RU	1 VPC : 4 RU
Guardium Insights	1 MVS : 100 RU	1 VPC : 10 RU

How to map

The IBM Security Guardium Data Protection auditing activity can be mapped to:

1. IBM Security Guardium Data Protection monitors activity using S-TAP. The S-TAP Status report, accessed through **Quick Search Dialog using search string “S-TAP Status”** in *User Interface Search box*, which shows the S-TAP Host (server IP) that the IBM Security Guardium Data Protection Activity Monitor is monitoring.

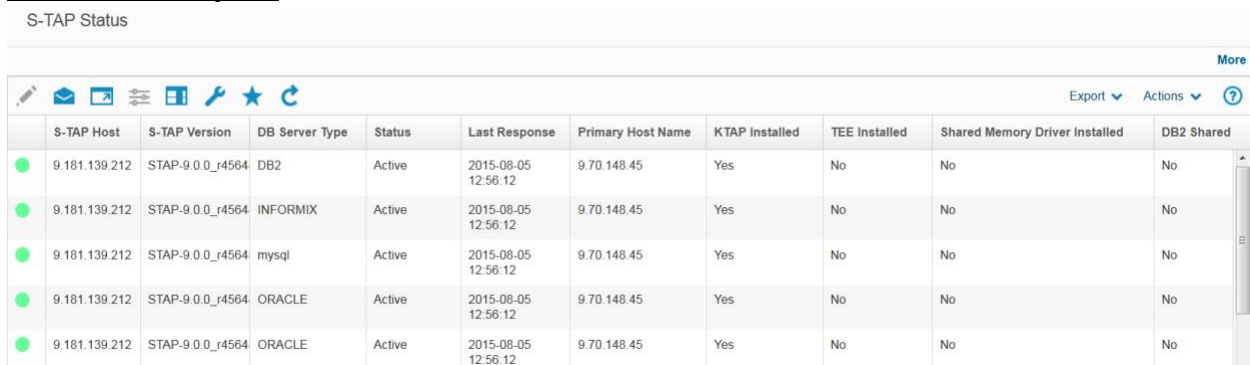
Search “STAP Status” :



The screenshot shows the top navigation bar of the application. The time is 22:41. There are icons for notifications (2), a checklist, and a help icon. The 'User Interface' dropdown menu is open, and the search bar contains the text 'STAP Status'. Below the search bar, a table of results is displayed. The table has two columns: 'NAME' and 'LOCATION'. The results are as follows:

NAME	LOCATION
Query Builder	Investigate > Query Builder
Query Builder	Reports > Report Configuration Tools > Query Builder
S-TAP Status	Manage > Maintenance > S-TAP Logs > S-TAP Status
S-TAP Status	Manage > Reports > Activity Monitoring > S-TAP Status
S-TAP Status	Reports > Guardium Operational Reports > S-TAP Status
S-TAP Status Monitor	Manage > System View > S-TAP Status Monitor
S-TAP Status Monitor	Manage > System View > System Monitor

STAP Status report :



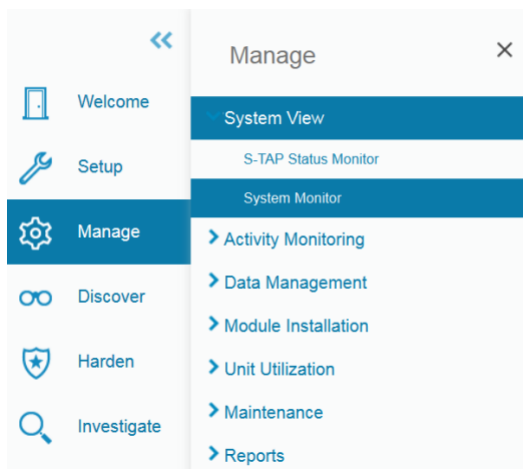
The screenshot shows the 'S-TAP Status' report. The table has 11 columns: S-TAP Host, S-TAP Version, DB Server Type, Status, Last Response, Primary Host Name, KTAP Installed, TEE Installed, Shared Memory Driver Installed, and DB2 Shared. There are 5 rows of data, all showing 'Active' status.

S-TAP Host	S-TAP Version	DB Server Type	Status	Last Response	Primary Host Name	KTAP Installed	TEE Installed	Shared Memory Driver Installed	DB2 Shared
9.181.139.212	STAP-9.0.0_r4564	DB2	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No
9.181.139.212	STAP-9.0.0_r4564	INFORMIX	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No
9.181.139.212	STAP-9.0.0_r4564	mysql	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No
9.181.139.212	STAP-9.0.0_r4564	ORACLE	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No
9.181.139.212	STAP-9.0.0_r4564	ORACLE	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No

2. If not using S-TAP, but instead using network inspection you can go to the console inspection engines and see the Server IPs being monitored.

Access by going to:

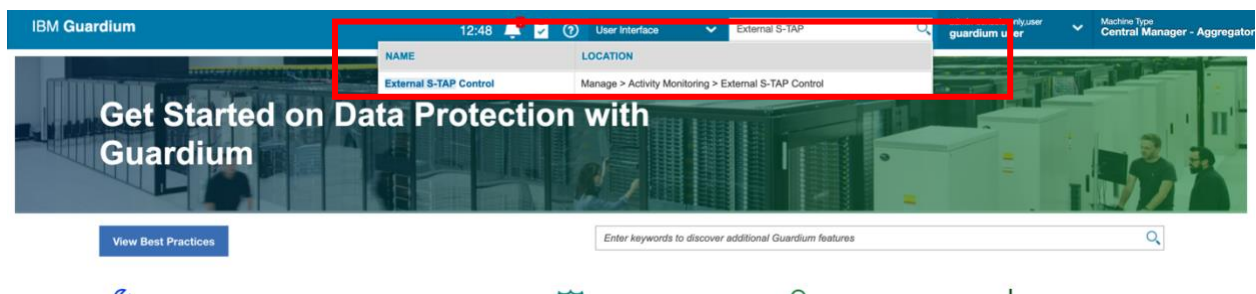
Manage -> System View -> System Monitor → Inspection Engine.



Slide down to look for Inspection Engine view

Inspection Engines			
S-TAP Host Name	DB Server Types	Count	
9.181.139.212	DB2	1	
9.181.139.212	INFORMIX	1	
9.181.139.212	mysql	1	
9.181.139.212	ORACLE	3	
9.181.139.212	PGSQL	1	
9.181.139.212	sybase	1	
Total: 41			

- If you are using External S-TAP, the External S-TAP Status report can be accessed through **Quick Search Dialog** using search string **“External S-TAP Control”** in *User Interface Search box*. This report shows the External S-TAP Host that the IBM Security Guardium Data Protection Activity Monitor is monitoring.



External S-TAP Control

4. If you are using the Cloud Provider APIs (AWS Database Activity Stream or Azure Event Hubs), the status report is accessed through **Quick Search Dialog using search string “Cloud DB Service Protection”** in the *User Interface Search box*, which shows the stream that the IBM Security Guardium Data Protection Activity Monitor is monitoring. The stream is mapped to the cloud data source that is being monitored

IBM Guardium

13:27

User Interface

cloud DB Service Protection

admin admin

Machine Type Central Manager - Aggregat

NAME

LOCATION

Cloud DB Service Protection

Discover > Database Discovery > Cloud DB Service Protection

Get Started on Data Protection with Guardium

View Best Practices

Enter keywords to discover additional Guardium features

Cloud DB Service Protection

Cloud DB Service Accounts

Amazon-D8

Provider: Amazon

Hide Discover Streams

Amazon Region

Endpoint

us-gov-west-1

kinesis.us-gov-west-1.amazonaws.com

us-east-1

kinesis.us-east-1.amazonaws.com

us-east-2

kinesis.us-east-2.amazonaws.com

us-west-1

kinesis.us-west-1.amazonaws.com

us-west-2

kinesis.us-west-2.amazonaws.com

Discover

Streams

Stream

Region

Assigned collectors

Monitor enabled

Status

Status changed

Comments

aws-rds-das-cluster-RG53AM076NBUFGQIN8N4BOZ7I

us-east-2

1

☒

●

2020-04-27 16:01:37

All Good

- If you are using the Cloud Native Logs (Universal Connector plugins), the status report is accessed through **Quick Search Dialog using search string “Cloud DB Service Protection” in User Interface Search box**, which shows the host that the IBM Security Guardium Data Protection Activity Monitor is monitoring.

Instance	Database Engine	Region	Guardium Datasource	Datasource User	Classification Process	Vulnerability Assessment	Active Collector	DB Audit Owner (CM env.)	DB Auditing	Objects
spoomam-oracle11	oracle-ee 11.2.0.4.v23	us-east-1	spoomam-oracle11:1521	spoomam	GDPR 2020-05-25 14:05:59.0		sys-vm21.guardsys.com	sys-vm01	Enabled, pending restart	
spoomam-oracle12	oracle-ee 12.1.0.2.v19	us-east-1	spoomam-oracle12:1521	spoomam	GDPR 2020-05-25 14:05:59.0		sys-vm22.guardsys.com	sys-vm01	Enabled	

Note:

[CC - IBM Security Guardium Data Protection for Databases](#)

Access reports, such as the **Data-Sources**, accessed by going to **Reports -> Report Configuration Tools -> Data-Sources**, can be used to show a listing of the server IPs for the database servers seen during a reporting period. This CC is charged based on the RVU (Resource Value Units) based on MVS (Managed Virtual Server) on the hosts being monitored, either by STAP, External S-TAP, Native Logs or Network monitoring.

[CC - IBM Security Guardium Data Protection for Data Warehouses](#)

Access reports, such as the **Data-Sources**, accessed by going to **Reports -> Report Configuration Tools -> Data-Sources**, can be used to show a listing of the server IPs for the data warehouse servers seen during a reporting period. This CC is charged based on the RVU (Resource Value Units) based on MVS (Managed Virtual Server) of the data warehouse hosts being monitored, either by STAP, External S-TAP, Native Logs or Network monitoring.

CC- IBM Security Guardium Data Protection for Big Data

Access reports, such as the **Data-Sources**, accessed by going to **Reports -> Report Configuration Tools -> Data-Sources**, can be used to show a listing of the server IPs for the Big Data servers seen during a reporting period. This CC is charged based on the RVU (Resource Value Units) based on Managed Virtual Servers (MVS) or nodes of the Big Data environment being monitored, either by STAP, External S-TAP, Native Logs or Network monitoring.

CC- IBM Security Guardium Data Protection for SAP HANA

Access reports, such as the **Data-Sources**, accessed by going to **Reports -> Report Configuration Tools -> Data-Sources**, can be used to show a listing of the server IPs for the SAP HANA servers seen during a reporting period. This CC is charged based on the RVU (Resource Value Units) based on Managed Activated Processor Cores (MAPC) of the SAP HANA environment being monitored, either by STAP, External S-TAP, Native Logs or Network monitoring.

CC- IBM Security Guardium Data Protection for Database Services

Access reports, such as the **Data-Sources**, accessed by going to **Reports -> Report Configuration Tools -> Data-Sources**, can be used to show a listing of the server IPs for the Database Services seen during a reporting period. This CC is charged based on the RVU (Resource Value Units) based on Managed Activated Processor Cores (MAPC) of the Cloud data source environment being monitored, either by External S-TAP, Native Logs or Cloud Provider APIs.

Note:

Except for the Database Services listed below, the MAPC entitlements for Database Services are calculated by converting standard compute metrics such as VPC or vCPU or Core at a ratio of 1 to 1.

For the following list of Database Services, the MAPC entitlements are calculated by converting as described below:

For AWS DynamoDB, 1 DynamoDB account or instance : 10 MAPC 100 Capacity Units (CUs) : 10 MAPC

For AWS S3, 1 S3 Bucket : 10 MAPC

For Azure Database Transaction Unit, 1 DTU : 1 MAPC

For Azure Datawarehouse Unit, 10 DWU: 1 MAPC

For Google Cloud BigQuery, 10 slots : 1 MAPC

For Google Cloud Spanner, 1 node: 10 MAPC

For Oracle Cloud, 1 OCPU : 2 MAPC

For Snowflake, 2 large nodes: 10 MAPC

4 medium nodes: 10 MAPC

8 small nodes: 10 MAPC

For Blocking:

IBM Security Guardium Data Protection for Databases, Data Warehouse, BigData, SAP HANA and Express Database Protection Activity Monitor package includes blocking capabilities and monitors and enforces data protection using an S-GATE instead of an STAP. To find if a policy has been configured to use S-GATE, you can look at the policy rules and their actions by going to **Protect -> Policy Builder for Data-> Selecting the Policy -> Edit Rules** and then expanding the individual rules to see if **S-GATE** is part of the Actions defined. If S-GATE rules are in use then the list of server IPs would then be one of the following:

- If the S-GATE Policy Rules include specific Server IPs (or a group of IPs) or hostnames – then these IPs and hostnames are in scope
- If the S-GATE Policy Rules have ‘ANY’ for Server IPs or hostnames – use the Server IPs or hostnames are defined for the IBM Security Guardium Database Activity Monitor group (see above).

Note: IBM Security Guardium Data Protection for Database, Data Warehouse, BigData, SAP HANA, Database Services entitlements *include* Central Management and Aggregation Pack

IBM Security Guardium provides the ability for central management, aggregation of data and reports, and Compliance Workflow Automation, to streamline the compliance workflow process by consolidating the database activity that is uploaded to the appliance from the customer’s environment. The Data Protection package includes central management and aggregation licenses.

CC - [IBM Security Guardium Vulnerability Assessment for Databases](#)

How to map

1. The list of data sources defined under **Harden -> Vulnerability Assessment → Datasource Definitions** will provide the database server IPs being used. (Note: when datasource presents just the hostname, you’d need to click the ‘Modify’ button to see its IP address for)
2. The configuration, as seen through **Harden -> Reports -> CAS Configuration**

- **CAS Instances & CAS Instance Config** , will display the list of server IPs.

Note: IBM Security Guardium Data Protection for SAP HANA entitlements *include* Vulnerability Assessment for SAP HANA

IBM Security Guardium includes the ability to run vulnerability assessment scans for SAP HANA environment.

PID 5725-I12 - IBM Security Guardium Data Security and Compliance - IBM Security Guardium Data Protection

The following chargeable components can be classified as belonging to an activity monitoring group that possesses identical criteria for mapping server IPs.

IBM Security Guardium Data Protection

CC - **IBM Security Guardium Data Protection for Databases**

CC - **IBM Security Guardium Data Protection for Data Warehouses**

CC- **IBM Security Guardium Data Protection for Big Data**

CC- **IBM Security Guardium Data Protection for SAP HANA**





CC- **IBM Security Guardium Data Protection for Database Services**

How to map

The IBM Security Guardium Data Protection auditing activity can be mapped to:


6. IBM Security Guardium Data Protection monitors activity using S-TAP. The S-TAP Status report, accessed through **Quick Search Dialog using search string “S-TAP Status”** in *User Interface Search box*, which shows the S-TAP Host (server IP) that the IBM Security Guardium Data Protection Activity Monitor is monitoring.


Search “STAP Status” :


22:41   		User Interface	STAP Status 
NAME	LOCATION		
Query Builder	Investigate > Query Builder		
Query Builder	Reports > Report Configuration Tools > Query Builder		
S-TAP Status	Manage > Maintenance > S-TAP Logs > S-TAP Status		
S-TAP Status	Manage > Reports > Activity Monitoring > S-TAP Status		
S-TAP Status	Reports > Guardium Operational Reports > S-TAP Status		
S-TAP Status Monitor	Manage > System View > S-TAP Status Monitor		
S-TAP Status Monitor	Manage > System View > System Monitor		


STAP Status report :


S-TAP Status


























Export

Actions

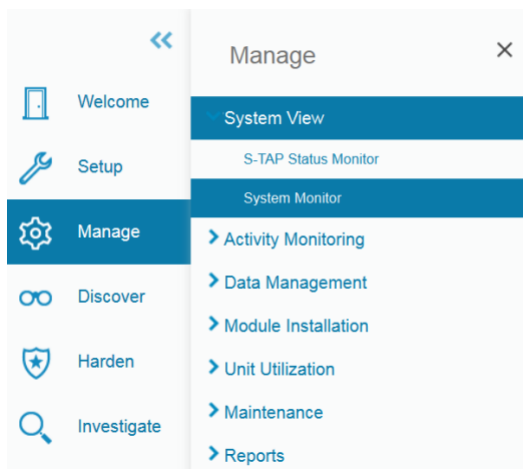


	S-TAP Host	S-TAP Version	DB Server Type	Status	Last Response	Primary Host Name	KTAP Installed	TEE Installed	Shared Memory Driver Installed	DB2 Shared
	9.181.139.212	STAP-9.0.0_r4564	DB2	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No
	9.181.139.212	STAP-9.0.0_r4564	INFORMIX	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No
	9.181.139.212	STAP-9.0.0_r4564	mysql	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No
	9.181.139.212	STAP-9.0.0_r4564	ORACLE	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No
	9.181.139.212	STAP-9.0.0_r4564	ORACLE	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No

7. If not using S-TAP, but instead using network inspection you can go to the console inspection engines and see the Server IPs being monitored.

Access by going to:

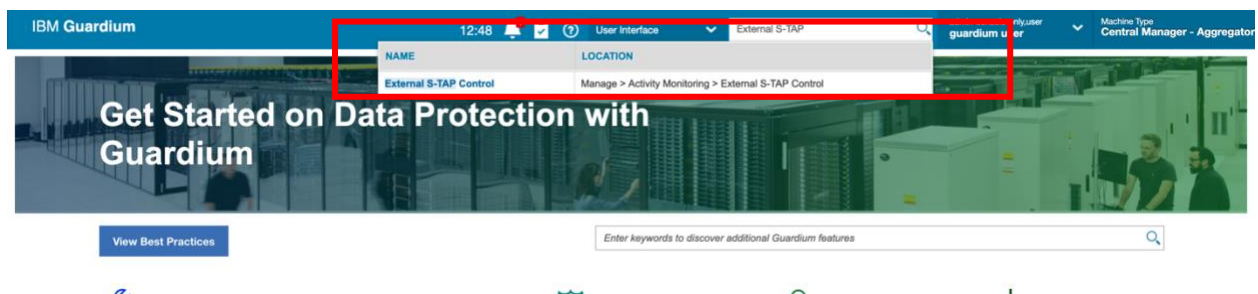
Manage -> System View -> System Monitor → Inspection Engine.



Slide down to look for Inspection Engine view

Inspection Engines			
S-TAP Host Name	DB Server Types	Count	
9.181.139.212	DB2	1	
9.181.139.212	INFORMIX	1	
9.181.139.212	mysql	1	
9.181.139.212	ORACLE	3	
9.181.139.212	PGSQL	1	
9.181.139.212	sybase	1	
Total: 41			

- If you are using External S-TAP, the External S-TAP Status report can be accessed through **Quick Search Dialog** using search string **“External S-TAP Control”** in *User Interface Search box*. This report shows the External S-TAP Host that the IBM Security Guardium Data Protection Activity Monitor is monitoring.



External S-TAP Control

External S-TAP group	Group uid	Host	Database type	Total members	Overall status	Healthy members	Collector
db2_9.70.164.122	cb9d2e3d-d1ad-4db0-9283-85af6451c470	9.70.164.122	db2	2	●	2	lit4-vm02.guard.swg.usma.ibm.com
mysql_9.70.164.122	d364f6f5-e553-4669-9cce-c2b55b95c82	9.70.164.122	mysql	2	●	2	lit4-vm02.guard.swg.usma.ibm.com
mongodb_9.70.164.122	84339197-d7ed-48a8-930d-1a3c0a2b9df5	9.70.164.122	mongodb	2	●	2	lit4-vm02.guard.swg.usma.ibm.com
redis_9.70.164.122	72ec2f5a-19ea-496c-a86e-fd1d540d426	9.70.164.122	redis	2	●	2	lit4-vm02.guard.swg.usma.ibm.com

Total: 5 Selected: 1

9. If you are using the Cloud Provider APIs (AWS Database Activity Stream or Azure Event Hubs), the status report is accessed through **Quick Search Dialog using search string “Cloud DB Service Protection”** in the *User Interface Search box*, which shows the stream that the IBM Security Guardium Data Protection Activity Monitor is monitoring. The stream is mapped to the cloud data source that is being monitored

IBM Guardium 13:27 User Interface cloud DB Service Protection admin admin Machine Type Central Manager - Aggregat

NAME LOCATION

Cloud DB Service Protection Discover > Database Discovery > Cloud DB Service Protection

Get Started on Data Protection with Guardium

View Best Practices Enter keywords to discover additional Guardium features

Cloud DB Service Protection

Cloud DB Service Accounts

Provider: Amazon

Hide Discover Streams

Amazon Region Endpoint

us-gov-west-1 kinesys.us-gov-west-1.amazonaws.com

us-east-1 kinesys.us-east-1.amazonaws.com

us-east-2 kinesys.us-east-2.amazonaws.com

us-west-1 kinesys.us-west-1.amazonaws.com

us-west-2 kinesys.us-west-2.amazonaws.com

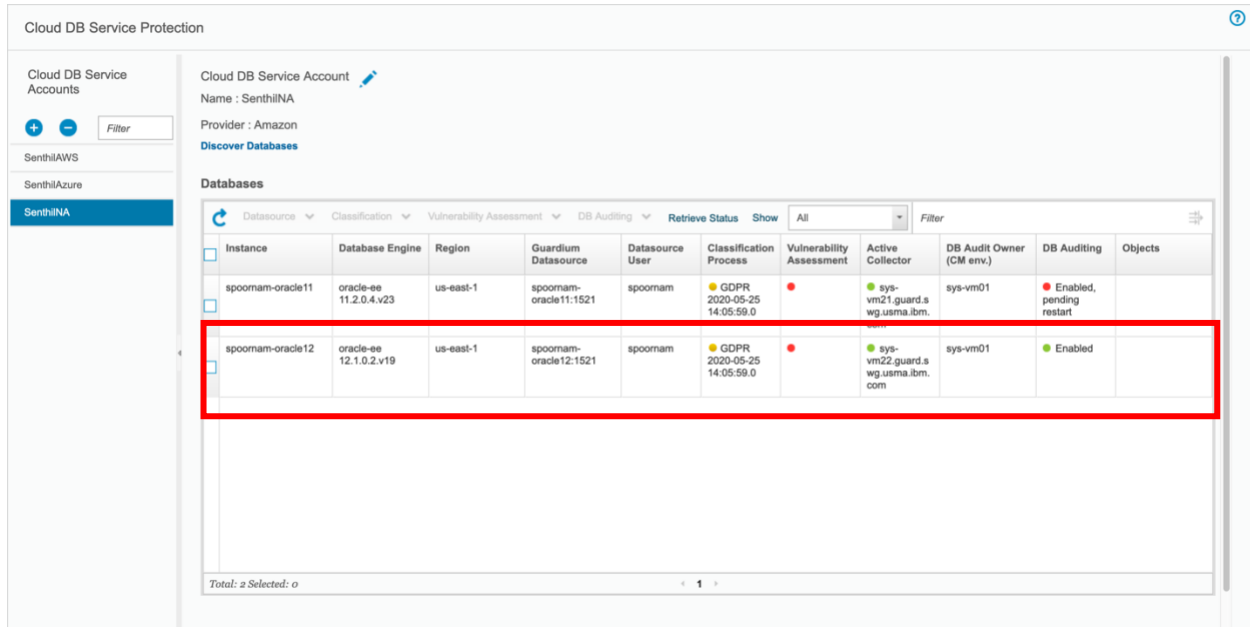
Discover

Streams

Assign Collector Enable Monitoring Disable Monitoring Status History Filter

Stream	Region	Assigned collectors	Monitor enabled	Status	Status changed	Comments
aws-rds-das-cluster-RG53AM076NBUFGQIN8N4BOZ7I	us-east-2	1	1	●		All Good
aws-rds-das-cluster-RG53AM076NBUFGQIN8N4BOZ7I	us-east-2	typ-cod6.guard.swg.usma.ibm.com	<input checked="" type="checkbox"/>	●	2020-04-27 16:01:37	All Good

10. If you are using the Cloud Native Logs (Universal Connector plugins), the status report is accessed through **Quick Search Dialog using search string “Cloud DB Service Protection” in User Interface Search box**, which shows the host that the IBM Security Guardium Data Protection Activity Monitor is monitoring.



Instance	Database Engine	Region	Guardium Datasource	Datasource User	Classification Process	Vulnerability Assessment	Active Collector	DB Audit Owner (CM env.)	DB Auditing	Objects
spoomam-oracle11	oracle-ee 11.2.0.4.v23	us-east-1	spoomam-oracle11:1521	spoomam	GDPR 2020-05-25 14:05:59.0	●	sys-vm21.guard.s wg.usma.ibm.	sys-vm01	● Enabled, pending restart	
spoomam-oracle12	oracle-ee 12.1.0.2.v19	us-east-1	spoomam-oracle12:1521	spoomam	GDPR 2020-05-25 14:05:59.0	●	sys-vm22.guard.s wg.usma.ibm. com	sys-vm01	● Enabled	

Note:

CC - IBM Security Guardium Data Protection for Databases

Access reports, such as the **Data-Sources**, accessed by going to **Reports -> Report Configuration Tools -> Data-Sources**, can be used to show a listing of the server IPs for the database servers seen during a reporting period. This CC is charged based on the RVU (Resource Value Units) based on MVS (Managed Virtual Server) on the hosts being monitored, either by STAP, External S-TAP, Native Logs or Network monitoring.

CC - IBM Security Guardium Data Protection for Data Warehouses

Access reports, such as the **Data-Sources**, accessed by going to **Reports -> Report Configuration Tools -> Data-Sources**, can be used to show a listing of the server IPs for the data warehouse servers seen during a reporting period. This CC is charged based on the RVU (Resource Value Units) based on MVS (Managed Virtual Server) of the data warehouse hosts being monitored, either by STAP, External S-TAP, Native Logs or Network monitoring.

CC- IBM Security Guardium Data Protection for Big Data

Access reports, such as the **Data-Sources**, accessed by going to **Reports -> Report Configuration Tools -> Data-Sources**, can be used to show a listing of the server IPs for the Big Data servers seen during a reporting period. This CC is charged based on the RVU (Resource Value Units) based on Managed Virtual Servers (MVS) or nodes of the Big Data environment being monitored, either by STAP, External S-TAP, Native Logs or Network monitoring.

CC- IBM Security Guardium Data Protection for SAP HANA

Access reports, such as the **Data-Sources**, accessed by going to **Reports -> Report Configuration Tools -> Data-Sources**, can be used to show a listing of the server IPs for the SAP HANA servers seen during a reporting period. This CC is charged based on the RVU (Resource Value Units) based on Managed Activated Processor Cores (MAPC) of the SAP HANA environment being monitored, either by STAP, External S-TAP, Native Logs or Network monitoring.

CC- IBM Security Guardium Data Protection for Database Services

Access reports, such as the **Data-Sources**, accessed by going to **Reports -> Report Configuration Tools -> Data-Sources**, can be used to show a listing of the server IPs for the Database Services seen during a reporting period. This CC is charged based on the RVU (Resource Value Units) based on Managed Activated Processor Cores (MAPC) of the Cloud data source environment being monitored, either by External S-TAP, Native Logs or Cloud Provider APIs.

For Blocking:

IBM Security Guardium Data Protection for Databases, Data Warehouse, BigData, SAP HANA and Express Database Protection Activity Monitor package includes blocking capabilities and monitors and enforces data protection using an S-GATE instead of an STAP. To find if a policy has been configured to use S-GATE, you can look at the policy rules and their actions by going to **Protect -> Policy Builder for Data-> Selecting the Policy -> Edit Rules** and then expanding the individual rules to see if **S-GATE** is part of the Actions defined. If S-GATE rules are in use then the list of server IPs would then be one of the following:

- If the S-GATE Policy Rules include specific Server IPs (or a group of IPs) or hostnames – then these IPs and hostnames are in scope
- If the S-GATE Policy Rules have ‘ANY’ for Server IPs or hostnames – use the Server IPs or hostnames are defined for the IBM Security Guardium Database Activity Monitor group (see above).

Note: IBM Security Guardium Data Protection for Database, Data Warehouse, BigData, SAP HANA, Database Services entitlements *include* Central Management and Aggregation Pack

IBM Security Guardium provides the ability for central management, aggregation of data and reports, and Compliance Workflow Automation, to streamline the compliance workflow process by consolidating the database activity that is uploaded to the appliance from the customer's environment. The Data Protection package includes central management and aggregation licenses.

CC - IBM Security Guardium Vulnerability Assessment for Databases

How to map

3. The list of data sources defined under **Harden -> Vulnerability Assessment -> Datasource Definitions** will provide the database server IPs being used. (Note: when datasource presents just the hostname, you'd need to click the 'Modify' button to see its IP address for)
4. The configuration, as seen through **Harden -> Reports -> CAS Configuration**
 - **CAS Instances & CAS Instance Config** , will display the list of server IPs.

Note: IBM Security Guardium Data Protection for SAP HANA entitlements *include* Vulnerability Assessment for SAP HANA

IBM Security Guardium includes the ability to run vulnerability assessment scans for SAP HANA environment.

PID 5725-V56 - IBM Security Guardium for Files - IBM Security Guardium Data Protection for Files

The following chargeable component can be classified as belonging to an activity monitoring group that possesses identical criteria for mapping server IPs.

cc - IBM Security Guardium Data Protection for Files






How to map

The IBM Security Guardium Data Protection for Files Activity Monitor auditing activity can be mapped to:

Normally the IBM Security Guardium Data Protection for Files Activity Monitor monitors activity using FS-TAP. The S-TAP Status report, accessed through **Quick Search Dialog using search string " S-TAP Status"** in *User Interface Search box*, which shows the S-TAP

Host (server IP) that the IBM Security Guardium Data Protection for Files Activity Monitor is monitoring.

Search “STAP Status” :

22:41   		User Interface 	STAP Status 
NAME	LOCATION		
Query Builder	Investigate > Query Builder		
Query Builder	Reports > Report Configuration Tools > Query Builder		
S-TAP Status	Manage > Maintenance > S-TAP Logs > S-TAP Status		
S-TAP Status	Manage > Reports > Activity Monitoring > S-TAP Status		
S-TAP Status	Reports > Guardium Operational Reports > S-TAP Status		
S-TAP Status Monitor	Manage > System View > S-TAP Status Monitor		
S-TAP Status Monitor	Manage > System View > System Monitor		

STAP Status report :

S-TAP Status

M								
Export Actions								
	S-TAP Host	S-TAP Version	DB Server Type	Status	Last Response	Primary Host Name	KTAP Installed	TEE Inst
	9.112.237.30	STAP-10.1.0_r88287_trunk_1-00000000		Active	2016-07-22 13:13:19	9.70.157.116	Yes	No
	9.112.237.30:FAM	Guardium_FSM_10.1.0r88287		Active	2016-07-22 13:13:20	9.70.157.116	No	No
	9.115.65.34	STAP-10.1.0_r88287_trunk_1-00000000		Active	2016-07-22 13:13:19	9.70.157.116	Yes	No
	9.115.71.55	STAP-10.1.0_r88657_v10_1_scmom_1-00000000		Active	2016-07-22 13:13:19	9.70.157.116	Yes	No
	9.115.71.55:FAM	Guardium_FSM_10.1.0r88657		Active	2016-07-22 13:13:20	9.70.157.116	No	No
	9.125.73.192	10.1.8.7834		Active	2016-07-22 13:13:20	9.70.157.116	No	No

For Blocking:

IBM Security Guardium Data Protection for Files monitors and enforces data protection using an STAP. To find if a policy has been configured to use STAP for blocking, you can look at the policy rules and their actions by going to **Protect -> Policy Builder for Files -> Selecting the Policy -> Edit Rules** and then expanding the individual rules to see if **Block, Log As Violation & Audit** is part of the Rule Action section.

- If the File Policy Rules include specific Server IPs (or a group of IPs) or Hostnames– then these IPs and Hostnames are in scope

Note: This CC is charged based on RVU (Resource Value Units) for MVS (Managed Virtual Server), on the hosts being monitored by STAP, or where a Data Protection for File Activity Monitoring (Discovery & Classification) is installed.

Note: IBM Security Guardium Data Protection for Files entitlements *include* Central Management and Aggregation Pack

IBM Security Guardium provides the ability for central management, aggregation of data and reports, and Compliance Workflow Automation, to streamline the compliance workflow process by consolidating the database activity that is uploaded to the appliance from the customer's environment. The Data Protection package includes central management and aggregation licenses.

PID 5737-H31- IBM Security Guardium for SharePoint - IBM Security Guardium Data Protection for SharePoint

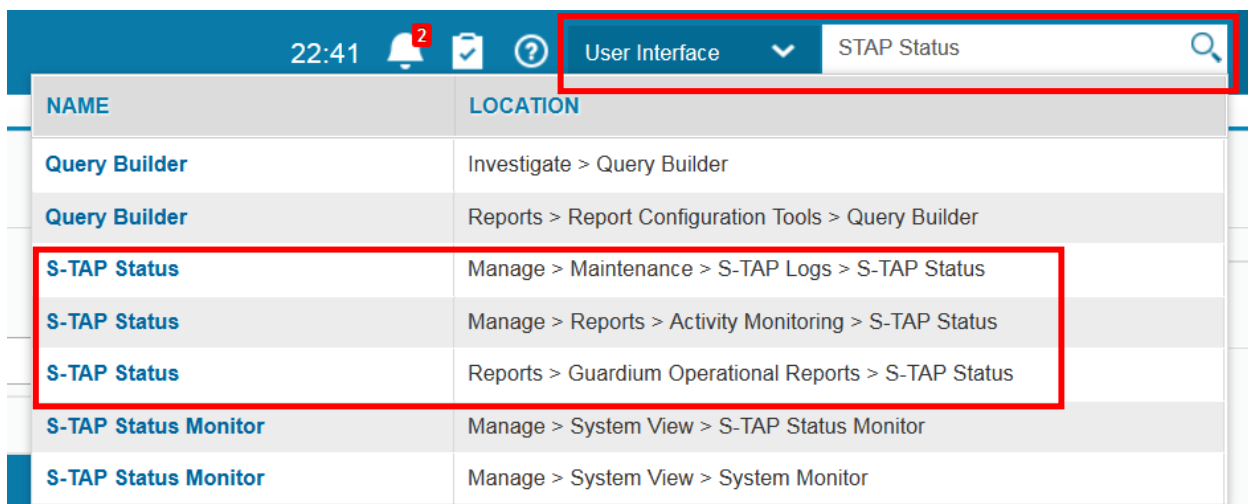
The following chargeable component can be classified as belonging to an activity monitoring group that possesses identical criteria for mapping server IPs.

cc - [IBM Security Guardium Data Protection for SharePoint](#)

How to map

Normally the IBM Security Guardium Data Protection maps to FDEC-SP and FAM-SP. The S-TAP Status report, accessed through **Quick Search Dialog using search string” S-TAP Status” in User Interface Search box**, which shows the S-TAP Host (server IP) that the IBM Security Guardium Data Protection for SharePoint is installed to discover, classify and/or monitor data.

Search “STAP Status” :



The screenshot shows the IBM Security Guardium User Interface. At the top, there is a search bar with the text 'STAP Status' and a magnifying glass icon. Below the search bar, a table displays the search results. The table has two columns: 'NAME' and 'LOCATION'. The results are as follows:

NAME	LOCATION
Query Builder	Investigate > Query Builder
Query Builder	Reports > Report Configuration Tools > Query Builder
S-TAP Status	Manage > Maintenance > S-TAP Logs > S-TAP Status
S-TAP Status	Manage > Reports > Activity Monitoring > S-TAP Status
S-TAP Status	Reports > Guardium Operational Reports > S-TAP Status
S-TAP Status Monitor	Manage > System View > S-TAP Status Monitor
S-TAP Status Monitor	Manage > System View > System Monitor

STAP Status report :

	S-TAP Host	S-TAP Version	DB Server Type	Status	Last Response
●	9.70.157.232	10.2.40.95	INFORMIX	Active	2019-04-06 16:38:57
●	9.70.157.232	10.2.40.95	MONGO	Active	2019-04-06 16:38:57
●	9.70.157.232	10.2.40.95	MSSQL	Active	2019-04-06 16:38:57
●	9.70.157.232	10.2.40.95	ORACLE	Active	2019-04-06 16:38:57
●	9.70.157.232:FAM	IBM_FSM_10.2.40.95		Active	2019-04-06 16:38:56
●	qsw2k16fig:Scan 1:FDEC-NAS	IBM_FSM_11.0.0.37		Active	2019-04-06 16:38:56
●	sp2013w2k12-03:FAM-SP	IBM_FSM_1.0.0.0		Active	2019-04-06 16:38:56
●	sp2013web1:FAM-SP	IBM_FSM_11.0.0.40		Active	2019-04-06 16:38:56
●	sp2013web2:FAM-SP	IBM_FSM_10.6.1.10		Active	2019-04-06 16:38:56
●	w2k12sql2k14:emc-cifs01:FAM-NAS	IBM_FSM_10.6.1.10		Active	2019-04-06 16:38:56

For Blocking:

IBM Security Guardium Data Protection for SharePoint monitors and enforces data protection using an STAP. To find if a policy has been configured to use STAP for blocking, you can look at the policy rules and their actions by going to **Protect -> Policy Builder for Files -> Selecting the Policy -> Edit Rules** and then expanding the individual rules to see if **Block, Log as Violation & Audit** is part of the Rule Action section.

- If the File Policy Rules include specific Server IPs (or a group of IPs) or Hostnames– then these IPs and Hostnames are in scope

Note: IBM Security Data Protection for SharePoint is charged based on Authorized Users (Active Directory accounts that have authorized access to SharePoint)

Please note the following for IBM Security Guardium Data Protections for SharePoint (SP):

IBM Security Guardium Data Protection for SP includes entitlements for File Discovery, Entitlement & Classification (FDEC), File Activity Monitoring (FAM) and necessary appliances required to discover, classify and monitor unstructured data on a SharePoint farm. FDEC for SP and FAM for SP can be installed independently using separately packaged installers.

PID 5737-H30- IBM Security Guardium for NAS - IBM Security Guardium Data Protection for NAS

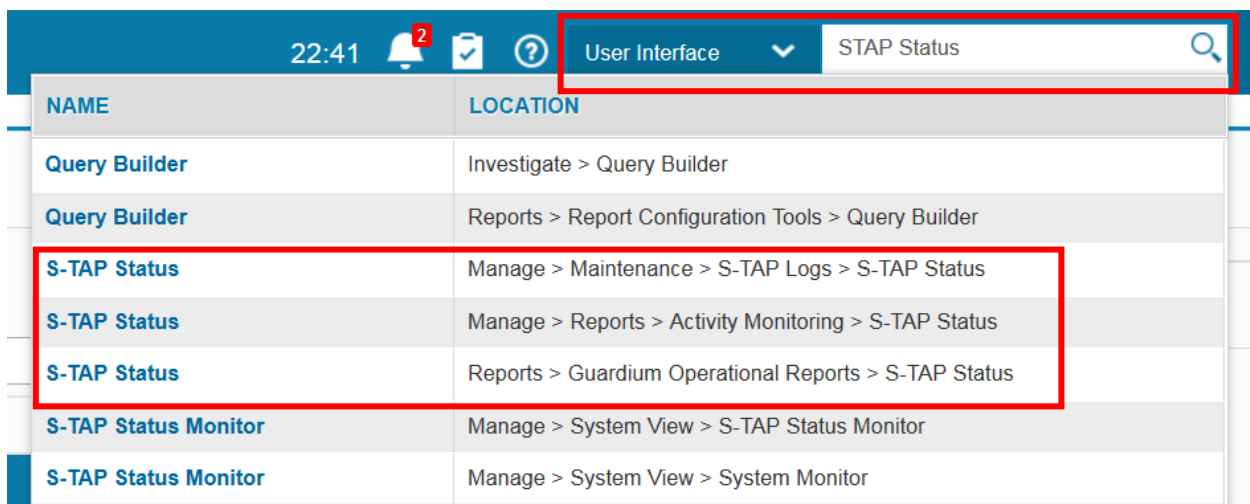
The following chargeable component can be classified as belonging to an activity monitoring group that possesses identical criteria for mapping server IPs.

cc - [IBM Security Guardium Data Protection for NAS](#)

How to map

Normally the IBM Security Guardium Data Protection for NAS is mapped to FDEC-NAS and FAM-NAS. The S-TAP Status report, accessed through **Quick Search Dialog using search string “S-TAP Status” in User Interface Search box**, which shows the S-TAP Host (server IP) that the IBM Security Guardium Data Protection for NAS is installed to discover, classify and/or monitor data.

Search “STAP Status” :



The screenshot shows the IBM Security Guardium User Interface. At the top, there is a search bar with the text 'STAP Status' and a magnifying glass icon. Below the search bar, a table displays the search results. The table has two columns: 'NAME' and 'LOCATION'. The results are as follows:

NAME	LOCATION
Query Builder	Investigate > Query Builder
Query Builder	Reports > Report Configuration Tools > Query Builder
S-TAP Status	Manage > Maintenance > S-TAP Logs > S-TAP Status
S-TAP Status	Manage > Reports > Activity Monitoring > S-TAP Status
S-TAP Status	Reports > Guardium Operational Reports > S-TAP Status
S-TAP Status Monitor	Manage > System View > S-TAP Status Monitor
S-TAP Status Monitor	Manage > System View > System Monitor

STAP Status report :

	S-TAP Host	S-TAP Version	DB Server Type	Status	Last Response	F
●	9.70.157.232	10.2.40.95	INFORMIX	Active	2019-04-06 16:38:57	9
●	9.70.157.232	10.2.40.95	MONGO	Active	2019-04-06 16:38:57	9
●	9.70.157.232	10.2.40.95	MSSQL	Active	2019-04-06 16:38:57	9
●	9.70.157.232	10.2.40.95	ORACLE	Active	2019-04-06 16:38:57	9
●	9.70.157.232:FAM	IBM_FSM_10.2.40.95		Active	2019-04-06 16:38:56	9
●	qsw2k16fig:Scan 1:FDEC-NAS	IBM_FSM_11.0.0.37		Active	2019-04-06 16:38:56	9
●	sp2013w2k12-03:FAM-SP	IBM_FSM_1.0.0.0		Active	2019-04-06 16:38:56	9
●	sp2013web1:FAM-SP	IBM_FSM_11.0.0.40		Active	2019-04-06 16:38:56	9
●	sp2013web2:FAM-SP	IBM_FSM_10.6.1.10		Active	2019-04-06 16:38:56	9
●	w2k12sql2k14:emc-cifs01:FAM-NAS	IBM_FSM_10.6.1.10		Active	2019-04-06 16:38:56	9

For Blocking:

IBM Security Guardium Data Protection for NAS monitors and enforces data protection using an STAP. To find if a policy has been configured to use STAP for blocking, you can look at the policy rules and their actions by going to **Protect -> Policy Builder for Files -> Selecting the Policy -> Edit Rules** and then expanding the individual rules to see if **Block, Log as Violation & Audit** is part of the Rule Action section.

- If the File Policy Rules include specific Server IPs (or a group of IPs) or Hostnames– then these IPs and Hostnames are in scope

Note: IBM Security Data Protection for NAS is charged based on Authorized Users I.e. Active Directory accounts that have authorized access to file shares mapped by NAS Devices (Hosts).

Please note the following for IBM Security Guardium Data Protections for NAS (DP for NAS):

IBM Security Guardium Data Protection for NAS includes entitlements for File Discovery, Entitlement & Classification (FDEC), File Activity Monitoring (FAM) and necessary appliances required to discover, classify and monitor unstructured data on NAS devices. FDEC for NAS and FAM for NAS can be installed independently using separately packaged installers.

PID 5725-I12 - IBM Security Guardium Data Security and Compliance - IBM Security Guardium Database Vulnerability Assessment Solution

How to map

CC - [IBM Security Guardium Vulnerability Assessment for Databases](#)

5. The list of data sources defined under **Harden -> Vulnerability Assessment -> Datasource Definitions** will provide the database server IPs being used. (Note: when datasource presents just the hostname, you'd need to click the 'Modify' button to see its IP address for)
6. The configuration, as seen through **Harden -> Reports -> CAS Configuration**
 - **CAS Instances & CAS Instance Config**, will display the list of server IPs.

PID 5725-I12 - IBM Security Guardium Data Security and Compliance - IBM Security Guardium Database Activity Monitor Group

The following chargeable components can be classified as belonging to an activity monitoring group that possesses identical criteria for mapping server IPs.

Standard Data Activity Monitoring:

CC - [IBM Security Guardium Standard Activity Monitor for Databases](#)

CC - [IBM Security Guardium Standard Activity Monitor for Data Warehouses](#)






CC- [IBM Security Guardium Standard Activity Monitor for Big Data](#)

How to map
















The IBM Security Guardium Standard Activity Monitor auditing activity can be mapped to:

11. Normally the IBM Security Guardium Database Activity Monitor monitors activity using S-TAP. The S-TAP Status report, accessed through **Quick Search Dialog using search string "S-TAP Status" in User Interface Search box**, which shows the S-TAP Host (server IP) that the IBM Security Guardium Database Activity Monitor is monitoring.

Search "STAP Status" :

22:41   		User Interface 	STAP Status 
NAME	LOCATION		
Query Builder	Investigate > Query Builder		
Query Builder	Reports > Report Configuration Tools > Query Builder		
S-TAP Status	Manage > Maintenance > S-TAP Logs > S-TAP Status		
S-TAP Status	Manage > Reports > Activity Monitoring > S-TAP Status		
S-TAP Status	Reports > Guardium Operational Reports > S-TAP Status		
S-TAP Status Monitor	Manage > System View > S-TAP Status Monitor		
S-TAP Status Monitor	Manage > System View > System Monitor		

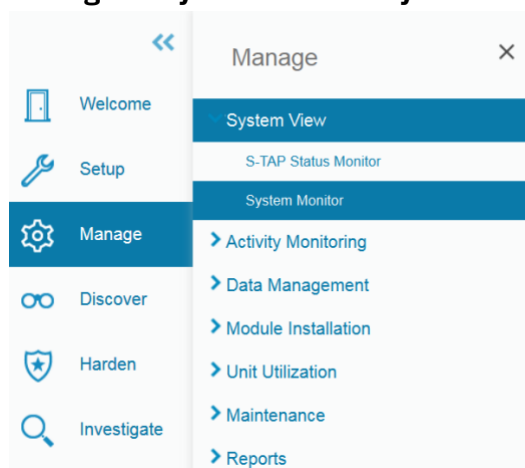
STAP Status report :

S-TAP Status										
<div>        </div> <div>Export  Actions  </div>										
	S-TAP Host	S-TAP Version	DB Server Type	Status	Last Response	Primary Host Name	KTAP Installed	TEE Installed	Shared Memory Driver Installed	DB2 Shared
	9.181.139.212	STAP-9.0.0_r4564	DB2	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No
	9.181.139.212	STAP-9.0.0_r4564	INFORMIX	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No
	9.181.139.212	STAP-9.0.0_r4564	mysql	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No
	9.181.139.212	STAP-9.0.0_r4564	ORACLE	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No
	9.181.139.212	STAP-9.0.0_r4564	ORACLE	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No

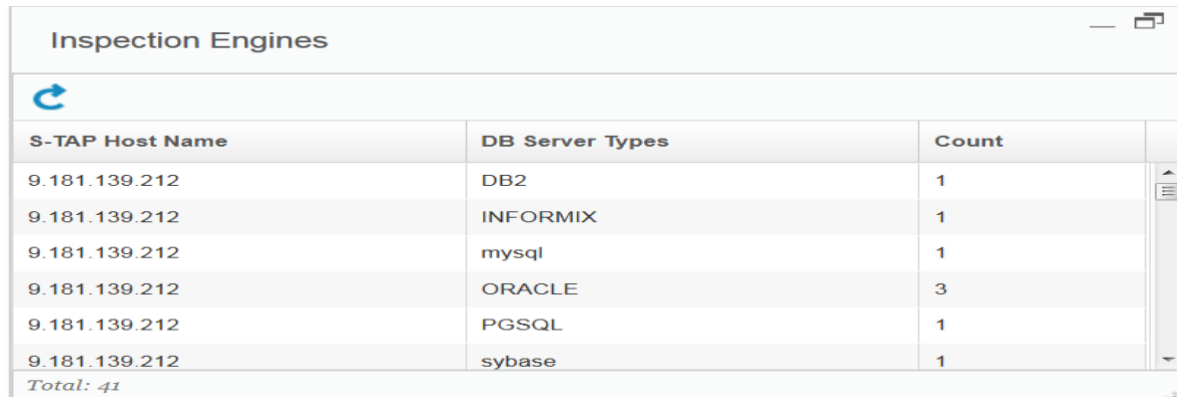
12. If not using S-TAP, but instead using network inspection you can go to the console inspection engines and see the Server IPs being monitored.

Access by going to :

Manage -> System View -> System Monitor → Inspection Engine.



Slide down to look for Inspection Engine view



The image shows a window titled "Inspection Engines" with a table of data. The table has three columns: "S-TAP Host Name", "DB Server Types", and "Count". There are six rows of data, each showing the same host name "9.181.139.212" and different database types: DB2, INFORMIX, mysql, ORACLE, PGSQL, and sybase. The counts are 1, 1, 1, 3, 1, and 1 respectively. A "Total: 41" is shown at the bottom left of the table area. There is a refresh icon in the top left of the table area and a scroll bar on the right.

S-TAP Host Name	DB Server Types	Count
9.181.139.212	DB2	1
9.181.139.212	INFORMIX	1
9.181.139.212	mysql	1
9.181.139.212	ORACLE	3
9.181.139.212	PGSQL	1
9.181.139.212	sybase	1

Total: 41

Note:

CC - IBM Security Guardium Standard Activity Monitor for Databases

Access reports, such as the **Data-Sources**, accessed by going to **Reports -> Report Configuration Tools -> Data-Sources**, can be used to show a listing of the server IPs for the database servers seen during a reporting period. This CC is charged based on the PVU (Processor Value Units) on the hosts being monitored, either by STAP or Network monitoring.

CC - IBM Security Guardium Standard Activity Monitor for Data Warehouses

Access reports, such as the **Data-Sources**, accessed by going to **Reports -> Report Configuration Tools -> Data-Sources**, can be used to show a listing of the server IPs for the data warehouse servers seen during a reporting period. This CC is charged based on the RVU (Resource Value Units) based on TB capacity of the data warehouse hosts being monitored, either by STAP or Network monitoring.

CC- IBM Security Guardium Standard Activity Monitor for Big Data

Access reports, such as the **Data-Sources**, accessed by going to **Reports -> Report Configuration Tools -> Data-Sources**, can be used to show a listing of the server IPs for the data warehouse servers seen during a reporting period. This CC is charged based on the RVU (Resource Value Units) based on Managed Virtual Servers (MVS) or nodes of the Big Data environment being monitored, either by STAP or Network monitoring.

Advanced Data Activity Monitoring:

CC- IBM Security Guardium Advanced Activity Monitor for Databases

CC- IBM Security Guardium Advanced Activity Monitor for Data Warehouses

CC- IBM Security Guardium Advanced Activity Monitor for BigData

How to map

IBM Security Guardium Advanced Activity Monitor for Databases monitors and enforces data protection using an S-GATE instead of an STAP. To find if a policy has been configured to use S-GATE, you can look at the policy rules and their actions by going to **Protect -> Policy Builder for Data-> Selecting the Policy -> Edit Rules** and then expanding the individual rules to see if **S-GATE** is part of the Actions defined. If S-GATE rules are in use, then the list of server IPs would then be one of the following:

- If the S-GATE Policy Rules include specific Server IPs (or a group of IPs) or hostnames – then these IPs and hostnames are in scope
- If the S-GATE Policy Rules have ‘ANY’ for Server IPs or hostnames – use the Server IPs or hostnames are defined for the IBM Security Guardium Database Activity Monitor group (see above).

Note :

CC- IBM Security Guardium Advanced Activity Monitor for Databases

This CC is charged based on the PVU (Processor Value Units) on the hosts being monitored, either by STAP or Network monitoring.

CC- IBM Security Guardium Advanced Activity Monitor for Data Warehouses

This CC is charged based on the RVU (Resource Value Units) based on TB capacity of the data warehouse hosts being monitored, either by STAP or Network monitoring.

CC- IBM Security Guardium Advanced Activity Monitor for BigData

This CC is charged based on the RVU (Resource Value Units) based on Managed Virtual Servers (MVS) or nodes of the Big Data environment being monitored, either by STAP or Network monitoring.

PID 5725-V56 - IBM Security Guardium for Files - IBM Security Guardium Activity Monitor for Files Group

The following chargeable components can be classified as belonging to an activity monitoring group that possesses identical criteria for mapping server IPs.

cc - [IBM Security Guardium Standard Activity Monitor for Files](#)

How to map

The IBM Security Guardium Standard Activity Monitor auditing activity can be mapped to:

13. Normally the IBM Security Guardium Database Activity Monitor monitors activity using S-TAP. The S-TAP Status report, accessed through **Quick Search Dialog using search string "S-TAP Status"** in *User Interface Search box*, which shows the S-TAP Host (server IP) that the IBM Security Guardium Database Activity Monitor is monitoring.

Search "STAP Status" :

The screenshot shows the 'User Interface' search results for 'STAP Status'. The results are displayed in a table with two columns: 'NAME' and 'LOCATION'. The 'NAME' column lists various components, and the 'LOCATION' column shows the navigation path to each component. A red box highlights the search bar and the first three results.

NAME	LOCATION
Query Builder	Investigate > Query Builder
Query Builder	Reports > Report Configuration Tools > Query Builder
S-TAP Status	Manage > Maintenance > S-TAP Logs > S-TAP Status
S-TAP Status	Manage > Reports > Activity Monitoring > S-TAP Status
S-TAP Status	Reports > Guardium Operational Reports > S-TAP Status
S-TAP Status Monitor	Manage > System View > S-TAP Status Monitor
S-TAP Status Monitor	Manage > System View > System Monitor

STAP Status report :

S-TAP Status

The screenshot shows the 'S-TAP Status' report table. The table has 11 columns: S-TAP Host, S-TAP Version, DB Server Type, Status, Last Response, Primary Host Name, KTAP Installed, TEE Installed, Shared Memory Driver Installed, and DB2 Shared. There are 5 rows of data, all showing 'Active' status.

S-TAP Host	S-TAP Version	DB Server Type	Status	Last Response	Primary Host Name	KTAP Installed	TEE Installed	Shared Memory Driver Installed	DB2 Shared
9.181.139.212	STAP-9.0.0_r4564	DB2	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No
9.181.139.212	STAP-9.0.0_r4564	INFORMIX	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No
9.181.139.212	STAP-9.0.0_r4564	mysql	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No
9.181.139.212	STAP-9.0.0_r4564	ORACLE	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No
9.181.139.212	STAP-9.0.0_r4564	ORACLE	Active	2015-08-05 12:56:12	9.70.148.45	Yes	No	No	No

CC- IBM Security Guardium Advanced Activity Monitor for Files

How to map

IBM Security Guardium Advanced Activity Monitor for Files monitors and enforces data protection using an STAP. To find if a policy has been configured to use STAP for blocking, you can look at the policy rules and their actions by going to **Protect -> Policy Builder for Files -> Selecting the Policy -> Edit Rules** and then expanding the individual rules to see if **Block, Log As Violation & Audit** is part of the Rule Action section.

- If the File Policy Rules include specific Server IPs (or a group of IPs) or Hostnames– then these IPs and Hostnames are in scope

Note: This CC is charged based on RVU (Resource Value Units) where the RVU is TB, on the hosts being monitored by STAP, or where a File Activity Monitoring (Discovery & Classification) are installed.

You can also tell if IBM Security Guardium Advanced Activity Monitor for Files is enabled by looking at the About page. From the banner, click "?" and then click About Guardium.



IBM Guardium
Version: 11.4

IBM

Functions Enabled:
Advanced Activity Monitor for Databases, z/OS, Big Data, and Data Warehouses, Advanced Activity Monitor for Files, Vulnerability Assessment for Databases

System Information:
Version: 11.4.0_r111014_v11_4_1-el79-20210812_1334
Latest patch number: 400
Latest patch description: Guardium Patch Update (GPU) for Version 11 (Aug 13 2021)
Latest patch upload: 2021-08-16 12:59:35.0

Licensed Materials - Property of IBM
5725-I11, 5725-I12, 5725-V56, 5737-D57, 5737-M13
Licensed Materials
5737-H30, 5737-H31
© Copyright IBM Corp. 2002, 2021 All Rights Reserved.
*Trademark of International Business Machines
Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

PID 5725-I12 - IBM Security Guardium Data Security and Compliance - IBM Security Guardium Central Management and Aggregation Group

How to map

CC - IBM Security Guardium Central Management and Aggregation for Databases Pack

IBM Security Guardium provides the ability, through Compliance Workflow Automation, to streamline the compliance workflow process by consolidating the database activity that is

uploaded to the appliance from the customer's environment. Thus, this is the same as defined for the IBM Security Guardium Database Activity Monitor for Databases group, see above.

CC - IBM Security Guardium Central Management and Aggregation for Data Warehouses Pack

IBM Security Guardium provides the ability, through Compliance Workflow Automation, to streamline the compliance workflow process by consolidating the data warehouse activity that is uploaded to the appliance from the customer's environment. Thus, this is the same as defined for the IBM Security Guardium Activity Monitor for Data Warehouse, see above.

CC - IBM Security Guardium Central Management and Aggregation for Big Data Pack

IBM Security Guardium provides the ability, through Compliance Workflow Automation, to streamline the compliance workflow process by consolidating the Big Data (Hadoop or NoSQL) environment activity that is uploaded to the appliance from the customer's environment. Thus, this is the same as defined for the IBM Security Guardium Activity Monitor for Big Data, see above.

IBM Security Guardium 12.0 Licensed Materials – Property of IBM. © Copyright IBM Corp. 2002, 2023 Rights Reserved. U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp. IBM, the IBM logo, and ibm.com are trademarks 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 www.ibm.com/legal/copytrade.shtml.

The following terms are trademarks or registered trademarks of other companies:

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product or service names may be trademarks or service marks of others.