What’s new in Guardium DP V11.3

Shay Harel
Director of Engineering – Data Security

Legal Disclaimer

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM’s current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM’s sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

The numbers behind 11.3

25+

Databases with new/updated currency

52

RFEs

24

Features targeting pain points

6

New/Improved Integrations

New WSTAP

2X SQL/Sec

5X Less CPU

2X Less Memory

Agenda

- Guardium Universal Connector
- MongoDB Classification
- Deployment Health Enhancements
- Policy Tagging
- Integration with Resilient for External Ticketing
- Integration with Venafi
- Integration with AWS Secret Manager

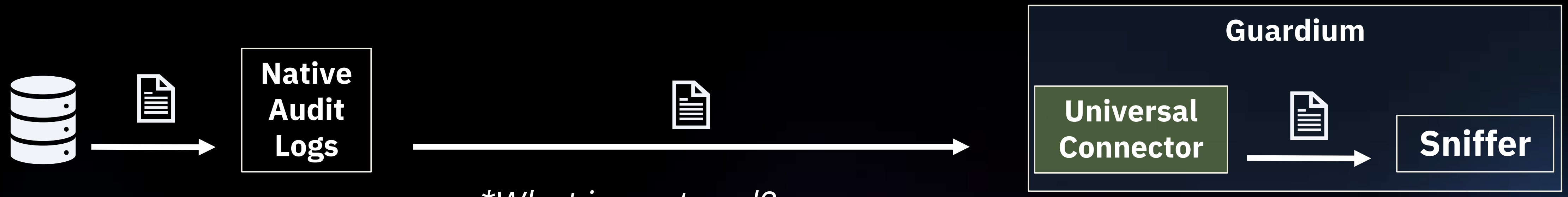
- Session Level Policy
- Windows STAP – New Protocol
- UNIX STAP
- Ansible Automation
- VA Enhancements
- Odd and Ends

Guardium Universal Connector

- **STAP is King –**
  - Separation of duties
  - Lightweight agent (no impact of DB),
  - Real time traffic monitoring
  - Blocking, redaction
  - Secure – no logs with clear text

- **…. But STAP is not perfect**
  - Needs to be synched with the server OS
  - ATAP is intrusive
  - Need to install and configure

Universal Connector - Flow



Native Audit Logs

Guardium

Universal Connector

Sniffer

Data source writes or pushes logs to storage

*<u>*What is captured?</u>*

***Sessions**: Who or What is talking to the database*

***Requests**: What data is being requested and Who is accessing it*

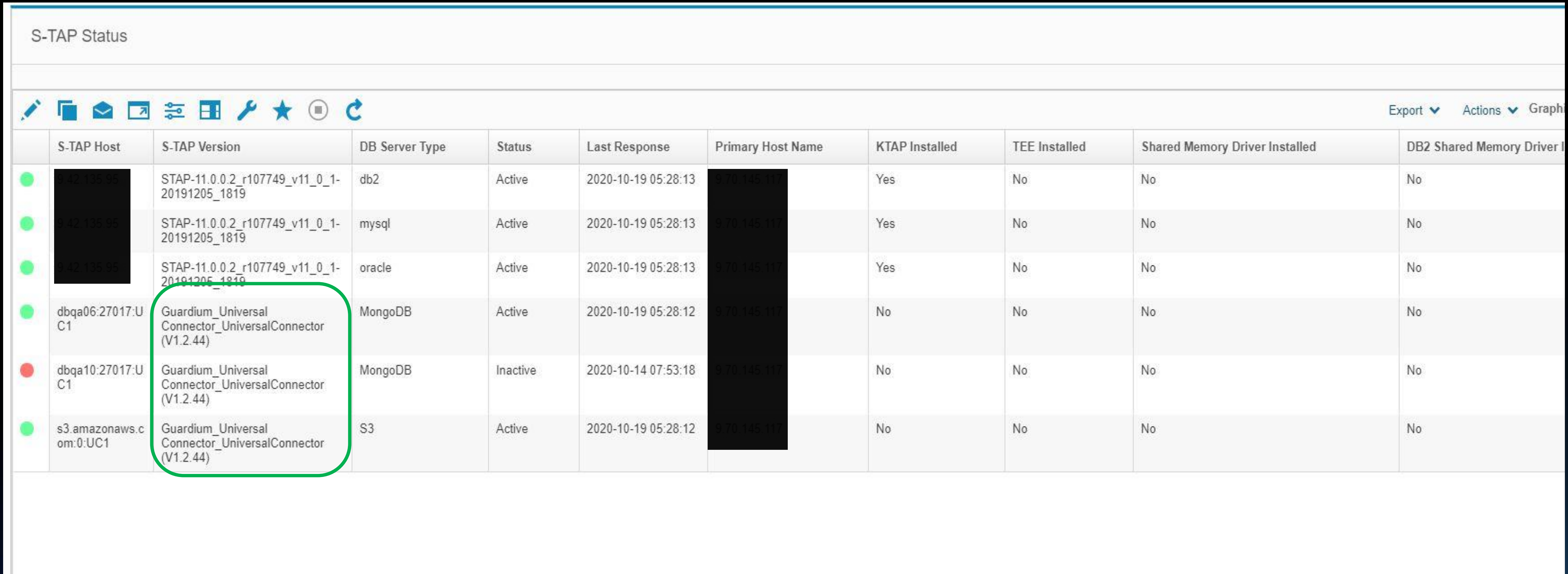
***Errors**: What exceptions have occurred*

** Varies with what is written to the native audit logs*

Pulls (or receives from Push) logs from data source

Parses and transforms the logs into a universal format that the Sniffer understands

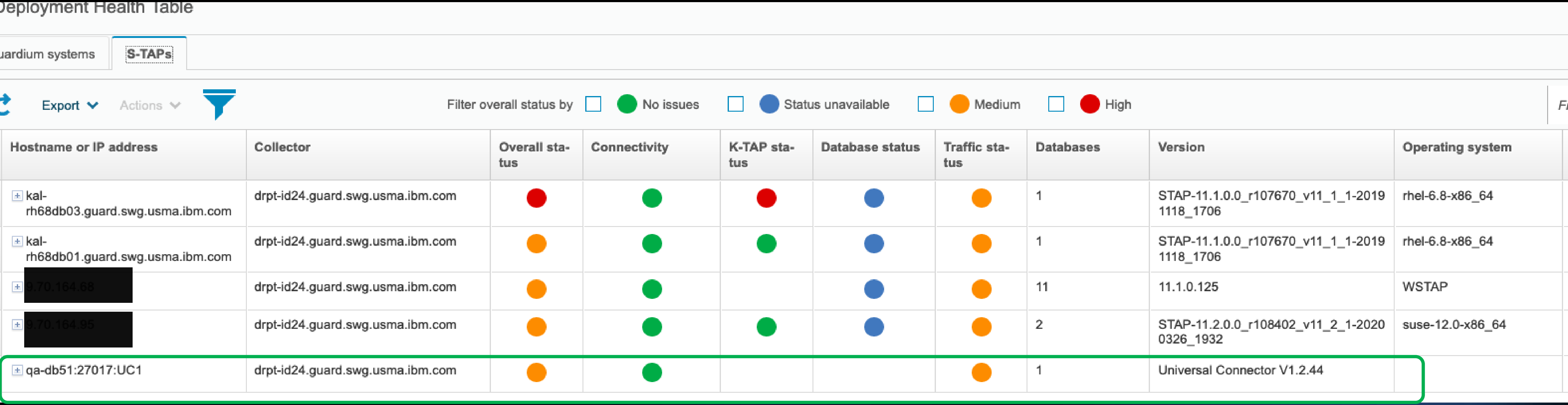
View Universal Connector status in Guardium



S-TAP 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 Memory Driver I
●	[redacted]	STAP-11.0.0.2_r107749_v11_0_1-20191205_1819	db2	Active	2020-10-19 05:28:13	[redacted]	Yes	No	No	No
●	[redacted]	STAP-11.0.0.2_r107749_v11_0_1-20191205_1819	mysql	Active	2020-10-19 05:28:13	[redacted]	Yes	No	No	No
●	[redacted]	STAP-11.0.0.2_r107749_v11_0_1-20191205_1819	oracle	Active	2020-10-19 05:28:13	[redacted]	Yes	No	No	No
●	dbqa06:27017:UC1	Guardium_Universal Connector_UniversalConnector (V1.2.44)	MongoDB	Active	2020-10-19 05:28:12	[redacted]	No	No	No	No
●	dbqa10:27017:UC1	Guardium_Universal Connector_UniversalConnector (V1.2.44)	MongoDB	Inactive	2020-10-14 07:53:18	[redacted]	No	No	No	No
●	s3.amazonaws.com:0:UC1	Guardium_Universal Connector_UniversalConnector (V1.2.44)	S3	Active	2020-10-19 05:28:12	[redacted]	No	No	No	No

Guardium Deployment Heath Table (on CM)



Deployment Health Table

uardium systems | S-TAPs

Filter overall status by □ 🟢 No issues □ 🔵 Status unavailable □ 🟠 Medium □ 🔴 High

Hostname or IP address	Collector	Overall status	Connectivity	K-TAP status	Database status	Traffic status	Databases	Version	Operating system
kal-rh68db03.guard.swg.usma.ibm.com	drpt-id24.guard.swg.usma.ibm.com	🔴	🟢	🔴	🔵	🟠	1	STAP-11.1.0.0_r107670_v11_1_1-20191118_1706	rhel-6.8-x86_64
kal-rh68db01.guard.swg.usma.ibm.com	drpt-id24.guard.swg.usma.ibm.com	🟠	🟢	🟢	🔵	🟠	1	STAP-11.1.0.0_r107670_v11_1_1-20191118_1706	rhel-6.8-x86_64
[redacted]	drpt-id24.guard.swg.usma.ibm.com	🟠	🟢		🔵	🟠	11	11.1.0.125	WSTAP
[redacted]	drpt-id24.guard.swg.usma.ibm.com	🟠	🟢	🟢	🔵	🟠	2	STAP-11.2.0.0_r108402_v11_2_1-20200326_1932	suse-12.0-x86_64
qa-db51:27017:UC1	drpt-id24.guard.swg.usma.ibm.com	🟠	🟢			🟠	1	Universal Connector V1.2.44	

Supported platforms

At GA

- MongoDB On premise Enterprise version 2.6 and above
  - Syslog
  - Filebeat
- Amazon S3
  - Cloudwatch and Cloudtrail
  - SQS

Around the corner

- HDFS/HIVE
- MySQL
- Oracle UOA/Exadata
- MSSQL

2Q21

- Redis
- PostgresSQL
- Snowflake
- DynamoDB
- SAP Hana
- Neo4j

One page with all the resources

- A single landing page (here) with all resources for the Universal Connector:
  - Supported platforms (and what’s coming next)
  - Training
  - Documentation
  - Examples of how to create your own connectors

MongoDB Classification

Classification for Mongo DB Adding support for discovery / classification for big data platforms like Mongo DB can scan sensitive data on the MongoDB for compliance frameworks like CCPA, GDPR, PII, HIPPA, PCI etc.

What's New

- New field - Datasource type
  - Relational DB
  - Document DB
- Custom and user defined policies can be used across scenarios with different datasource type

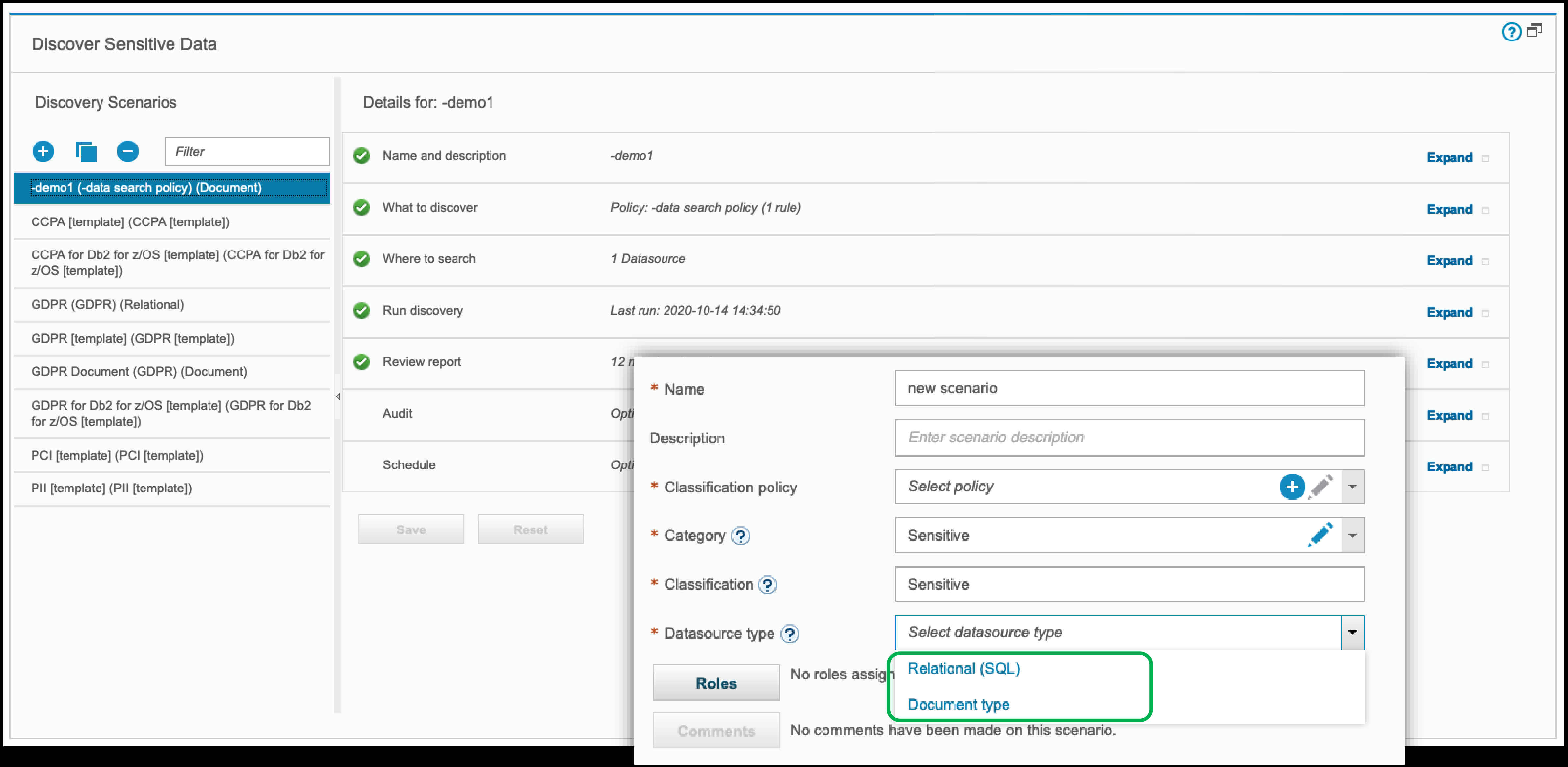
Benefits

- Clear separation between SQL vs NO-SQL databases
- Rules and reports use database terminology based on Datasource Type

Architecture

Mapping of MongoDB with SQL terminology.

Report	SQL: relational	MONGODB
Catalog name	Databases	dbs
Schema name	Schema	-
Table name	Tables	Collections
Column name	columns	attributes/ fields
-	rows	documents



Discover Sensitive Data

Discovery Scenarios

Filter

-demo1 (-data search policy) (Document)

CCPA [template] (CCPA [template])

CCPA for Db2 for z/OS [template] (CCPA for Db2 for z/OS [template])

GDPR (GDPR) (Relational)

GDPR [template] (GDPR [template])

GDPR Document (GDPR) (Document)

GDPR for Db2 for z/OS [template] (GDPR for Db2 for z/OS [template])

PCI [template] (PCI [template])

PII [template] (PII [template])

Details for: -demo1

✓ Name and description	-demo1	Expand
✓ What to discover	Policy: -data search policy (1 rule)	Expand
✓ Where to search	1 Datasource	Expand
✓ Run discovery	Last run: 2020-10-14 14:34:50	Expand
✓ Review report	12 n	Expand
Audit	Opti	Expand
Schedule	Opti	Expand

* Name: new scenario

Description: Enter scenario description

* Classification policy: Select policy

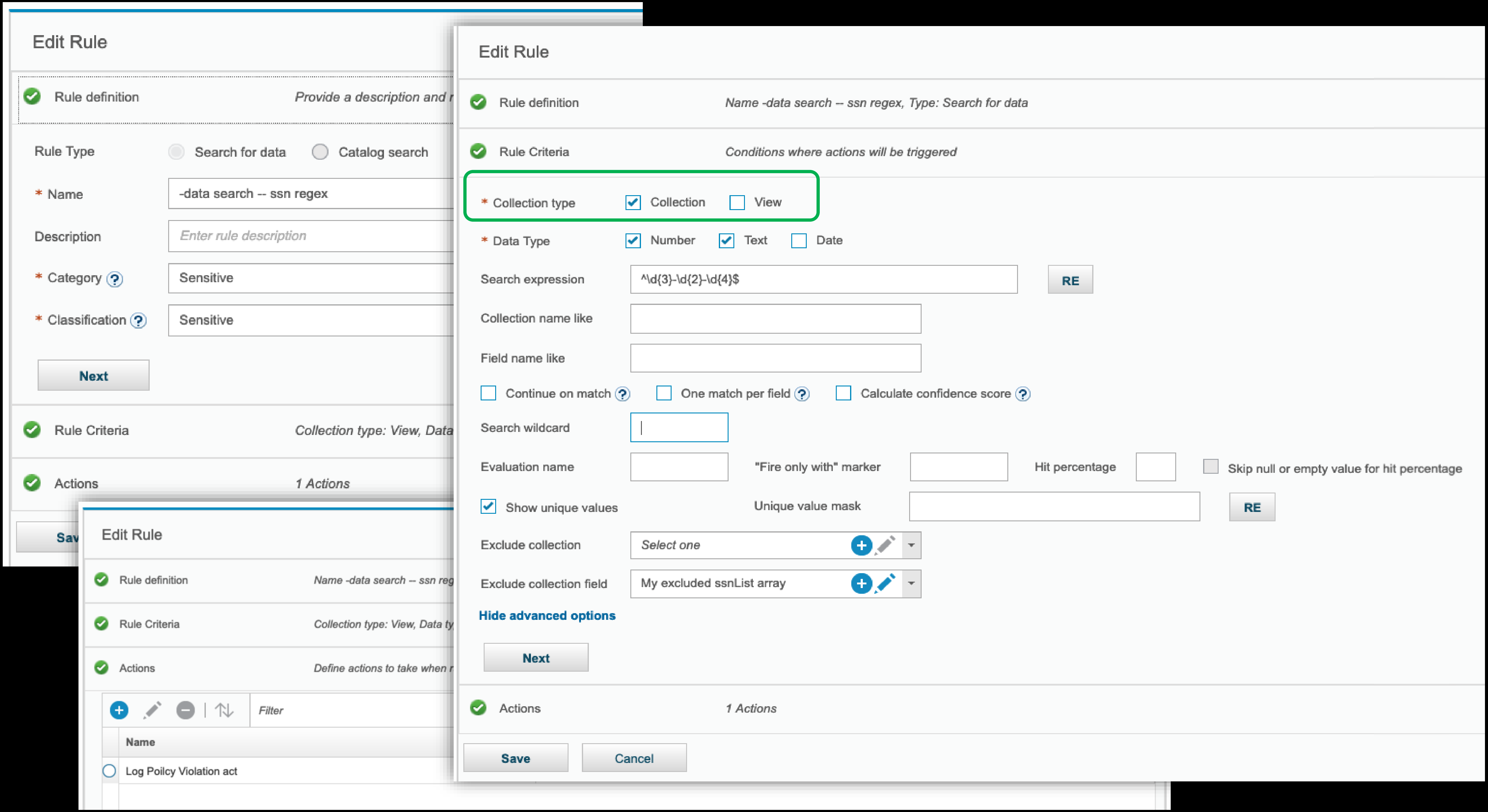
* Category: Sensitive

* Classification: Sensitive

* Datasource type: Select datasource type

No roles assig

No comments have been made on this scenario.



Edit Rule

✓ Rule definition *Provide a description and r*

Rule Type ○ Search for data ○ Catalog search

* Name: -data search -- ssn regex

Description: *Enter rule description*

* Category ?: Sensitive

* Classification ?: Sensitive

Next

✓ Rule Criteria *Collection type: View, Data*

✓ Actions *1 Actions*

Sav

Edit Rule

✓ Rule definition *Name -data search -- ssn reg*

✓ Rule Criteria *Collection type: View, Data ty*

✓ Actions *Define actions to take when r*

Filter

Name

○ Log Poilcy Violation act

Edit Rule

✓ Rule definition *Name -data search -- ssn regex, Type: Search for data*

✓ Rule Criteria *Conditions where actions will be triggered*

* Collection type ☑ Collection □ View

* Data Type ☑ Number ☑ Text □ Date

Search expression: ^\d{3}-\d{2}-\d{4}$ RE

Collection name like:

Field name like:

□ Continue on match ? □ One match per field ? □ Calculate confidence score ?

Search wildcard:

Evaluation name: "Fire only with" marker: Hit percentage: □ Skip null or empty value for hit percentage

☑ Show unique values Unique value mask: RE

Exclude collection: *Select one*

Exclude collection field: My excluded ssnList array

Hide advanced options

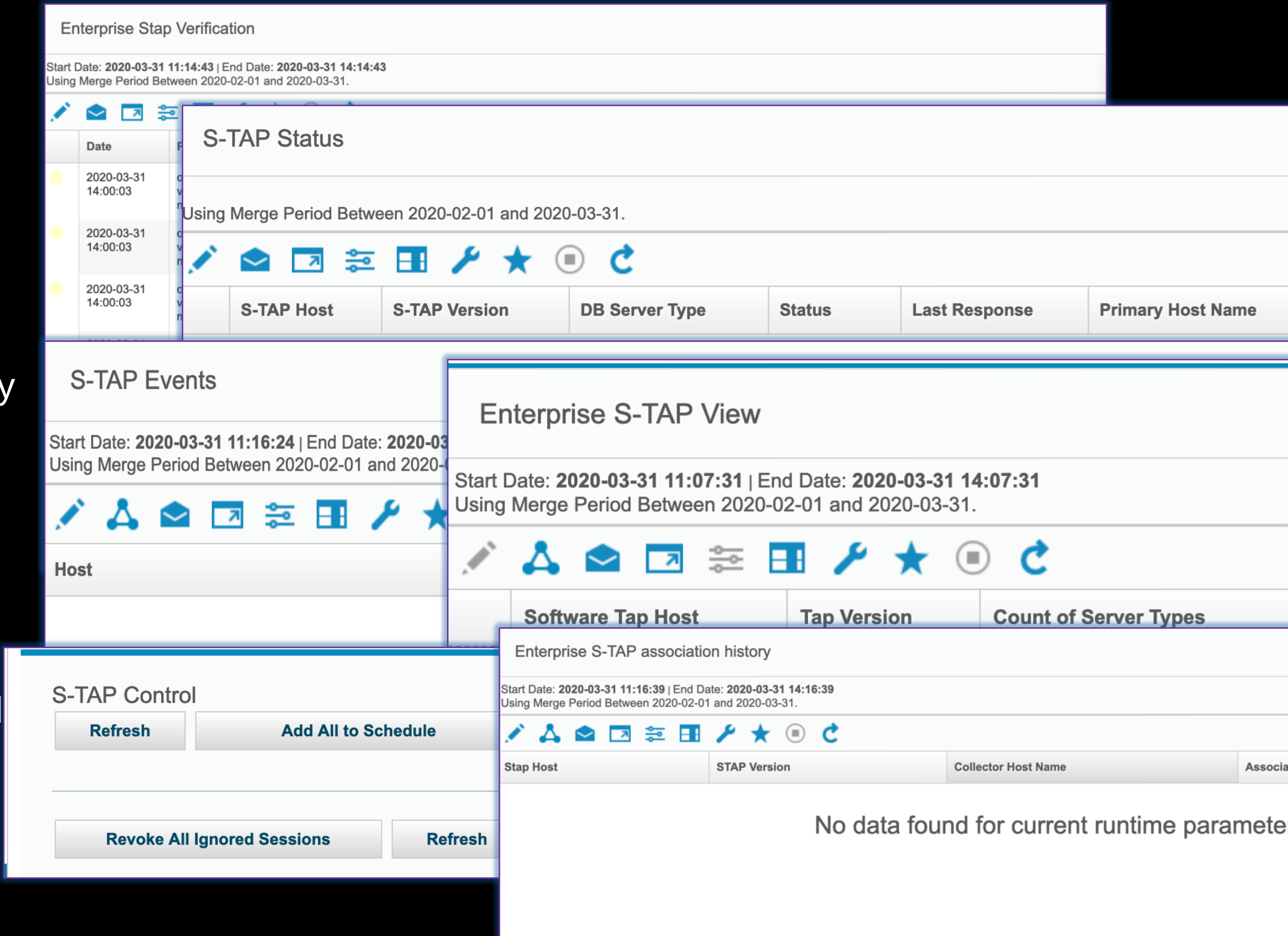
Next

✓ Actions *1 Actions*

Save Cancel

Deployment health – Before 11.2

- Lots (over 10) S-TAP reports/pages with similar names
- No summary counts or graphs
- No centralized data for many reports - need to log onto each managed unit individually
- Some have no data to start with
- Some need to be scheduled



Enterprise Stap Verification

Start Date: **2020-03-31 11:14:43** | End Date: **2020-03-31 14:14:43**
Using Merge Period Between 2020-02-01 and 2020-03-31.

Date
2020-03-31 14:00:03
2020-03-31 14:00:03
2020-03-31 14:00:03

S-TAP Status

Using Merge Period Between 2020-02-01 and 2020-03-31.

S-TAP Host	S-TAP Version	DB Server Type	Status	Last Response	Primary Host Name

S-TAP Events

Start Date: **2020-03-31 11:16:24** | End Date: **2020-03**
Using Merge Period Between 2020-02-01 and 2020-

Host

Enterprise S-TAP View

Start Date: **2020-03-31 11:07:31** | End Date: **2020-03-31 14:07:31**
Using Merge Period Between 2020-02-01 and 2020-03-31.

Software Tap Host	Tap Version	Count of Server Types

S-TAP Control

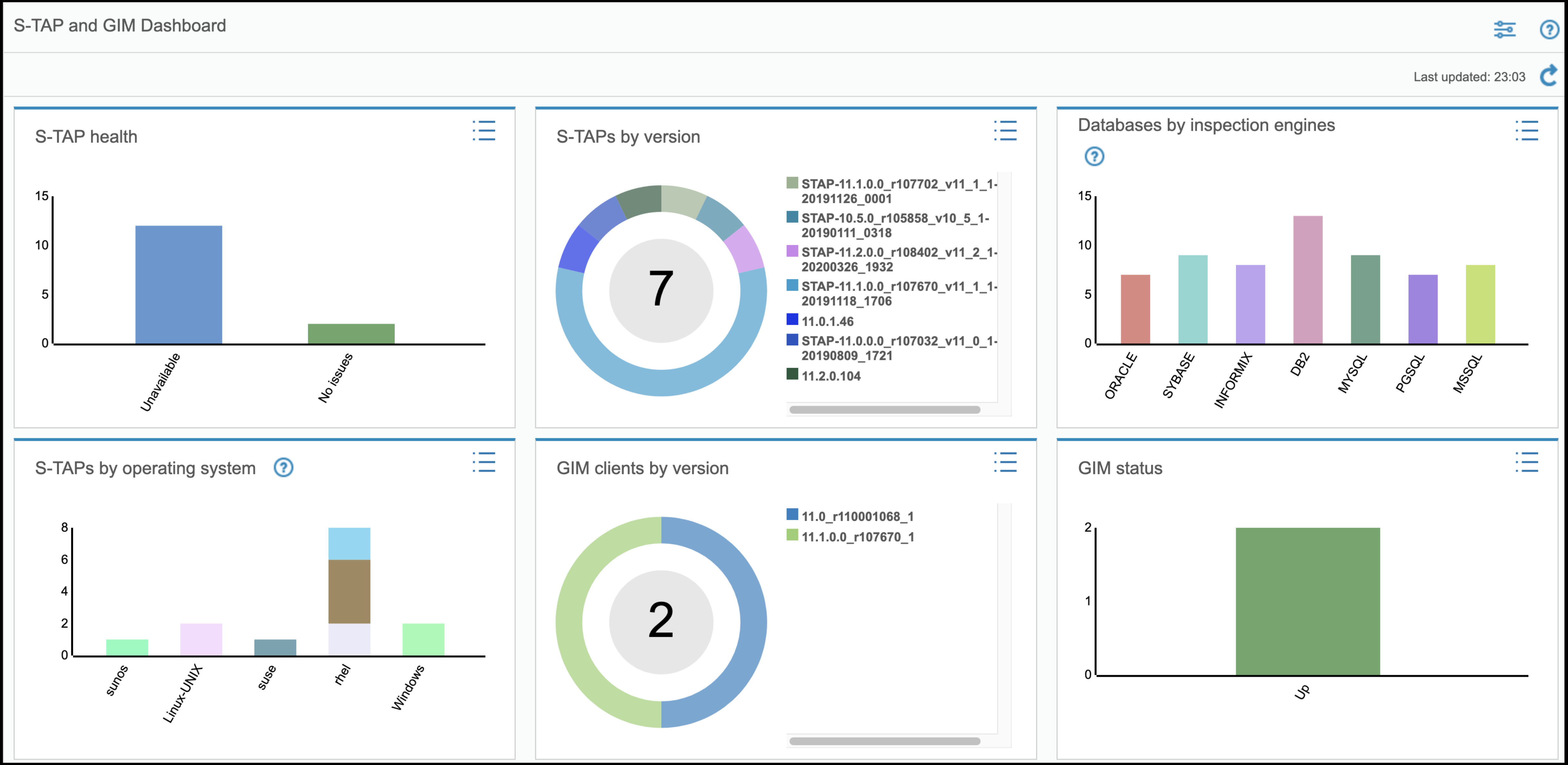
Enterprise S-TAP association history

Start Date: **2020-03-31 11:16:39** | End Date: **2020-03-31 14:16:39**
Using Merge Period Between 2020-02-01 and 2020-03-31.

Stap Host	STAP Version	Collector Host Name	Associa

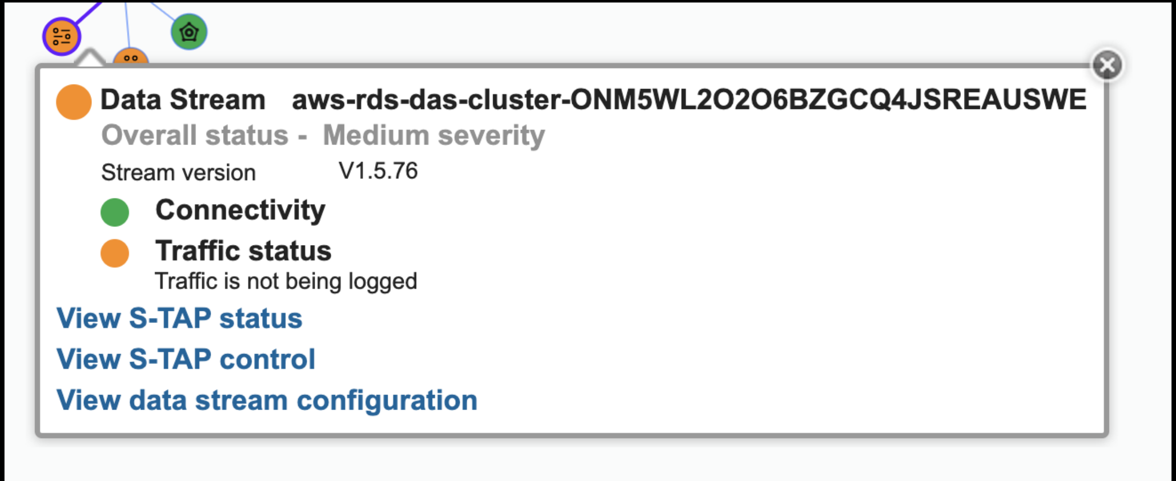
No data found for current runtime paramete

New in 11.2 - S-TAP and GIM dashboard: UI


S-TAP and GIM Dashboard
Last updated: 23:03
S-TAP health
15
10
5
0
Unavailable
No issues
S-TAPs by version
7
STAP-11.1.0.0_r107702_v11_1_1-20191126_0001
STAP-10.5.0_r105858_v10_5_1-20190111_0318
STAP-11.2.0.0_r108402_v11_2_1-20200326_1932
STAP-11.1.0.0_r107670_v11_1_1-20191118_1706
11.0.1.46
STAP-11.0.0.0_r107032_v11_0_1-20190809_1721
11.2.0.104
Databases by inspection engines
15
10
5
0
ORACLE
SYBASE
INFORMIX
DB2
MYSQL
PGSQL
MSSQL
S-TAPs by operating system
8
6
4
2
0
sunos
Linux-UNIX
suse
rhel
Windows
GIM clients by version
2
11.0_r110001068_1
11.1.0.0_r107670_1
GIM status
2
1
0
Up

Deployment Health Topology – we now show traffic status!

- Show Universal connector and datastreams



● **Data Stream aws-rds-das-cluster-ONM5WL2O2O6BZGCQ4JSREAUSWE**

Overall status - Medium severity

Stream version V1.5.76

● **Connectivity**

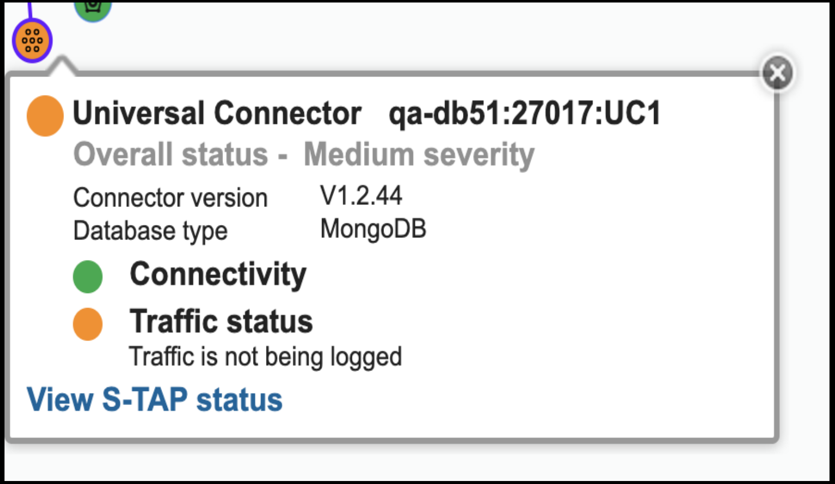
● **Traffic status**

Traffic is not being logged

View S-TAP status

View S-TAP control

View data stream configuration



● **Universal Connector qa-db51:27017:UC1**

Overall status - Medium severity

Connector version V1.2.44

Database type MongoDB

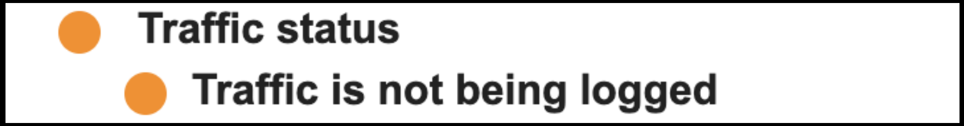
● **Connectivity**

● **Traffic status**

Traffic is not being logged

View S-TAP status

- Traffic status for S-TAPs



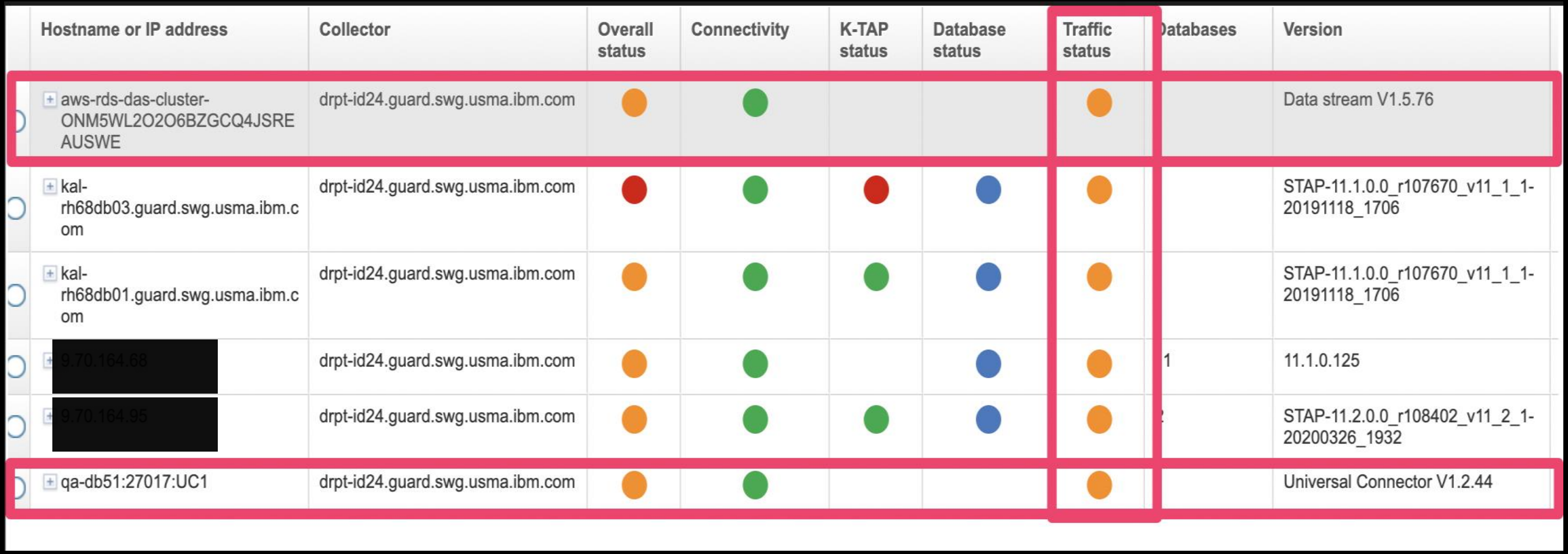
● **Traffic status**

● **Traffic is not being logged**

Deployment Health Table

- Show Universal connector and datastreams

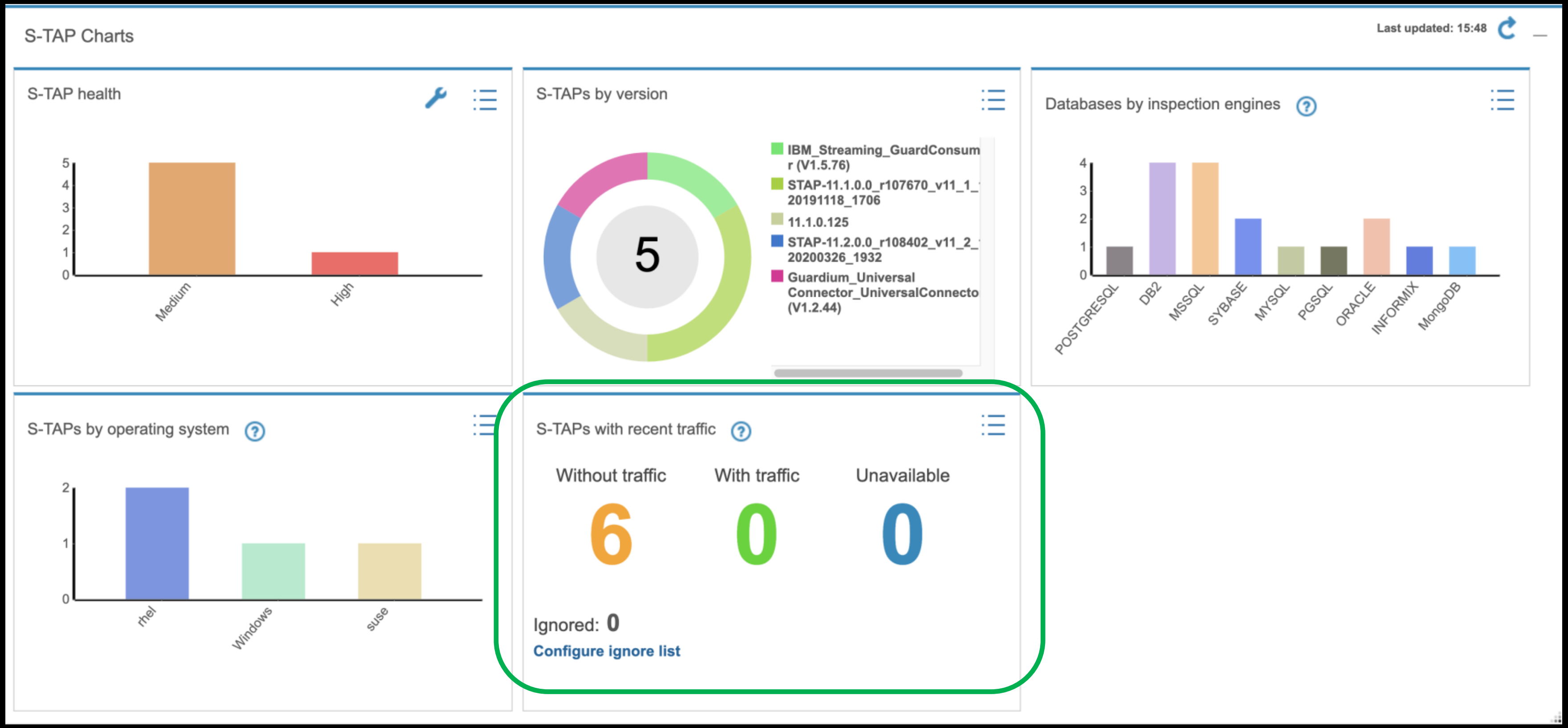
- Traffic status columns under S-TAP tab



	Hostname or IP address	Collector	Overall status	Connectivity	K-TAP status	Database status	Traffic status	Databases	Version
○	aws-rds-das-cluster-ONM5WL2O2O6BZGCQ4JSREAUSWE	drpt-id24.guard.swg.usma.ibm.com	🟠	🟢			🟠		Data stream V1.5.76
○	kal-rh68db03.guard.swg.usma.ibm.com	drpt-id24.guard.swg.usma.ibm.com	🔴	🟢	🔴	🔵	🟠		STAP-11.1.0.0_r107670_v11_1_1-20191118_1706
○	kal-rh68db01.guard.swg.usma.ibm.com	drpt-id24.guard.swg.usma.ibm.com	🟠	🟢	🟢	🔵	🟠		STAP-11.1.0.0_r107670_v11_1_1-20191118_1706
○	[redacted]	drpt-id24.guard.swg.usma.ibm.com	🟠	🟢		🔵	🟠	1	11.1.0.125
○	[redacted]	drpt-id24.guard.swg.usma.ibm.com	🟠	🟢	🟢	🔵	🟠	2	STAP-11.2.0.0_r108402_v11_2_1-20200326_1932
○	qa-db51:27017:UC1	drpt-id24.guard.swg.usma.ibm.com	🟠	🟢			🟠		Universal Connector V1.2.44

S-TAP Charts

- Charts which are part of this section: *S-TAP health, S-Taps by version, Databases by inspection engines, S-TAPs by operating system, S-TAPs with recent traffic (new)*
- S-TAPs with recent traffic chart shows the count of S-TAPs divided into with/without/unknown traffic
- User can also add S-TAPs to ignore list from this chart



S-TAP Charts
Last updated: 15:48
S-TAP health
5
4
3
2
1
0
Medium
High
S-TAPs by version
5
IBM_Streaming_GuardConsumr (V1.5.76)
STAP-11.1.0.0_r107670_v11_1_
20191118_1706
11.1.0.125
STAP-11.2.0.0_r108402_v11_2_
20200326_1932
Guardium_Universal Connector_UniversalConnecto (V1.2.44)
Databases by inspection engines
4
3
2
1
0
POSTGRESQL
DB2
MSSQL
SYBASE
MYSQL
PGSQL
ORACLE
INFORMIX
MongoDB
S-TAPs by operating system
2
1
0
rhel
Windows
suse

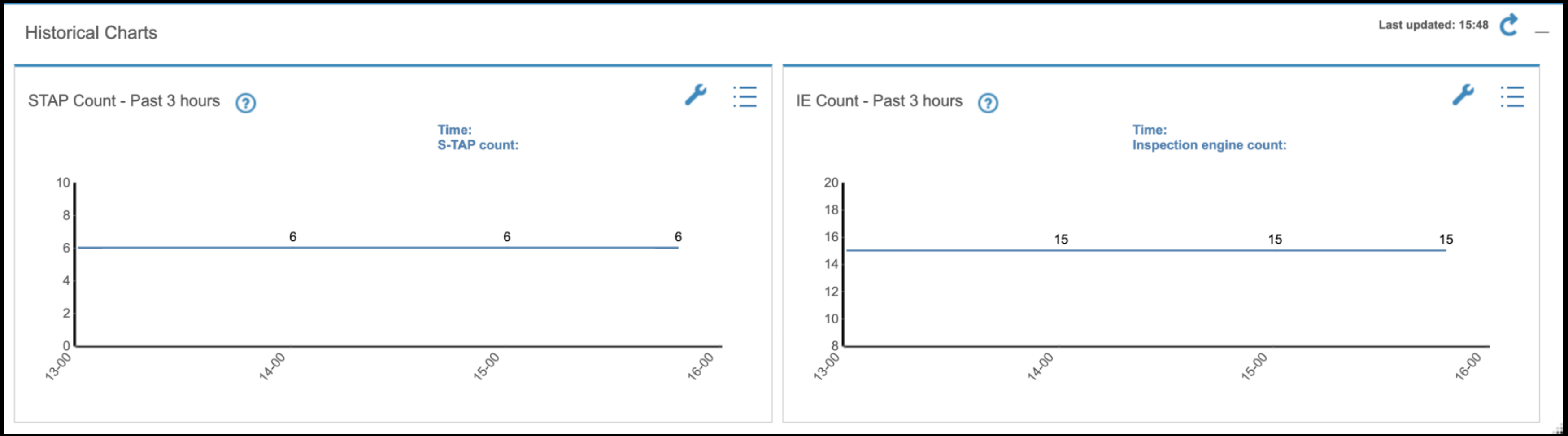
S-TAPs with recent traffic

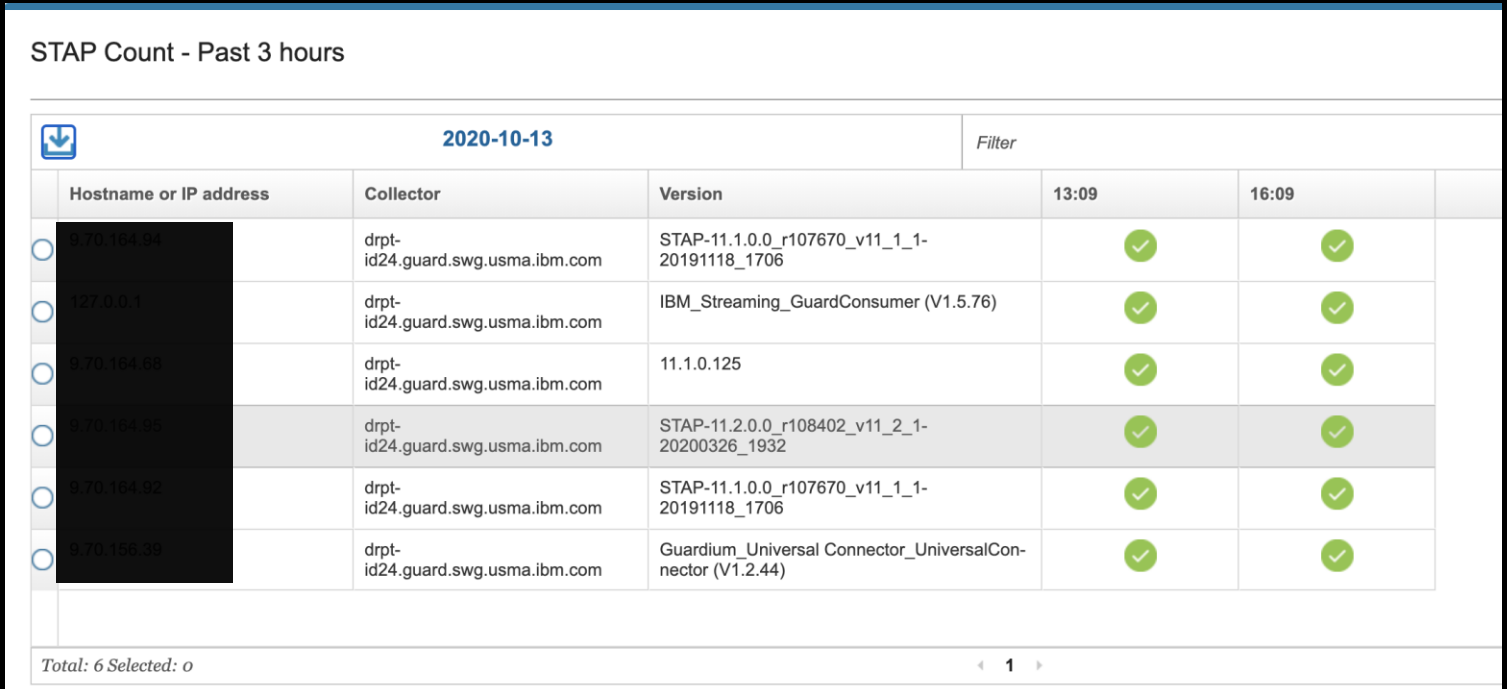
Without traffic	With traffic	Unavailable
6	0	0

Ignored: 0

Configure ignore list

Historical Charts





STAP Count - Past 3 hours

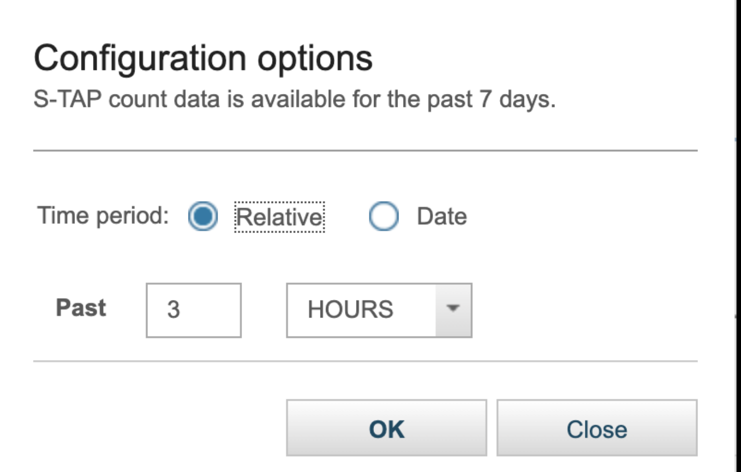
2020-10-13

Filter

	Hostname or IP address	Collector	Version	13:09	16:09
○	[redacted]	drpt-id24.guard.swg.usma.ibm.com	STAP-11.1.0.0_r107670_v11_1_1-20191118_1706	✓	✓
○	[redacted]	drpt-id24.guard.swg.usma.ibm.com	IBM_Streaming_GuardConsumer (V1.5.76)	✓	✓
○	[redacted]	drpt-id24.guard.swg.usma.ibm.com	11.1.0.125	✓	✓
○	[redacted]	drpt-id24.guard.swg.usma.ibm.com	STAP-11.2.0.0_r108402_v11_2_1-20200326_1932	✓	✓
○	[redacted]	drpt-id24.guard.swg.usma.ibm.com	STAP-11.1.0.0_r107670_v11_1_1-20191118_1706	✓	✓
○	[redacted]	drpt-id24.guard.swg.usma.ibm.com	Guardium_Universal Connector_UniversalConnector (V1.2.44)	✓	✓

Total: 6 Selected: 0

‹ 1 ›



Configuration options

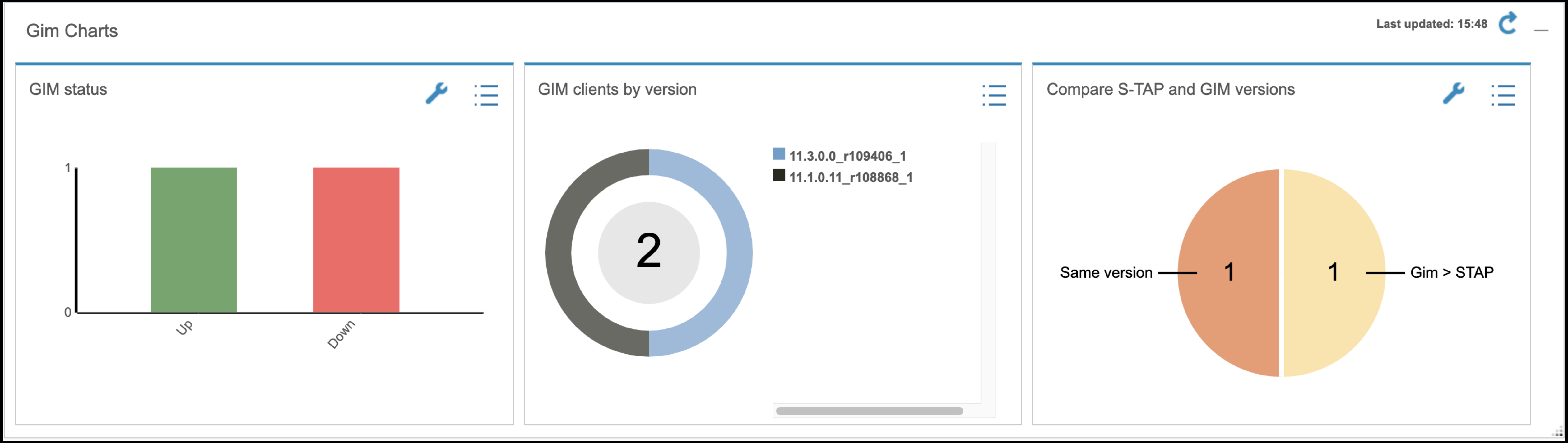
S-TAP count data is available for the past 7 days.

Time period: ● Relative ○ Date

Past 3 HOURS

GIM Charts

- Compare S-TAP and GIM versions is the new chart where we compare GIM and S-TAP versions to indicate whether both are same, either one of them is greater than other
- This section will only work or have information if the Central Manager is the GIM server. If the Central Manager is not a GIM server then this section will not be available

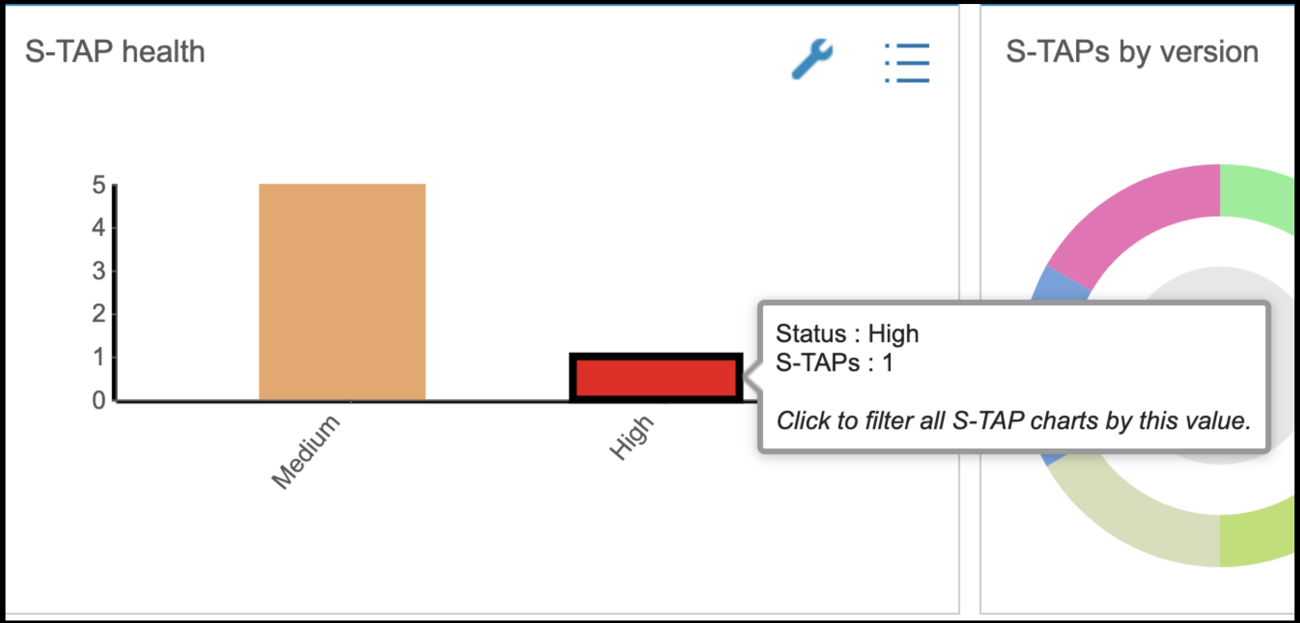


Filtering across tiles

This is a new feature we introduced where the user can click on a chart in particular section and all the other charts in that section will be filtered accordingly

For example, the user notices that there are 2 S-TAPs with red status on the S-TAP Health chart, the user can click on the red bar and all other charts in that section will filter to display only the information related to those 2 S-TAPs

This filter is available for all charts belonging to S-TAP and GIM charts section



Status : High
S-TAPs : 1

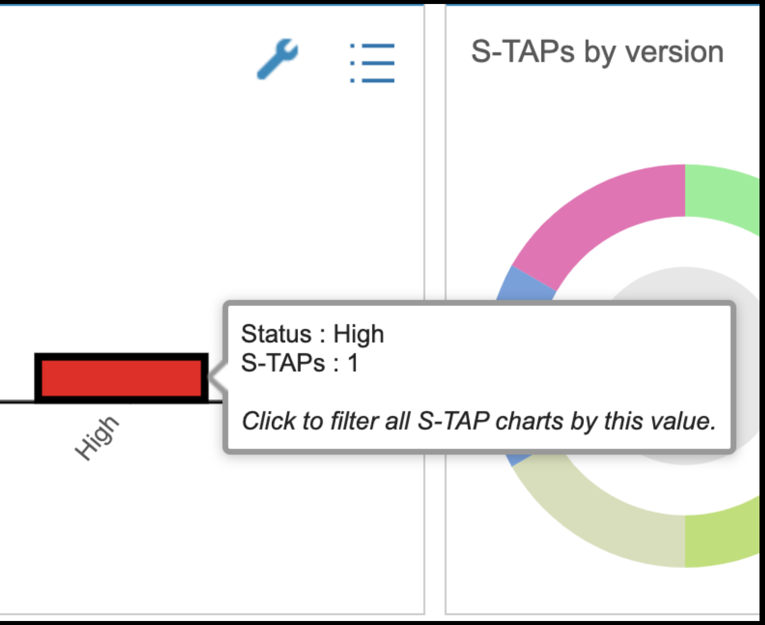
Click to filter all S-TAP charts by this value.

Filtering across tiles

This is a new feature we introduced where the user can click on a chart in particular section and all the other charts in that section will be filtered accordingly

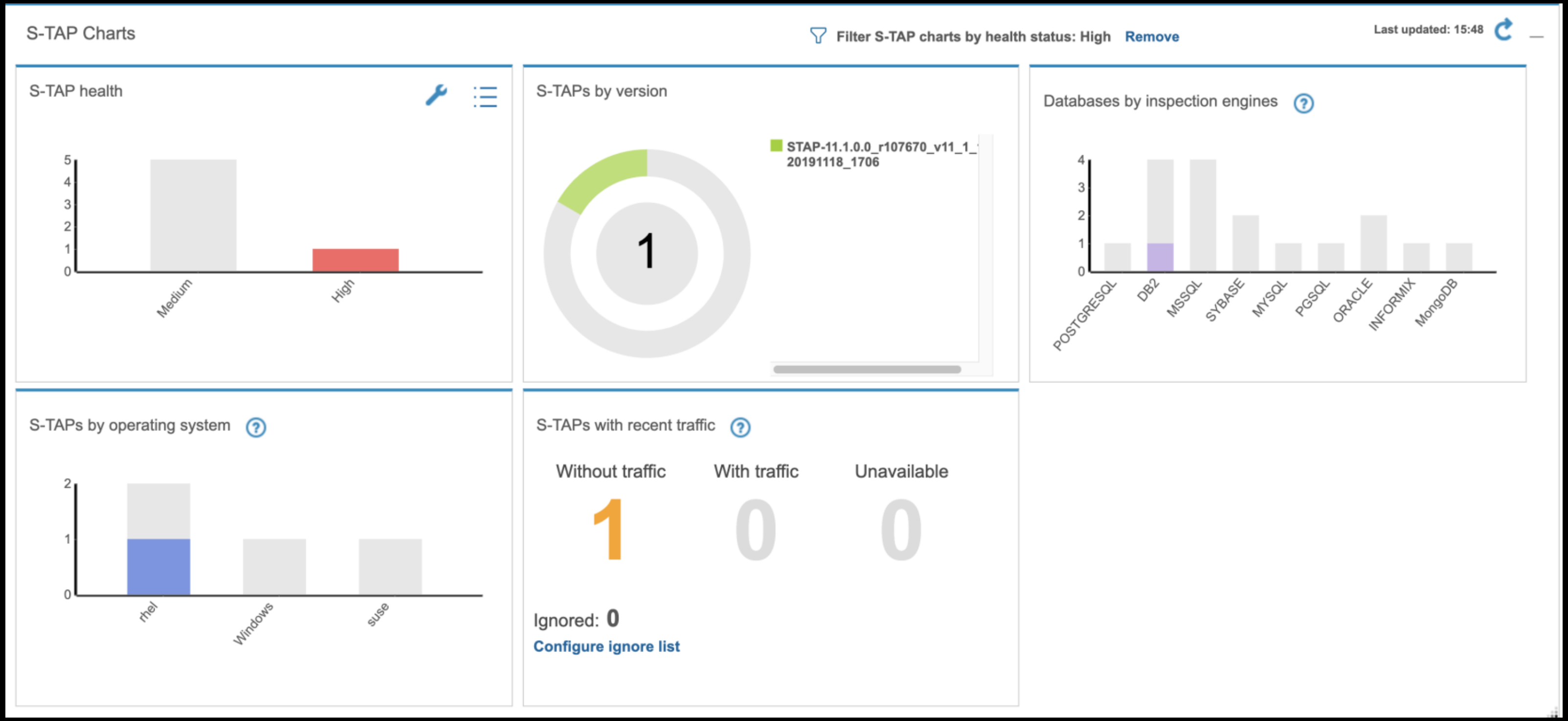
For example, the user notices that there are 2 S-TAPs with red status on the S-TAP Health chart, the user can click on the red bar and all other charts in that section will filter to display only the information related to those 2 S-TAPs

This filter is available for all charts belonging to S-TAP and GIM charts section



Status : High
S-TAPs : 1

Click to filter all S-TAP charts by this value.

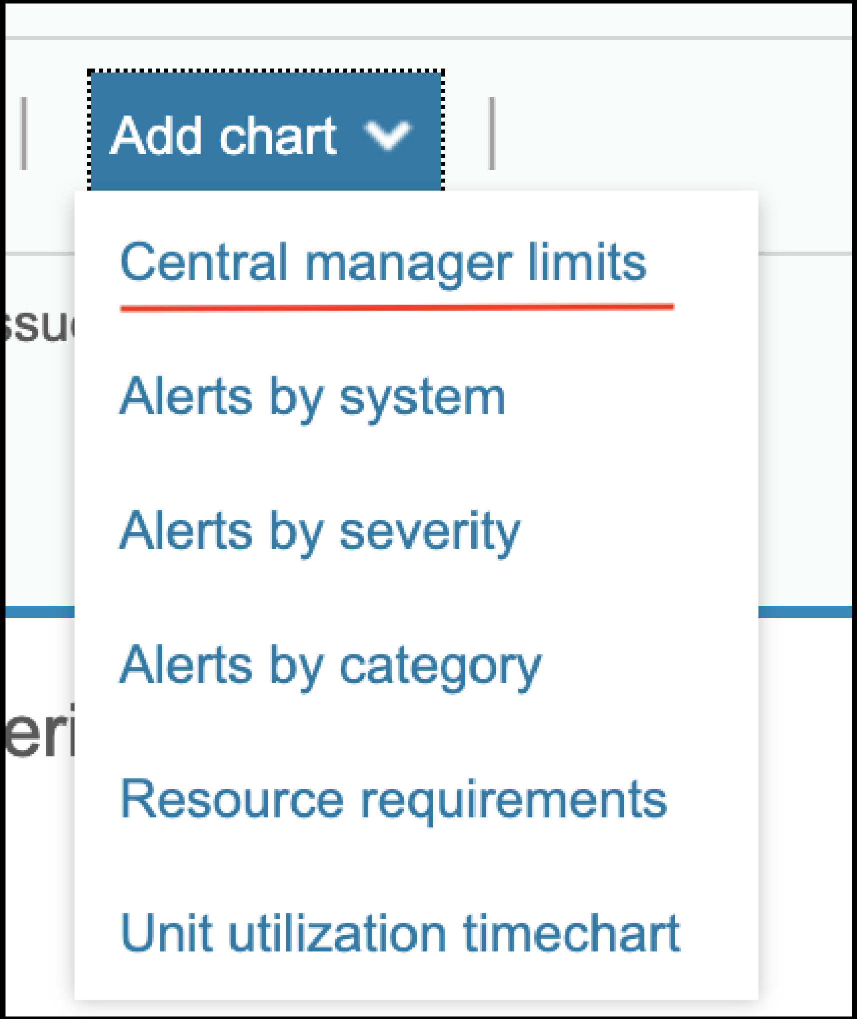


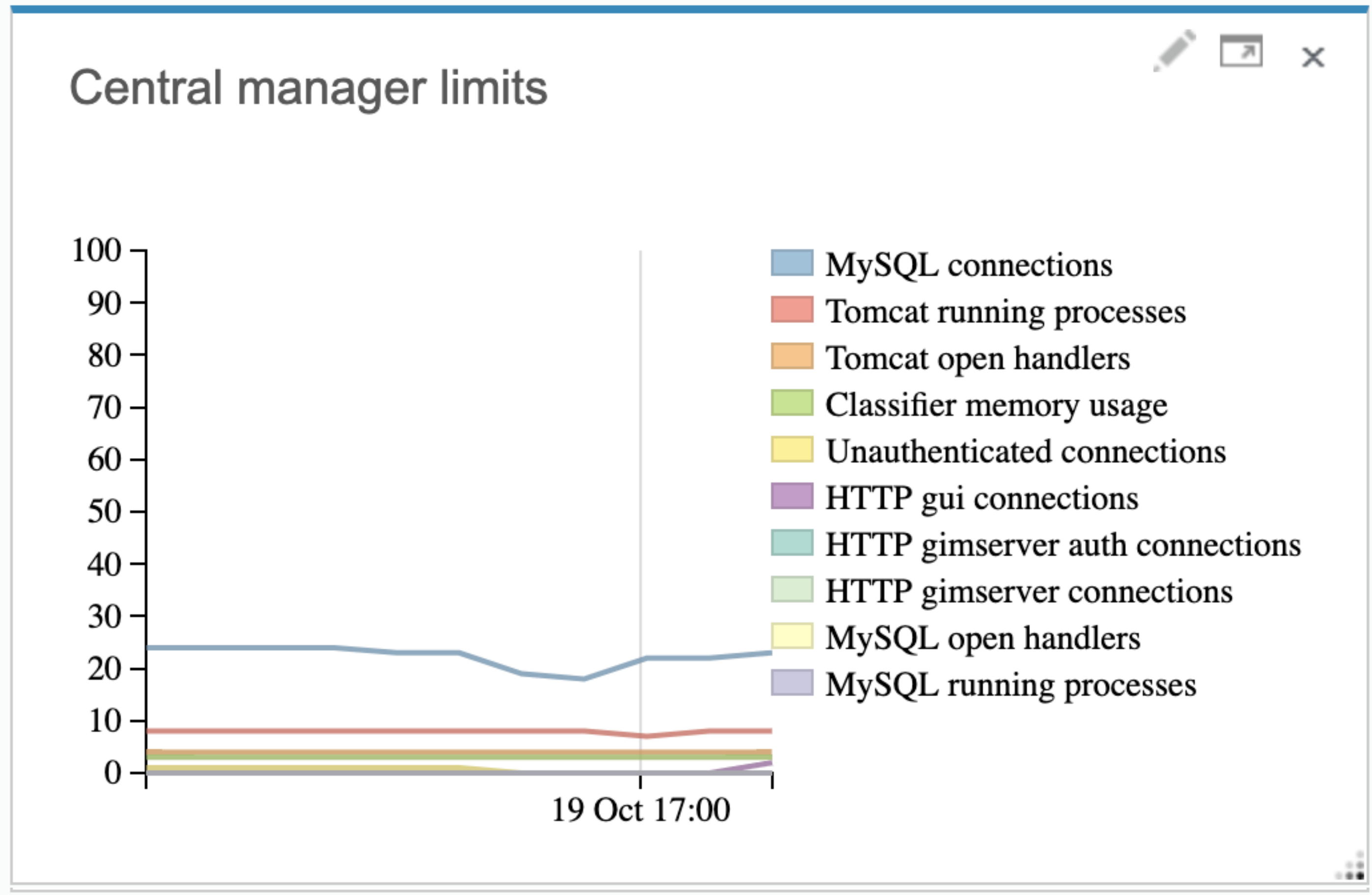
Filter S-TAP charts by health status: High Remove

Without traffic	With traffic	Unavailable
1	0	0

Ignored: 0

Central manager limits chart



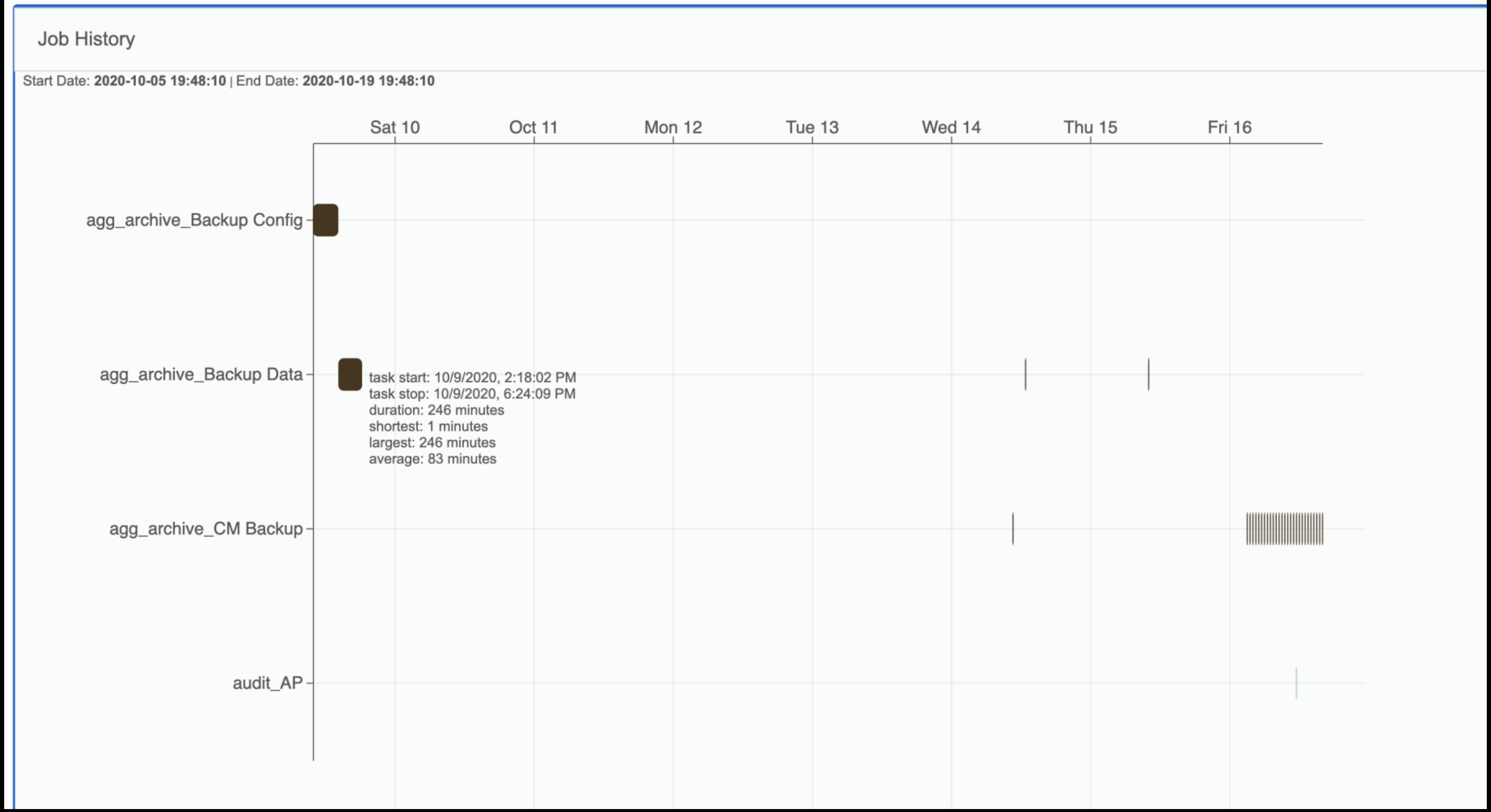


Job history - Gantt Chart

Shows scheduled jobs like datamart, aggregation and audit process

Available on CM, Aggregator and MU’s

Y-axis shows job type with name, x-axis shows the time range



Job History

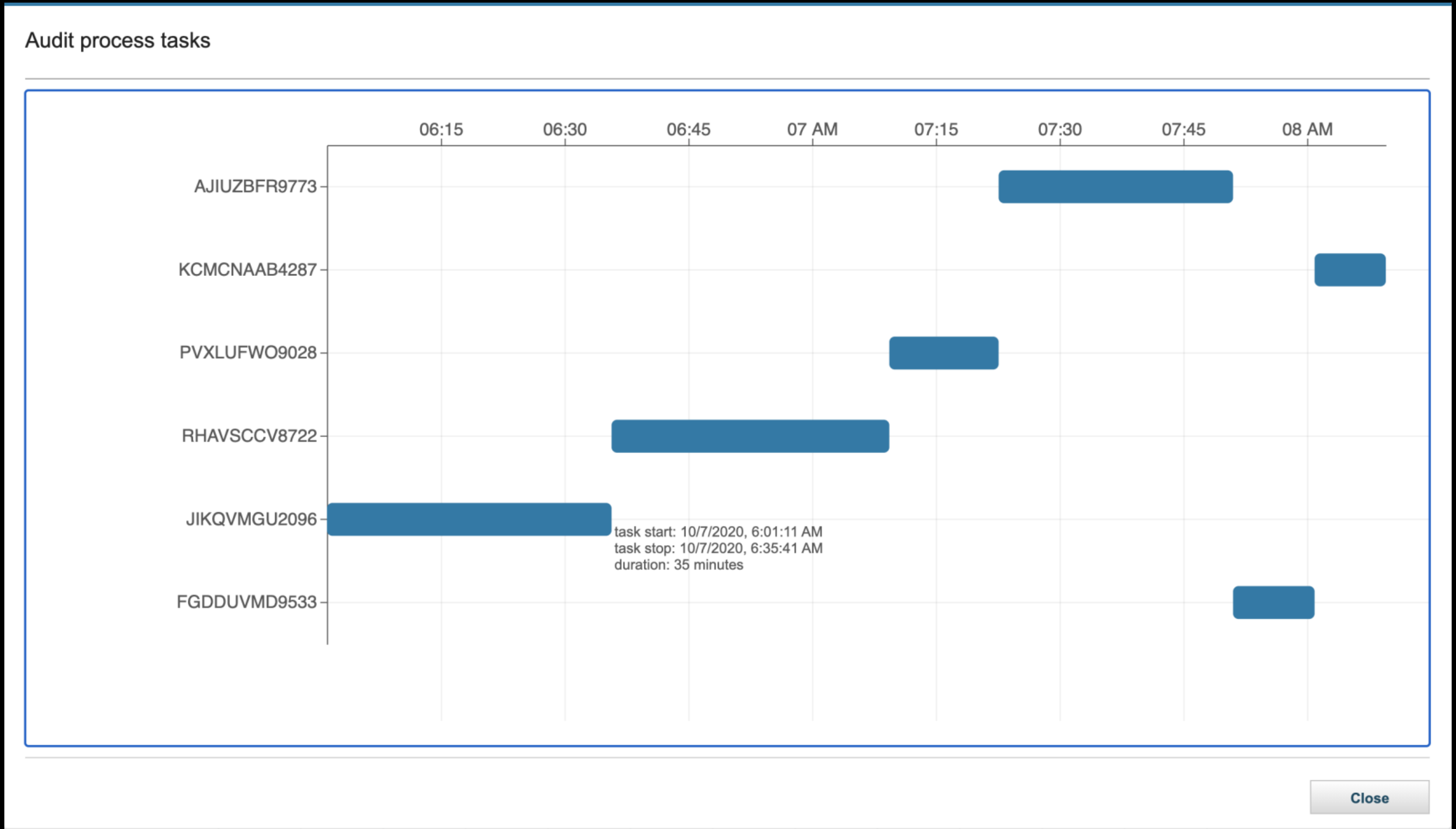
Start Date: **2020-10-05 19:48:10** | End Date: **2020-10-19 19:48:10**

task start: 10/9/2020, 2:18:02 PM
task stop: 10/9/2020, 6:24:09 PM
duration: 246 minutes
shortest: 1 minutes
largest: 246 minutes
average: 83 minutes

Audit Process - Gantt Chart

Audit process jobs show the drill down of the associated tasks

On hover, task start and stop time along with duration are displayed



task start: 10/7/2020, 6:01:11 AM
task stop: 10/7/2020, 6:35:41 AM
duration: 35 minutes

Policy Tagging

Most compliance regulations are very similar. However, we currently create template policies for individual regulations. This results in lots of rule duplication.

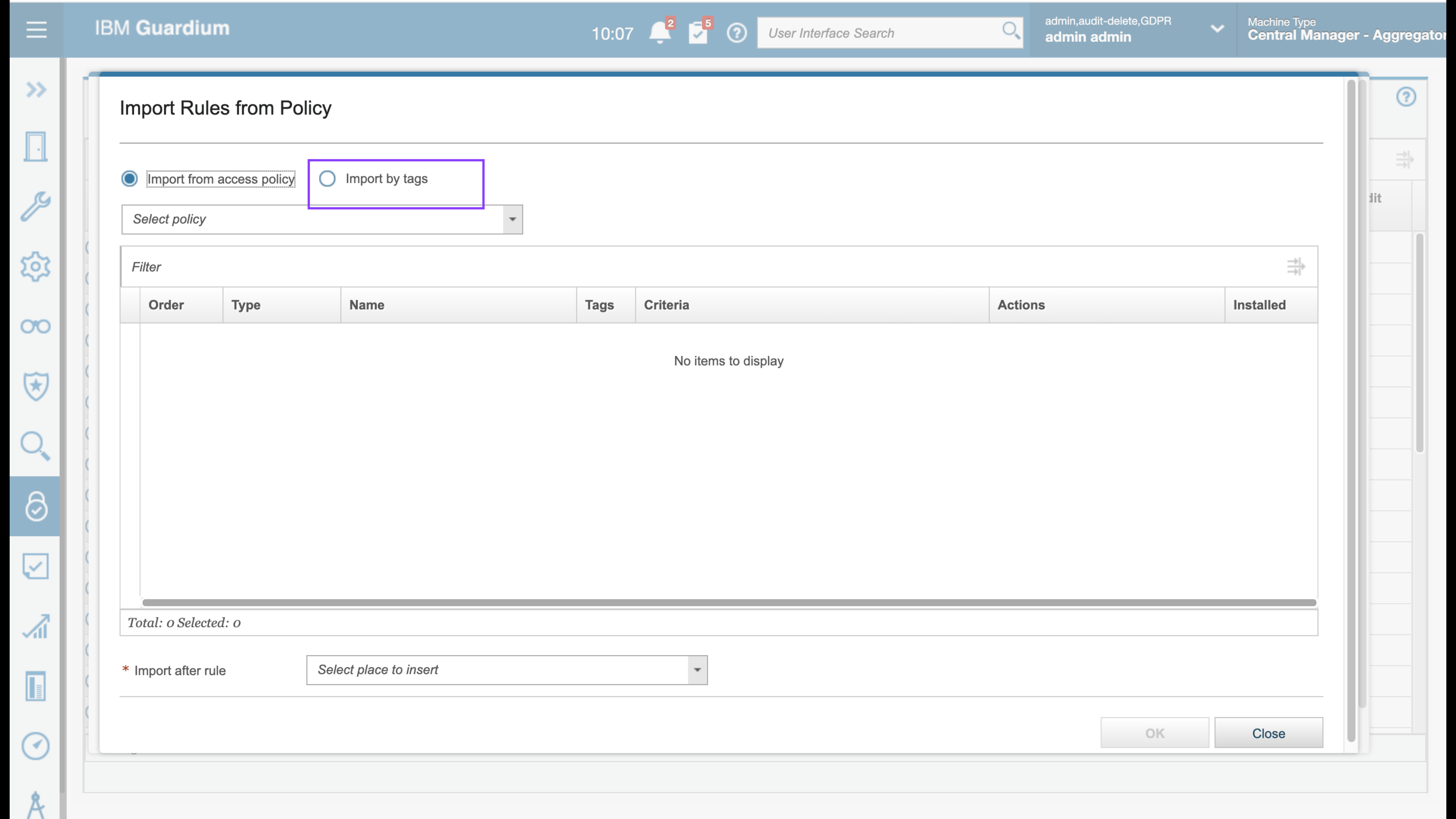
With this feature, new compliance regulations will be supported by **adding tags to existing** out-of-the box rules. (where possible).This enables us to support new regulations more quickly.

What's New

- Out of the box tags for compliance regulations
- Tagging supported for DAM policy rules

Benefits

- Ability to easily create policies that support multiple regulations
- Less wait for new regulation support
- Can create your own tags for version, geo, etc.
- Less "clutter" in the UI



Import Rules from Policy

● Import from access policy ○ Import by tags

Select policy

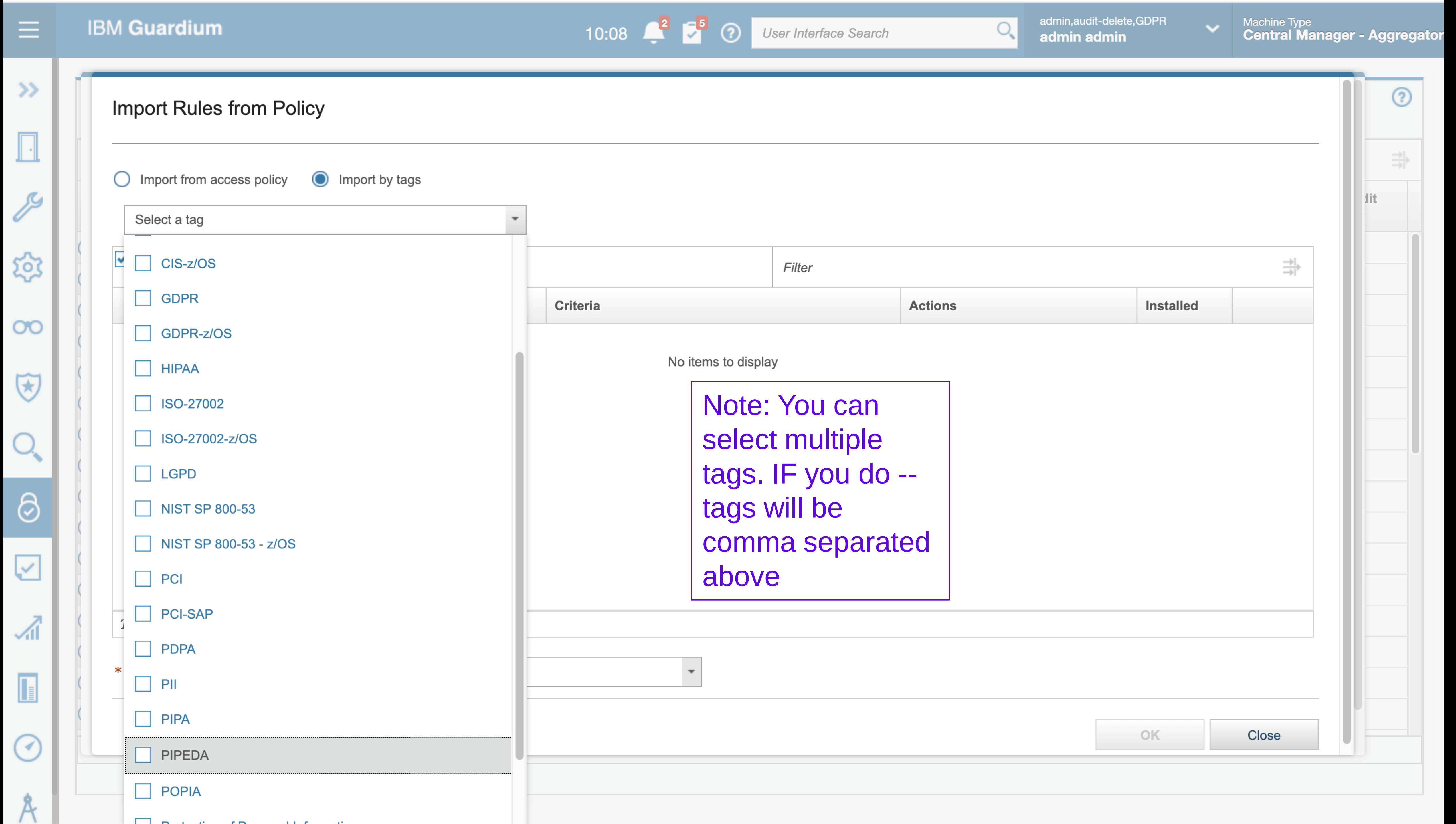
Filter

Order	Type	Name	Tags	Criteria	Actions	Installed

No items to display

Total: 0 Selected: 0

* Import after rule: Select place to insert



Import Rules from Policy

○ Import from access policy ● Import by tags

Select a tag

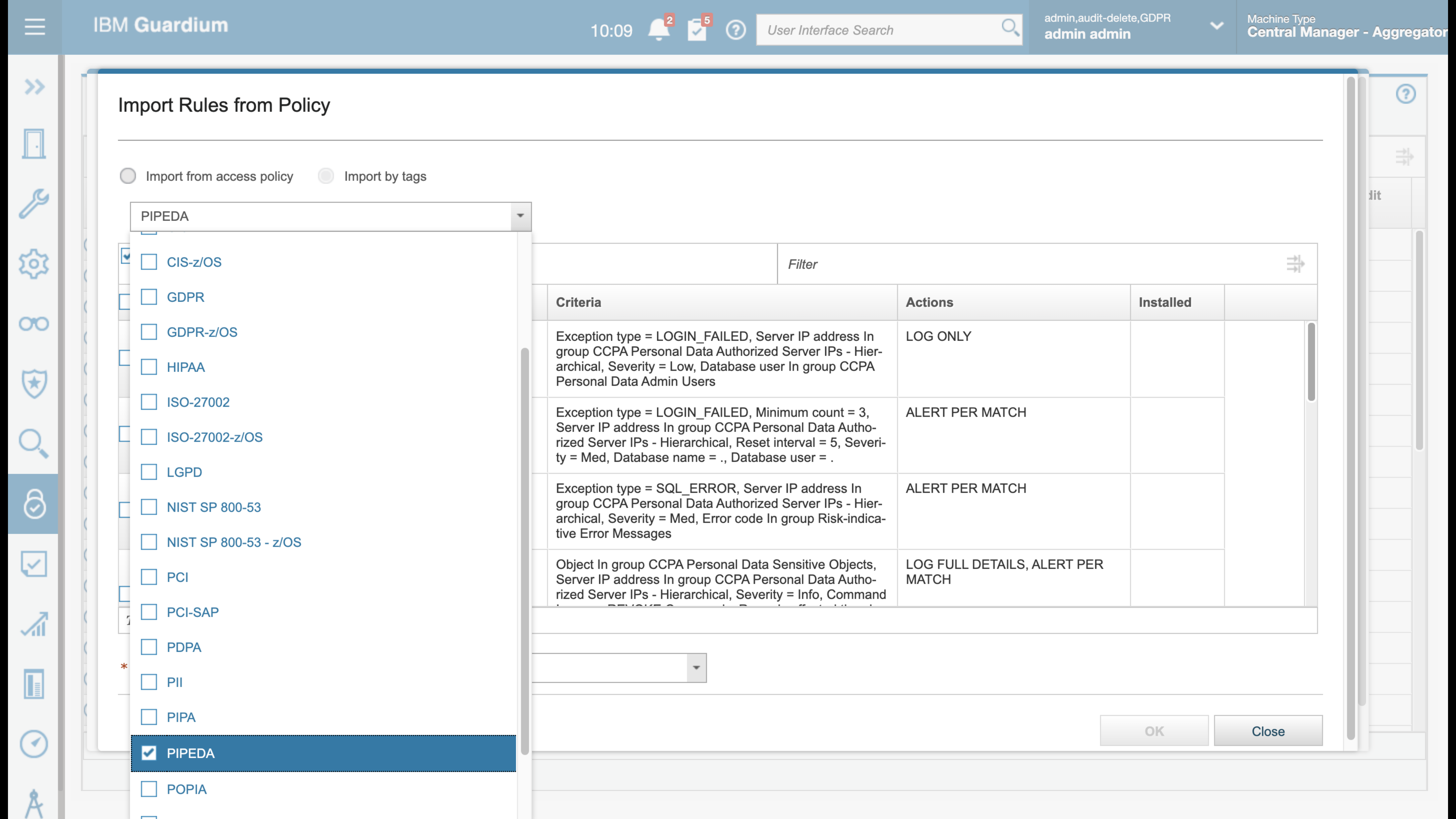
- □ CIS-z/OS
- □ GDPR
- □ GDPR-z/OS
- □ HIPAA
- □ ISO-27002
- □ ISO-27002-z/OS
- □ LGPD
- □ NIST SP 800-53
- □ NIST SP 800-53 - z/OS
- □ PCI
- □ PCI-SAP
- □ PDPA
- □ PII
- □ PIPA
- □ PIPEDA
- □ POPIA

Filter

Criteria	Actions	Installed

No items to display

Note: You can select multiple tags. IF you do -- tags will be comma separated above

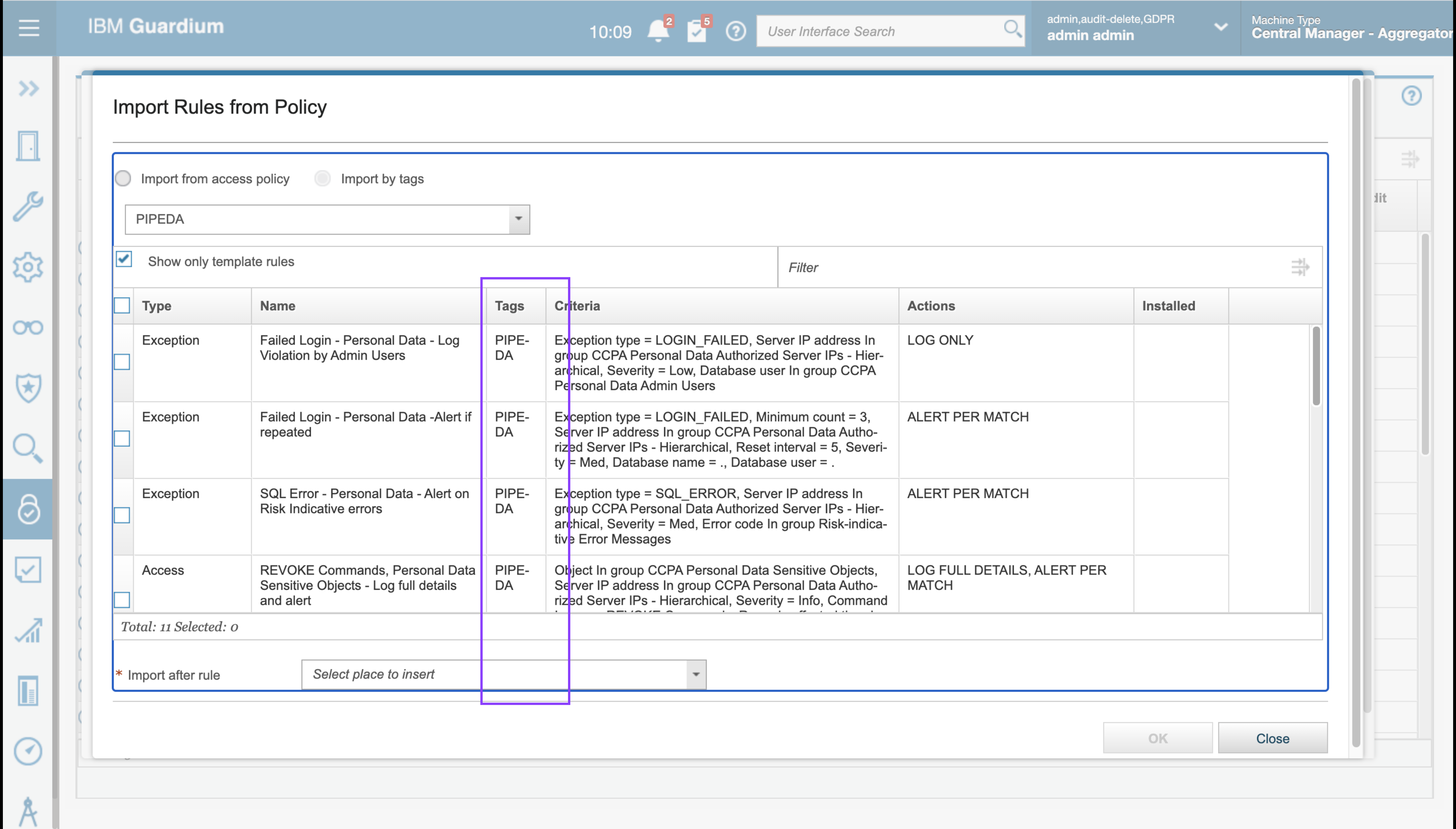


Import Rules from Policy

○ Import from access policy ○ Import by tags

PIPEDA

Criteria	Actions	Installed
Exception type = LOGIN_FAILED, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Low, Database user In group CCPA Personal Data Admin Users	LOG ONLY	
Exception type = LOGIN_FAILED, Minimum count = 3, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Reset interval = 5, Severity = Med, Database name = ., Database user = .	ALERT PER MATCH	
Exception type = SQL_ERROR, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Med, Error code In group Risk-indicative Error Messages	ALERT PER MATCH	
Object In group CCPA Personal Data Sensitive Objects, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Info, Command	LOG FULL DETAILS, ALERT PER MATCH	



Import Rules from Policy

○ Import from access policy ○ Import by tags

PIPEDA

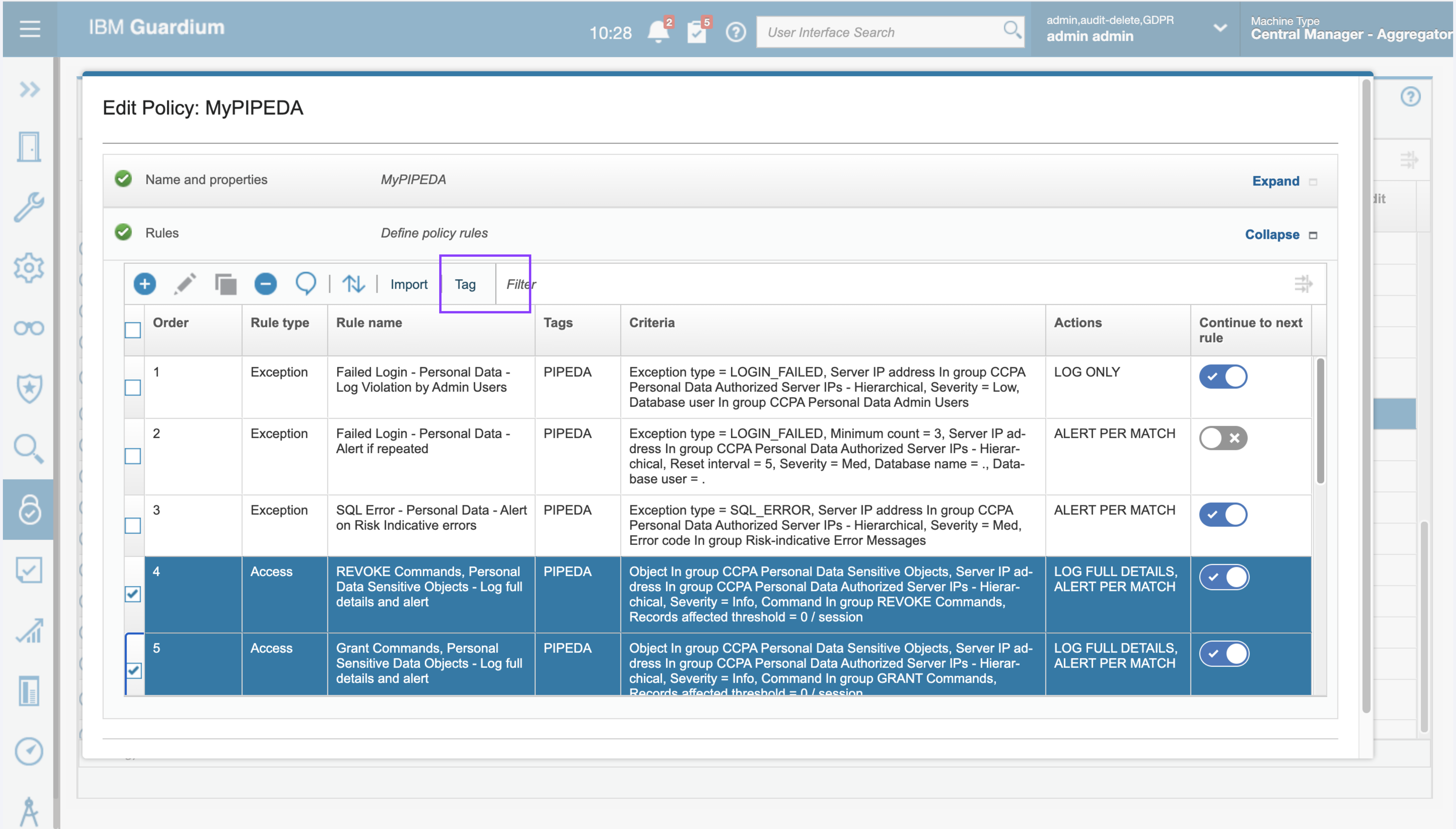
☑ Show only template rules

Filter

□	Type	Name	Tags	Criteria	Actions	Installed
□	Exception	Failed Login - Personal Data - Log Violation by Admin Users	PIPEDA	Exception type = LOGIN_FAILED, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Low, Database user In group CCPA Personal Data Admin Users	LOG ONLY	
□	Exception	Failed Login - Personal Data -Alert if repeated	PIPEDA	Exception type = LOGIN_FAILED, Minimum count = 3, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Reset interval = 5, Severity = Med, Database name = ., Database user = .	ALERT PER MATCH	
□	Exception	SQL Error - Personal Data - Alert on Risk Indicative errors	PIPEDA	Exception type = SQL_ERROR, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Med, Error code In group Risk-indicative Error Messages	ALERT PER MATCH	
□	Access	REVOKE Commands, Personal Data Sensitive Objects - Log full details and alert	PIPEDA	Object In group CCPA Personal Data Sensitive Objects, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Info, Command	LOG FULL DETAILS, ALERT PER MATCH	

Total: 11 Selected: 0

* Import after rule: *Select place to insert*

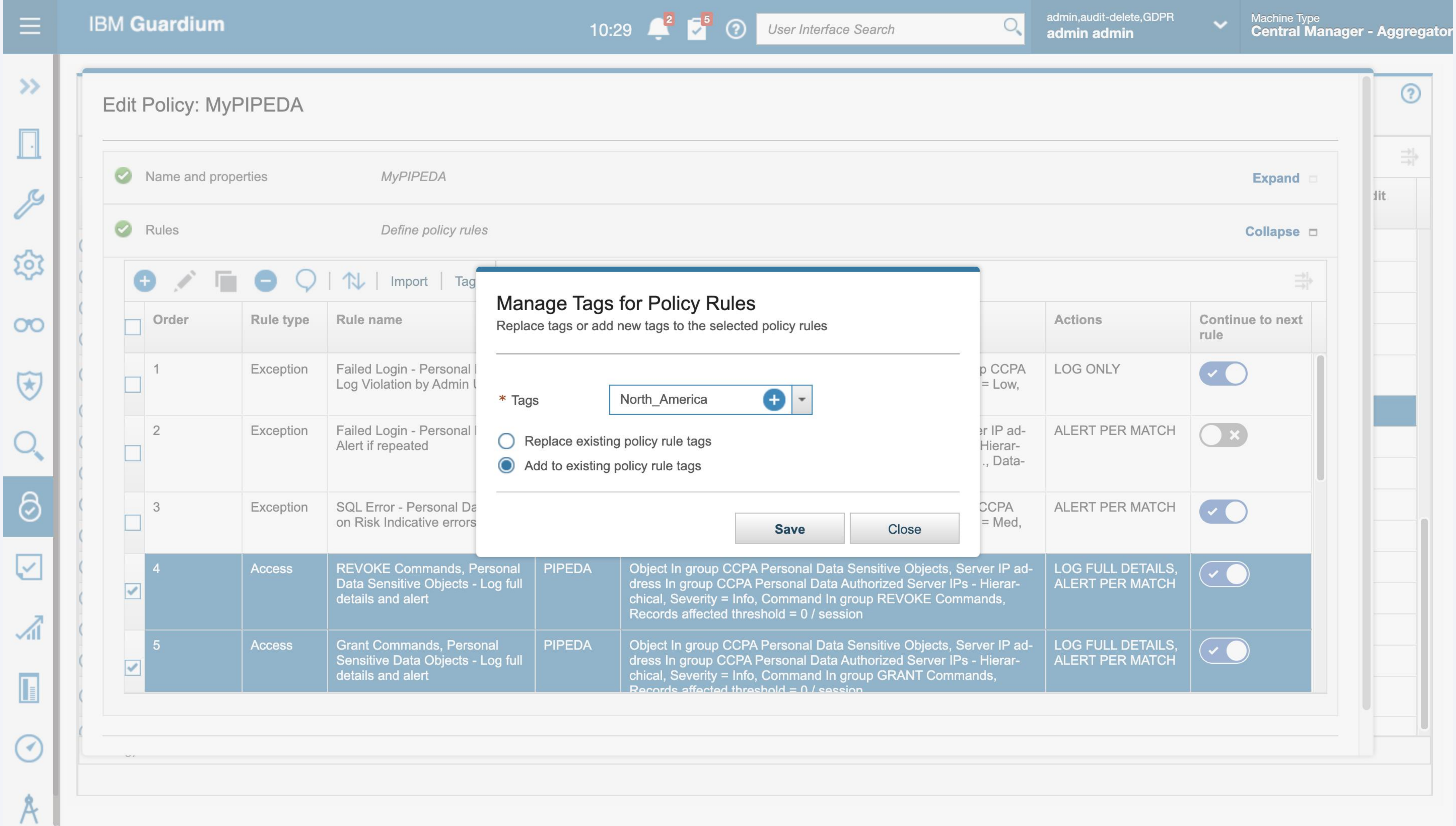


Edit Policy: MyPIPEDA

Name and properties *MyPIPEDA* **Expand**

Rules *Define policy rules* **Collapse**

□	Order	Rule type	Rule name	Tags	Criteria	Actions	Continue to next rule
□	1	Exception	Failed Login - Personal Data - Log Violation by Admin Users	PIPEDA	Exception type = LOGIN_FAILED, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Low, Database user In group CCPA Personal Data Admin Users	LOG ONLY	✓
□	2	Exception	Failed Login - Personal Data - Alert if repeated	PIPEDA	Exception type = LOGIN_FAILED, Minimum count = 3, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Reset interval = 5, Severity = Med, Database name = ., Database user = .	ALERT PER MATCH	✕
□	3	Exception	SQL Error - Personal Data - Alert on Risk Indicative errors	PIPEDA	Exception type = SQL_ERROR, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Med, Error code In group Risk-indicative Error Messages	ALERT PER MATCH	✓
☑	4	Access	REVOKE Commands, Personal Data Sensitive Objects - Log full details and alert	PIPEDA	Object In group CCPA Personal Data Sensitive Objects, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Info, Command In group REVOKE Commands, Records affected threshold = 0 / session	LOG FULL DETAILS, ALERT PER MATCH	✓
☑	5	Access	Grant Commands, Personal Sensitive Data Objects - Log full details and alert	PIPEDA	Object In group CCPA Personal Data Sensitive Objects, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Info, Command In group GRANT Commands, Records affected threshold = 0 / session	LOG FULL DETAILS, ALERT PER MATCH	✓



Edit Policy: MyPIPEDA

✓ Name and properties *MyPIPEDA* Expand

✓ Rules *Define policy rules* Collapse

Manage Tags for Policy Rules

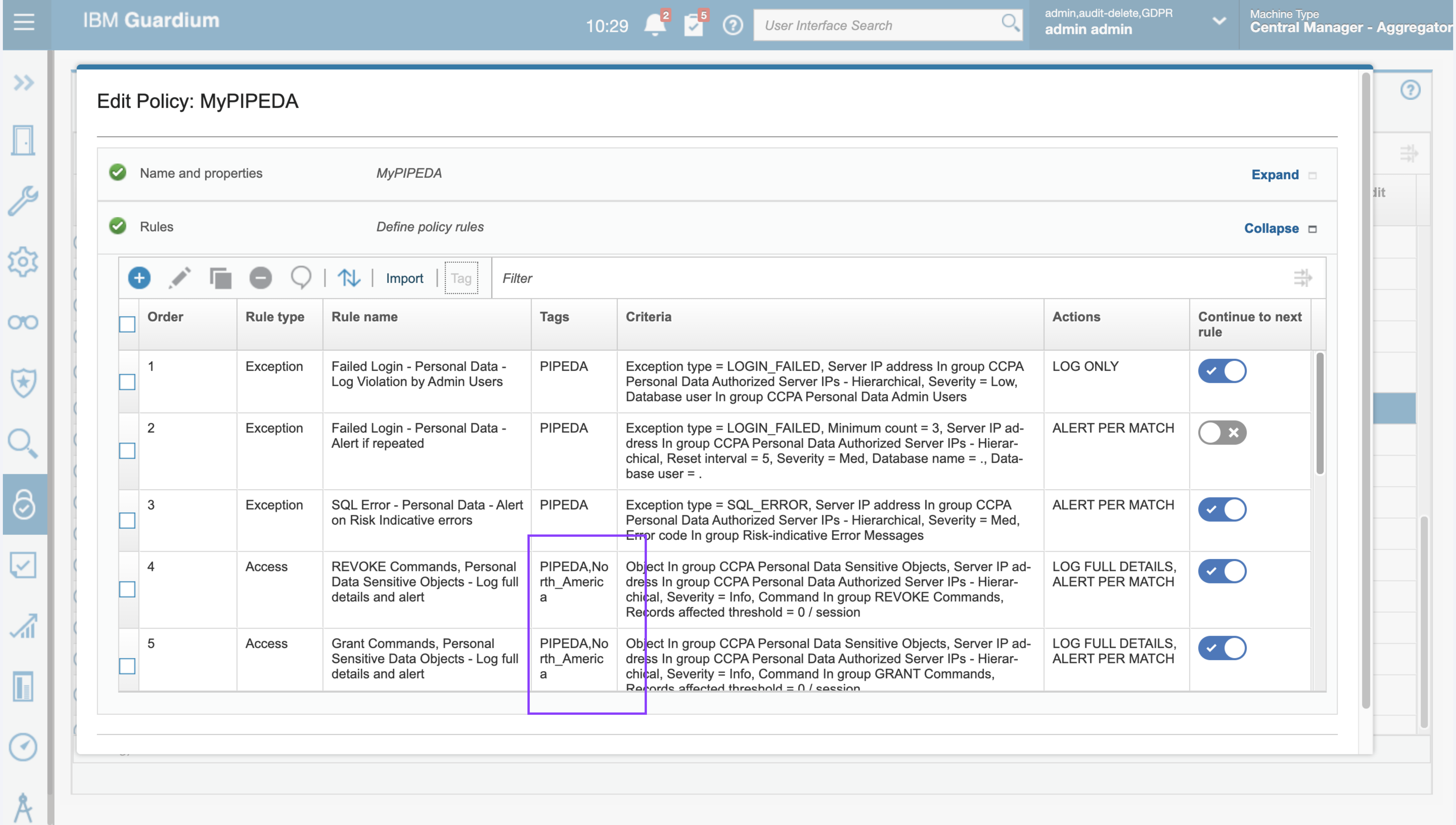
Replace tags or add new tags to the selected policy rules

* Tags: North_America

○ Replace existing policy rule tags

● Add to existing policy rule tags

□	Order	Rule type	Rule name			Actions	Continue to next rule
□	1	Exception	Failed Login - Personal I Log Violation by Admin U		p CCPA = Low,	LOG ONLY	✓
□	2	Exception	Failed Login - Personal I Alert if repeated		er IP ad- Hierar- ., Data-	ALERT PER MATCH	✗
□	3	Exception	SQL Error - Personal Da on Risk Indicative errors		CCPA = Med,	ALERT PER MATCH	✓
☑	4	Access	REVOKE Commands, Personal Data Sensitive Objects - Log full details and alert	PIPEDA	Object In group CCPA Personal Data Sensitive Objects, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Info, Command In group REVOKE Commands, Records affected threshold = 0 / session	LOG FULL DETAILS, ALERT PER MATCH	✓
☑	5	Access	Grant Commands, Personal Sensitive Data Objects - Log full details and alert	PIPEDA	Object In group CCPA Personal Data Sensitive Objects, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Info, Command In group GRANT Commands, Records affected threshold = 0 / session	LOG FULL DETAILS, ALERT PER MATCH	✓



Edit Policy: MyPIPEDA

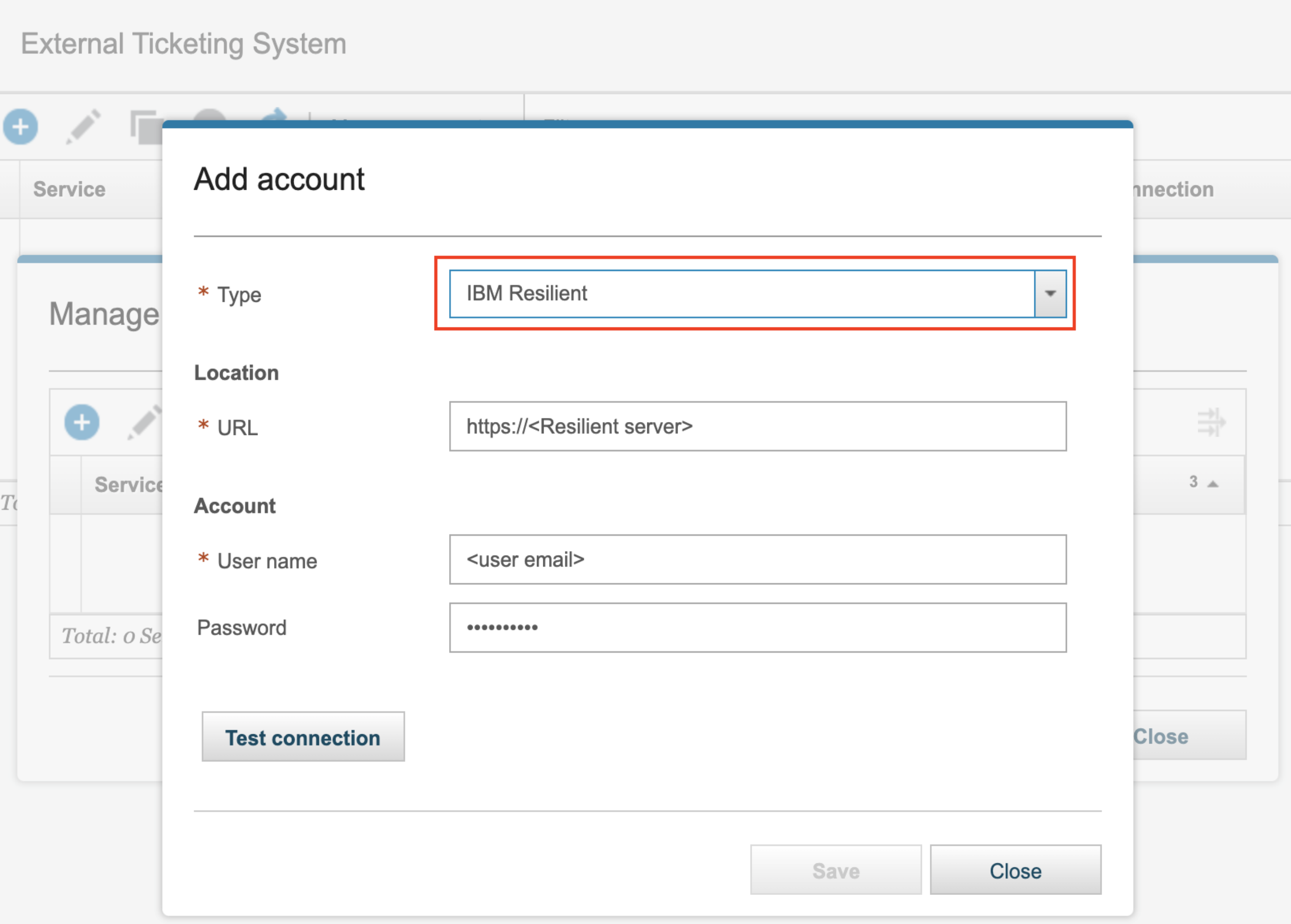
Name and properties — *MyPIPEDA* — Expand

Rules — *Define policy rules* — Collapse

☐	Order	Rule type	Rule name	Tags	Criteria	Actions	Continue to next rule
☐	1	Exception	Failed Login - Personal Data - Log Violation by Admin Users	PIPEDA	Exception type = LOGIN_FAILED, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Low, Database user In group CCPA Personal Data Admin Users	LOG ONLY	✓
☐	2	Exception	Failed Login - Personal Data - Alert if repeated	PIPEDA	Exception type = LOGIN_FAILED, Minimum count = 3, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Reset interval = 5, Severity = Med, Database name = ., Database user = .	ALERT PER MATCH	✕
☐	3	Exception	SQL Error - Personal Data - Alert on Risk Indicative errors	PIPEDA	Exception type = SQL_ERROR, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Med, Error code In group Risk-indicative Error Messages	ALERT PER MATCH	✓
☐	4	Access	REVOKE Commands, Personal Data Sensitive Objects - Log full details and alert	PIPEDA,North_America	Object In group CCPA Personal Data Sensitive Objects, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Info, Command In group REVOKE Commands, Records affected threshold = 0 / session	LOG FULL DETAILS, ALERT PER MATCH	✓
☐	5	Access	Grant Commands, Personal Sensitive Data Objects - Log full details and alert	PIPEDA,North_America	Object In group CCPA Personal Data Sensitive Objects, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Info, Command In group GRANT Commands, Records affected threshold = 0 / session	LOG FULL DETAILS, ALERT PER MATCH	✓

Resilient support for ticketing

In v11.3, Guardium supports creating external tickets with IBM Resilient



Add account

* Type: IBM Resilient

Location

* URL: https://<Resilient server>

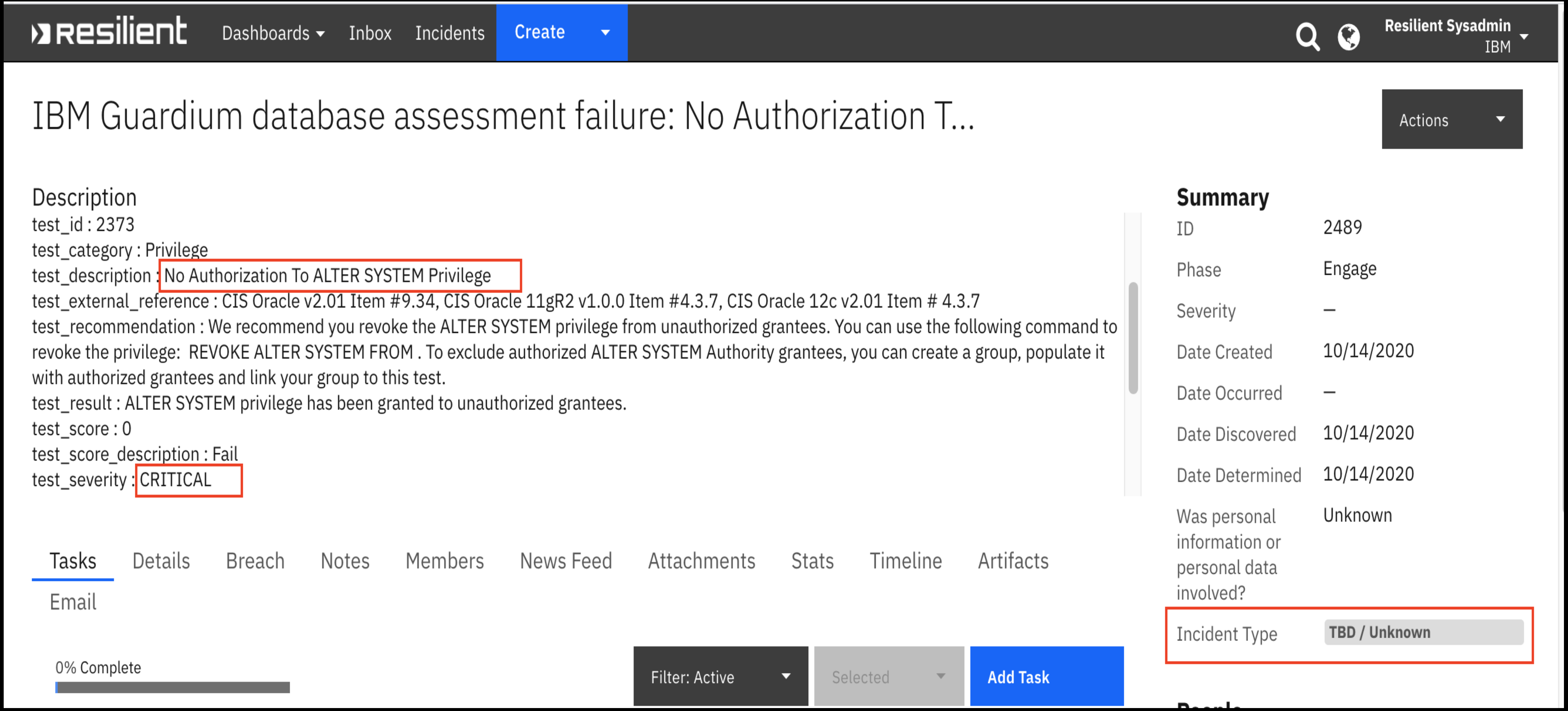
Account

* User name: <user email>

Password: ••••••••••

Resilient support for ticketing

Click on the link to open the IBM Resilient ticket on Resilient host



IBM Guardium database assessment failure: No Authorization T...

Description

test_id : 2373
test_category : Privilege
test_description : No Authorization To ALTER SYSTEM Privilege
test_external_reference : CIS Oracle v2.01 Item #9.34, CIS Oracle 11gR2 v1.0.0 Item #4.3.7, CIS Oracle 12c v2.01 Item # 4.3.7
test_recommendation : We recommend you revoke the ALTER SYSTEM privilege from unauthorized grantees. You can use the following command to revoke the privilege: REVOKE ALTER SYSTEM FROM . To exclude authorized ALTER SYSTEM Authority grantees, you can create a group, populate it with authorized grantees and link your group to this test.
test_result : ALTER SYSTEM privilege has been granted to unauthorized grantees.
test_score : 0
test_score_description : Fail
test_severity : CRITICAL

Summary

ID	2489
Phase	Engage
Severity	–
Date Created	10/14/2020
Date Occurred	–
Date Discovered	10/14/2020
Date Determined	10/14/2020
Was personal information or personal data involved?	Unknown
Incident Type	TBD / Unknown

Integration with Venafi

This new feature provides a framework to manage third-party Certificate Management System. Venafi is the first CMS platform that we support.

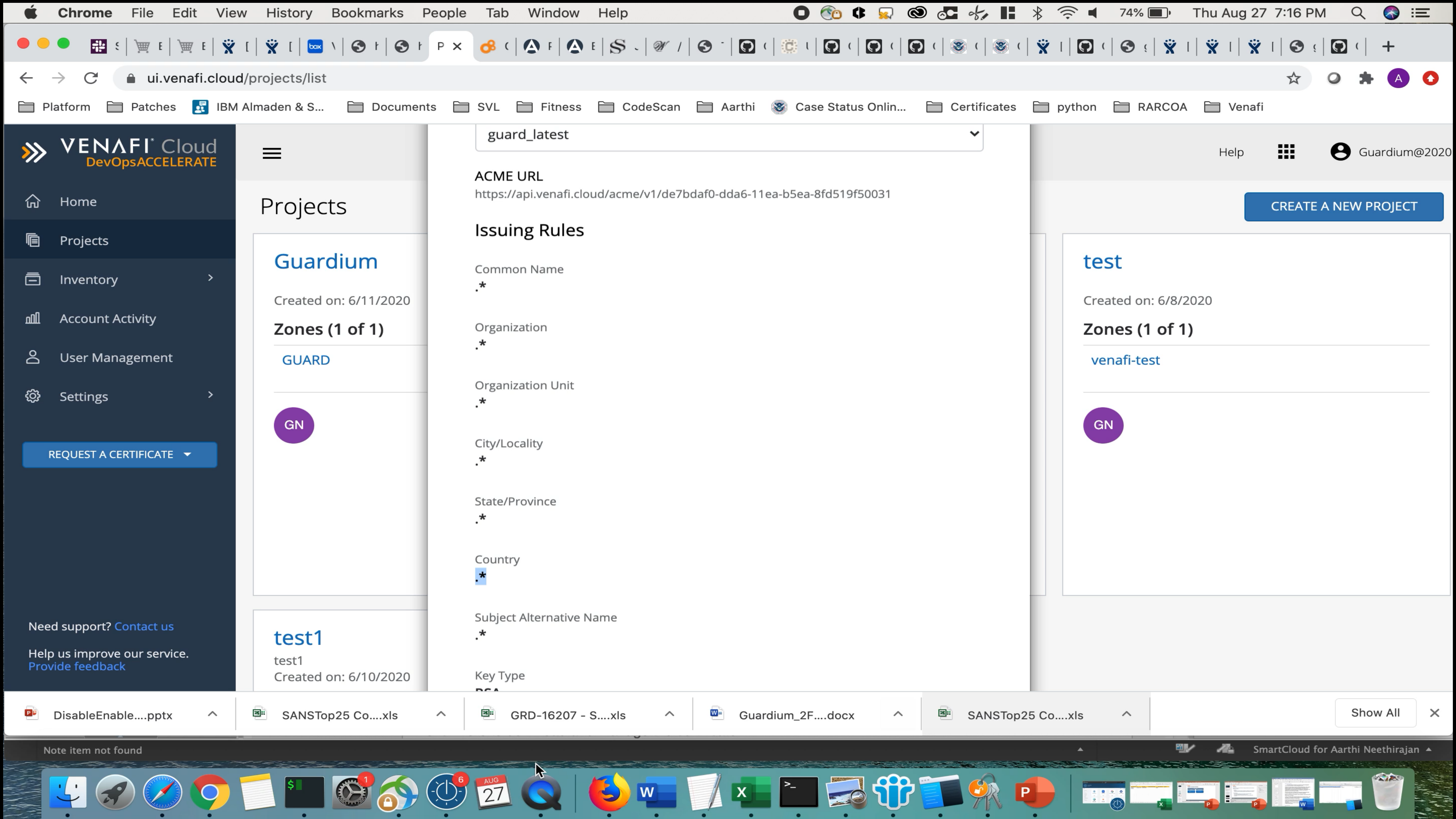
The current cycle of issue-renew of certificates in Guardium can be automated.

What’s New

- Ability to support a third-party Certificate Management system.

Benefits

- Provide framework to support external certificate management system.
- Automatically store certificates in all MU’s.
- Automatically renew certificates if expiring.



Projects

Guardium

Created on: 6/11/2020

Zones (1 of 1)

GUARD

GN

test1

test1

Created on: 6/10/2020

test

Created on: 6/8/2020

Zones (1 of 1)

venafi-test

GN

guard_latest

ACME URL

https://api.venafi.cloud/acme/v1/de7bdaf0-dda6-11ea-b5ea-8fd519f50031

Issuing Rules

Common Name

.*

Organization

.*

Organization Unit

.*

City/Locality

.*

State/Province

.*

Country

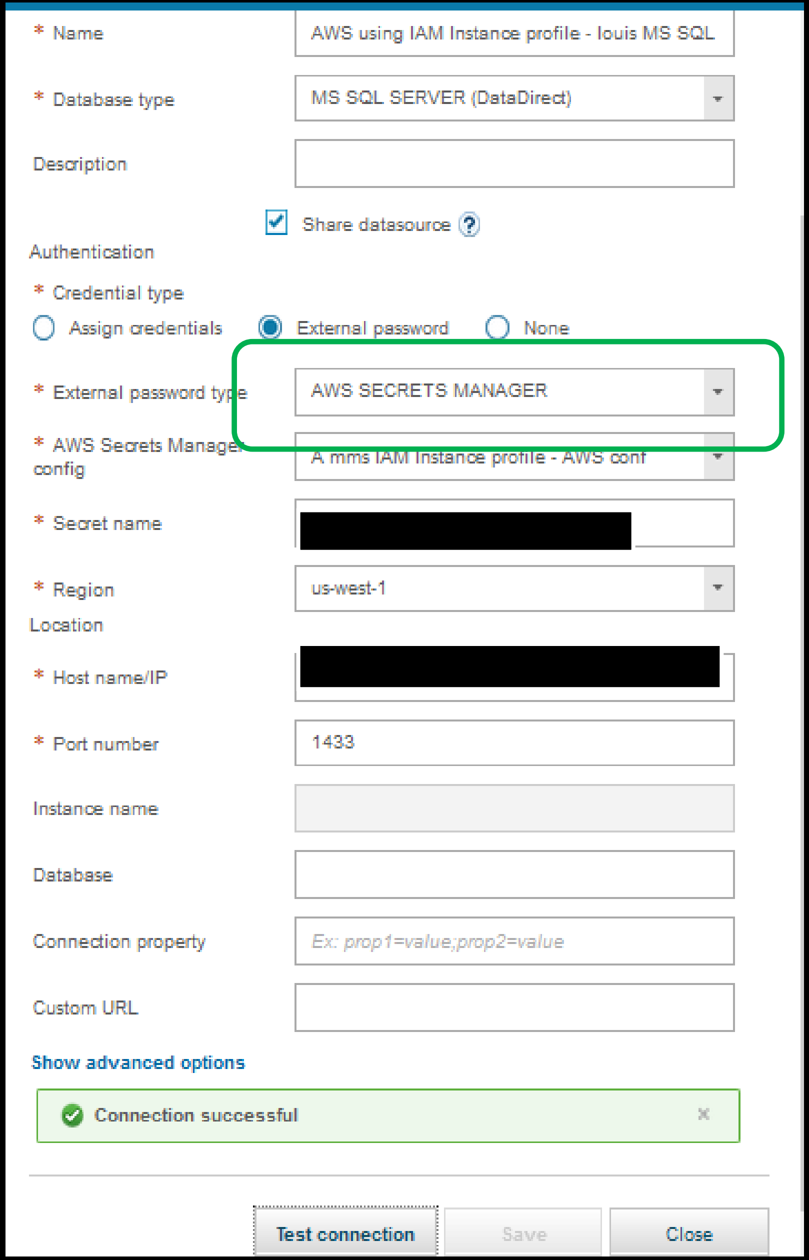
.*

Subject Alternative Name

.*

Key Type

Integration with AWS Secrets Manager



* Name	AWS using IAM Instance profile - louis MS SQL
* Database type	MS SQL SERVER (DataDirect)
Description	
	☑ Share datasource ?

Authentication

* Credential type
○ Assign credentials ● External password ○ None

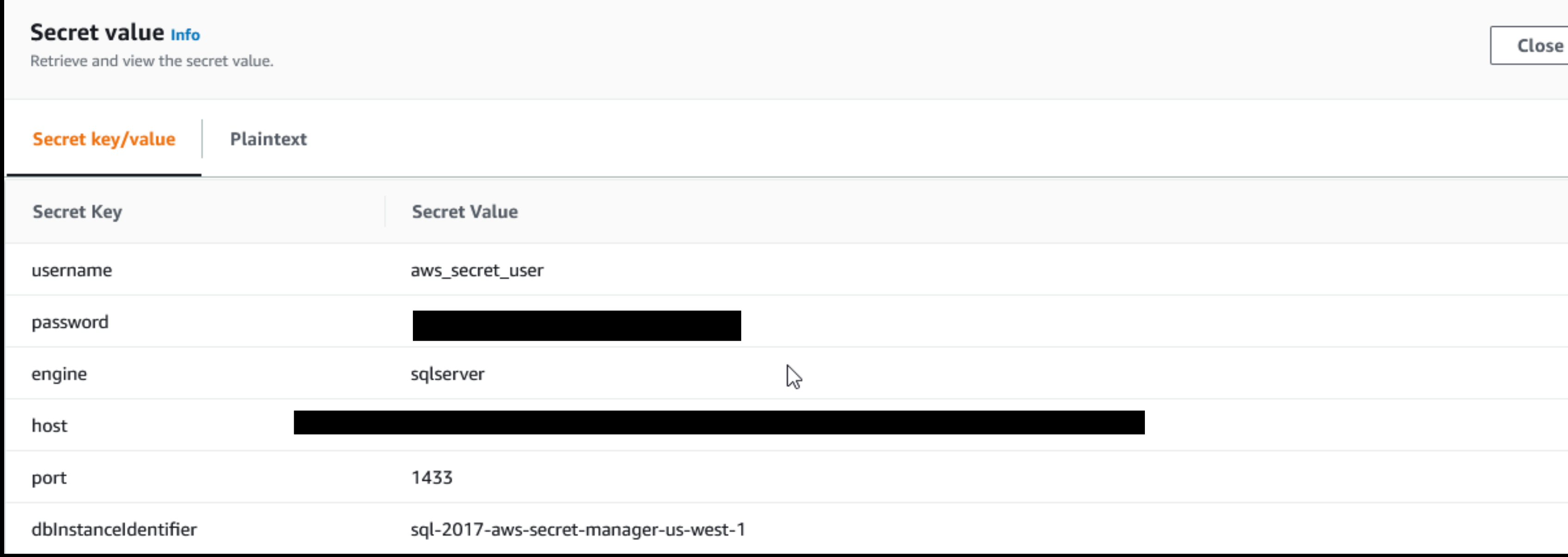
* External password type	AWS SECRETS MANAGER
* AWS Secrets Manager config	A mms IAM Instance profile - AWS conf
* Secret name	[redacted]
* Region	us-west-1

Location

* Host name/IP	[redacted]
* Port number	1433
Instance name	
Database	
Connection property	Ex: prop1=value;prop2=value
Custom URL	

Show advanced options

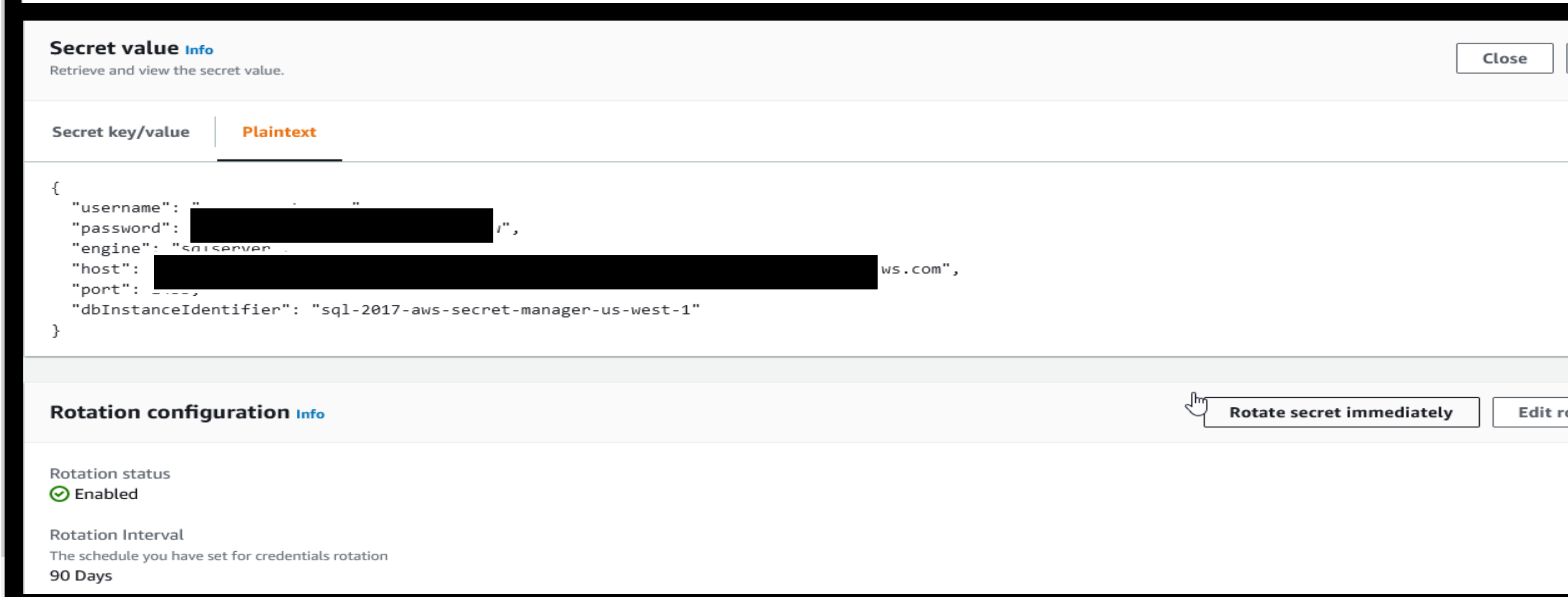
✓ Connection successful ×



Secret value Info

Retrieve and view the secret value.

Secret Key	Secret Value
username	aws_secret_user
password	[redacted]
engine	sqlserver
host	[redacted]
port	1433
dbInstanceIdentifier	sql-2017-aws-secret-manager-us-west-1



Secret value Info

Retrieve and view the secret value.

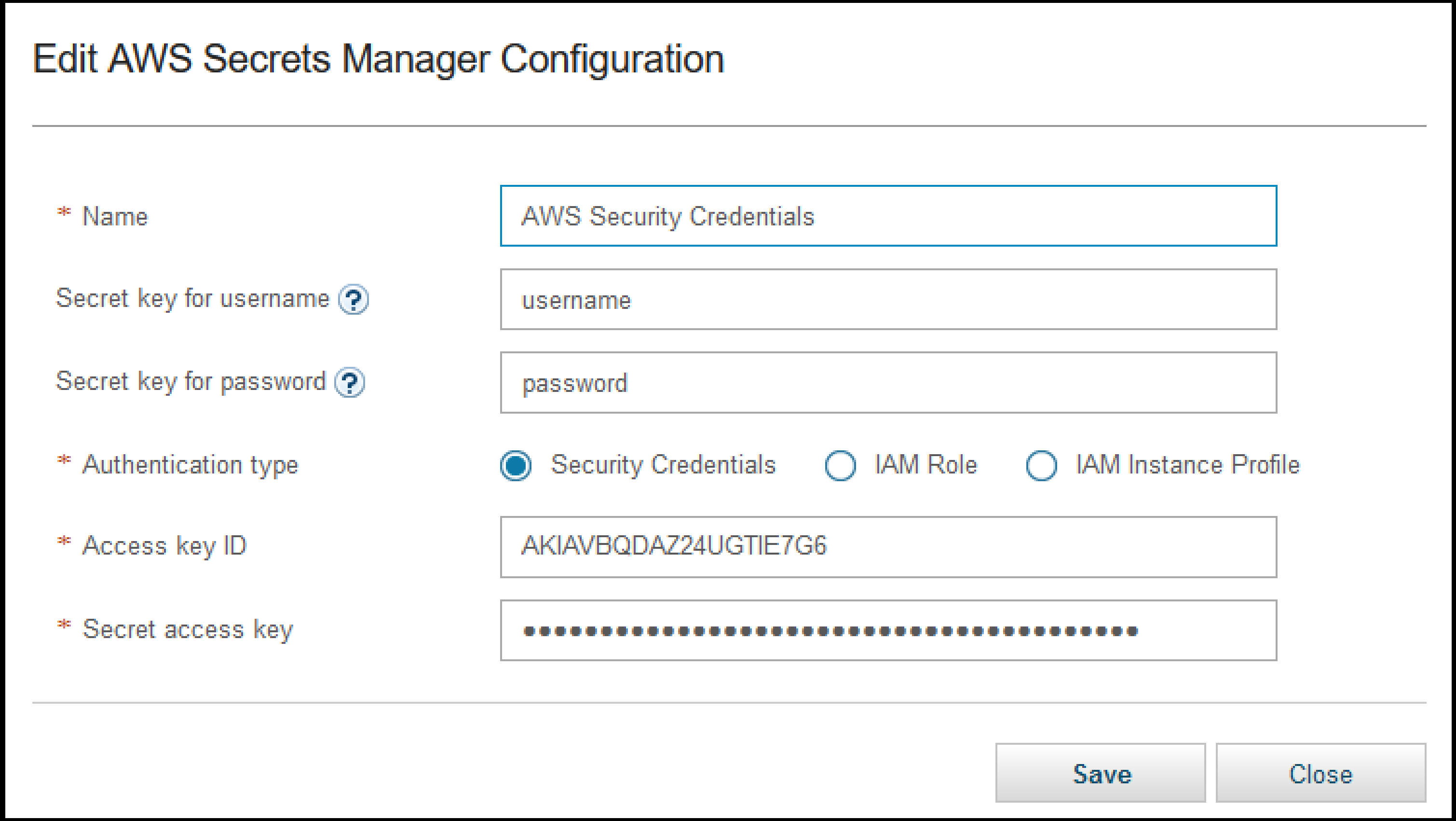
```
{
  "username": "[illegible]",
  "password": [redacted]",
  "engine": "sqlserver",
  "host": [redacted]ws.com",
  "port": [illegible],
  "dbInstanceIdentifier": "sql-2017-aws-secret-manager-us-west-1"
}
```

Rotation configuration Info

Rotation status
✓ Enabled

Rotation Interval
The schedule you have set for credentials rotation
90 Days

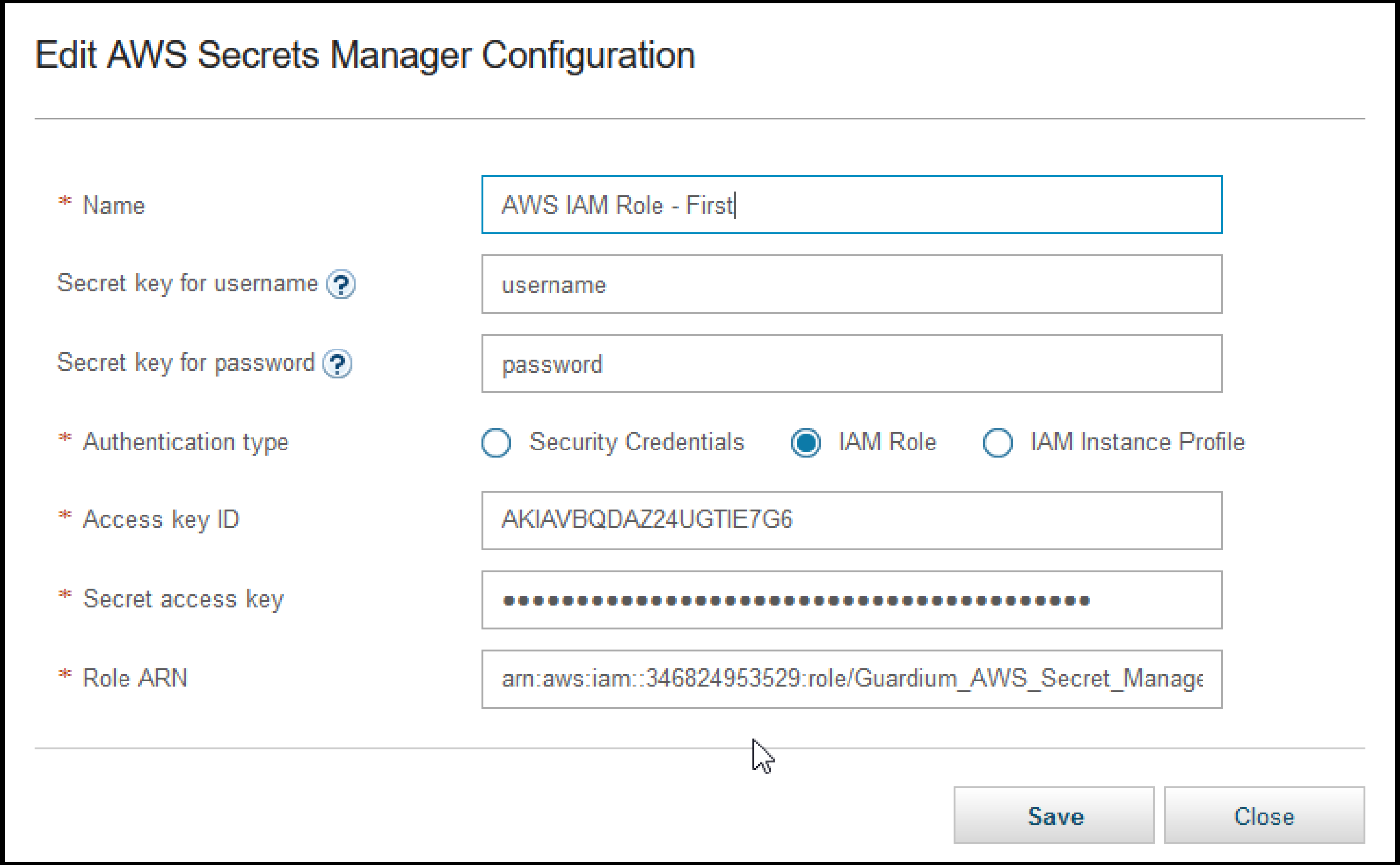
AWS Secrets Manager - Configuration



Edit AWS Secrets Manager Configuration

* Name	AWS Security Credentials
Secret key for username ?	username
Secret key for password ?	password
* Authentication type	● Security Credentials ○ IAM Role ○ IAM Instance Profile
* Access key ID	AKIAVBQDAZ24UGTIE7G6
* Secret access key	●●

AWS Secrets Manager – Configuration with IAM Role



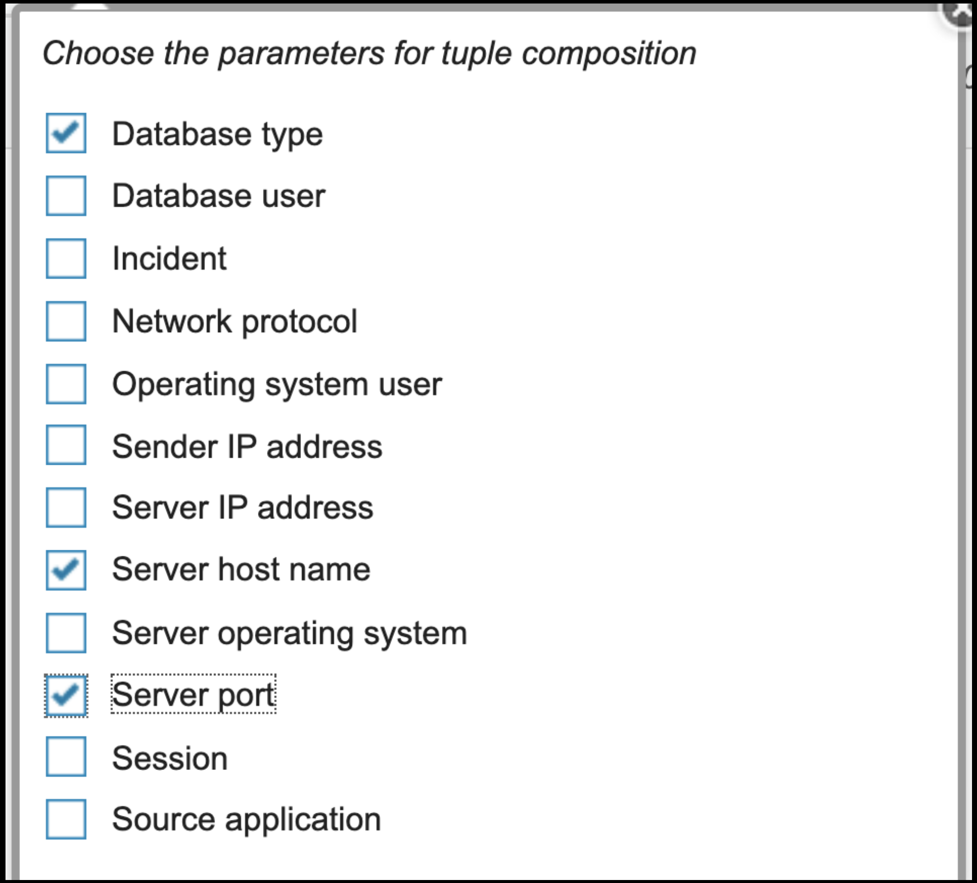
Edit AWS Secrets Manager Configuration

* Name	AWS IAM Role - First
Secret key for username ?	username
Secret key for password ?	password
* Authentication type	○ Security Credentials ● IAM Role ○ IAM Instance Profile
* Access key ID	AKIAVBQDAZ24UGTIE7G6
* Secret access key	●●
* Role ARN	arn:aws:iam::346824953529:role/Guardium_AWS_Secret_Manage

Session Level Policy: Log access only, Soft discard

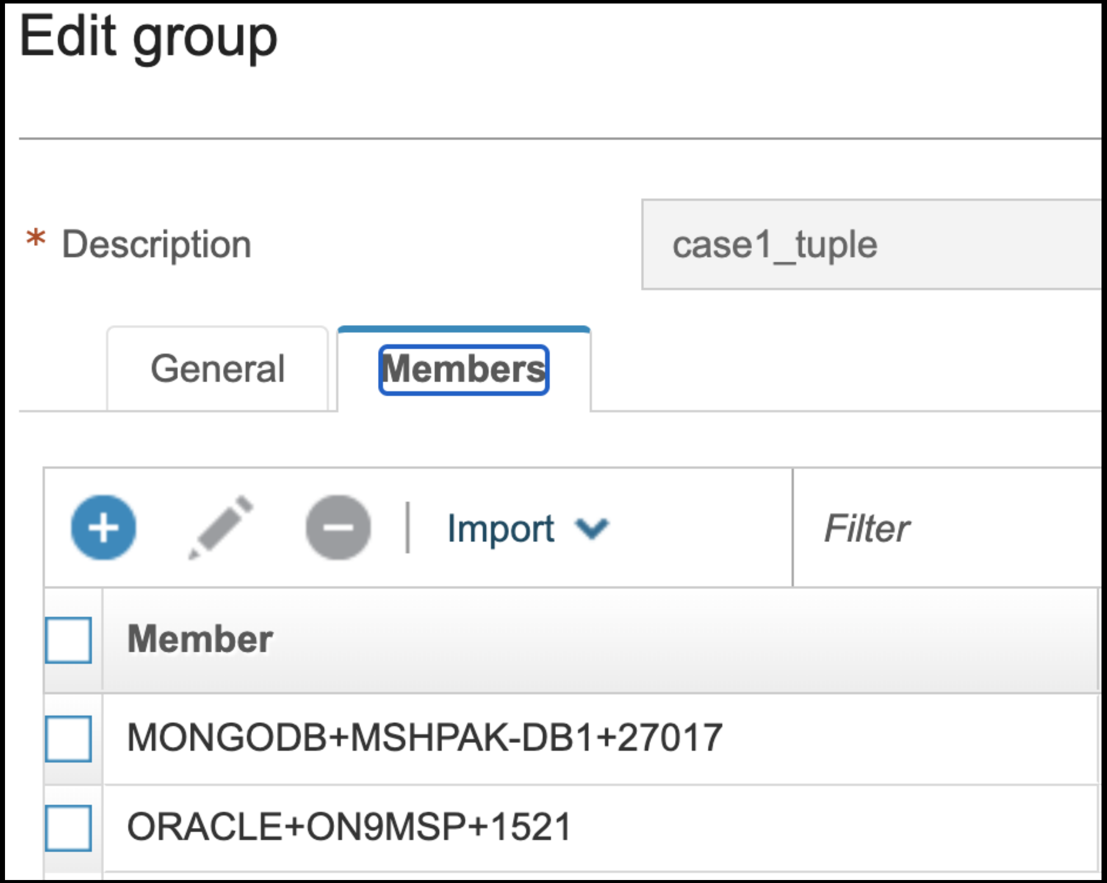
Case: Customer wants not to log any activity from the session, just the fact it happened

Problem: Customer wants to make a policy based on the tuple parameter combination not available in DSP



Choose the parameters for tuple composition

- ☑ Database type
- □ Database user
- □ Incident
- □ Network protocol
- □ Operating system user
- □ Sender IP address
- □ Server IP address
- ☑ Server host name
- □ Server operating system
- ☑ Server port
- □ Session
- □ Source application

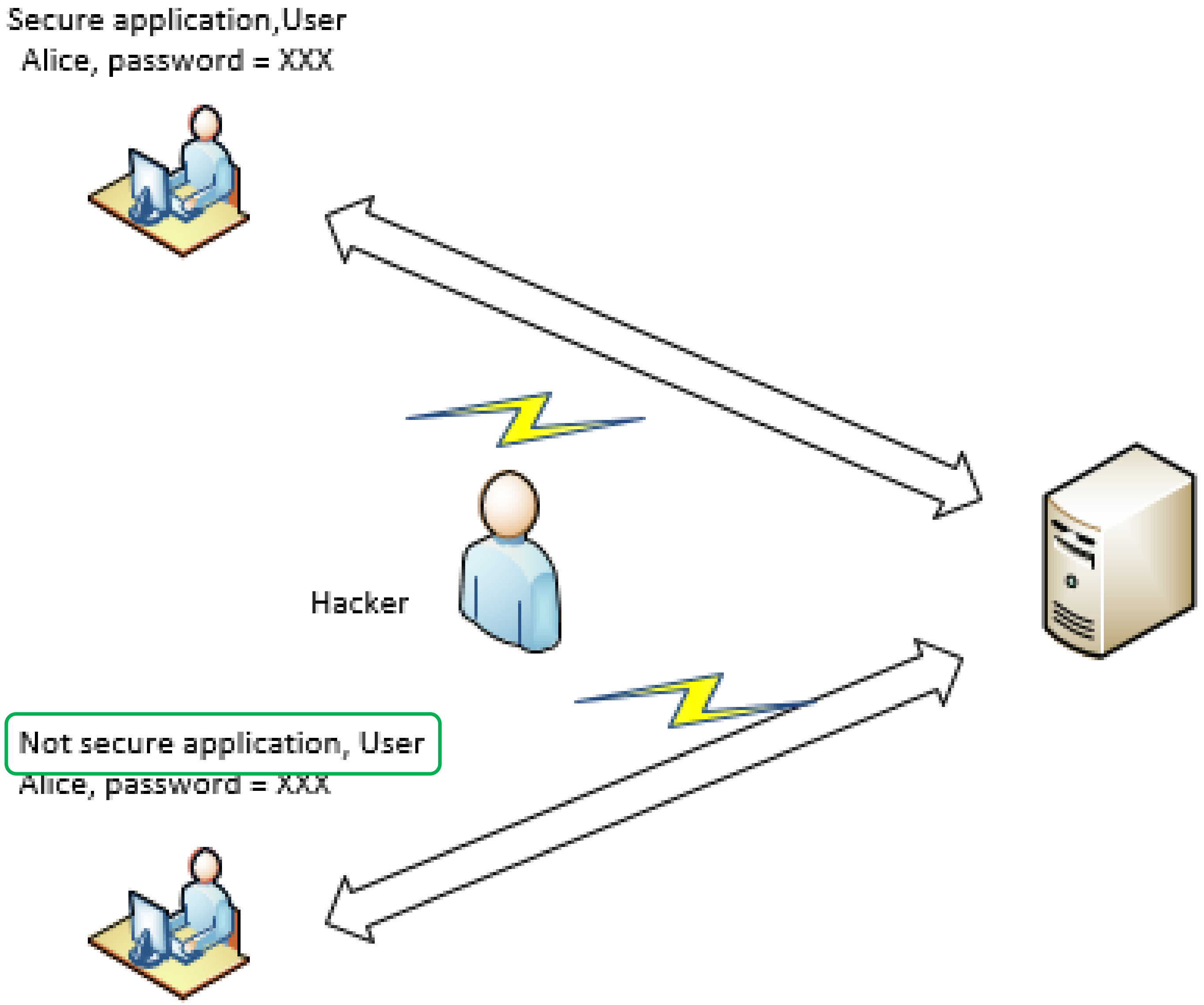


Edit group

* Description: case1_tuple

□	Member
□	MONGODB+MSHPAK-DB1+27017
□	ORACLE+ON9MSP+1521

Now possible to import tuple groups



Secure application,User
Alice, password = XXX

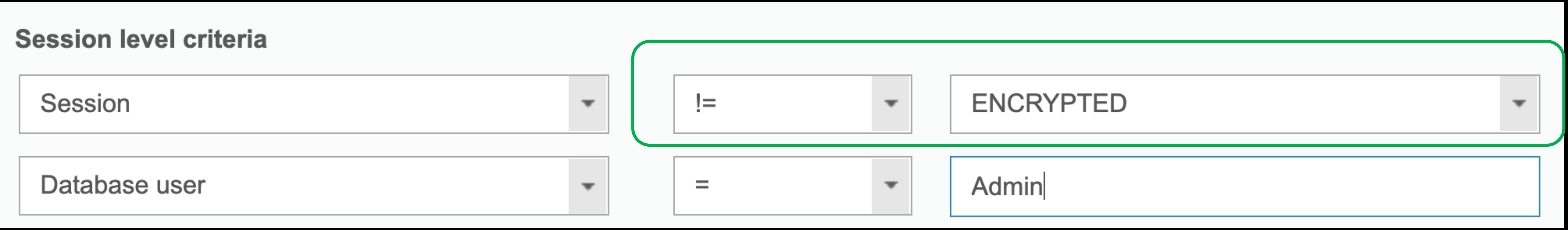
Hacker

Not secure application, User
Alice, password = XXX

Session Level Policy: Security incident and Throw exception

Case: Customer wants all unencrypted sessions with administrative users to throw exceptions

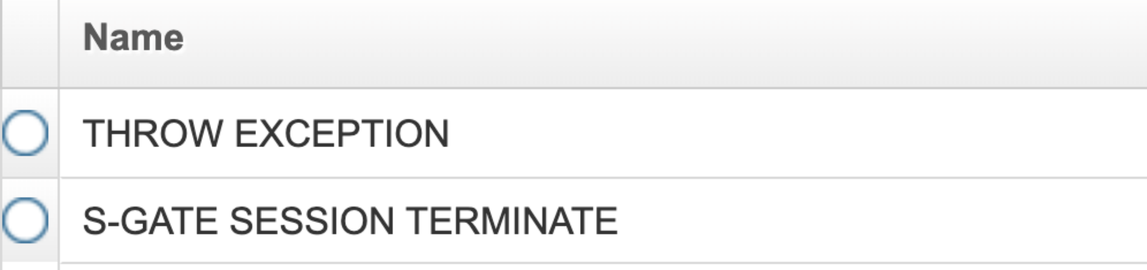
Rule criteria



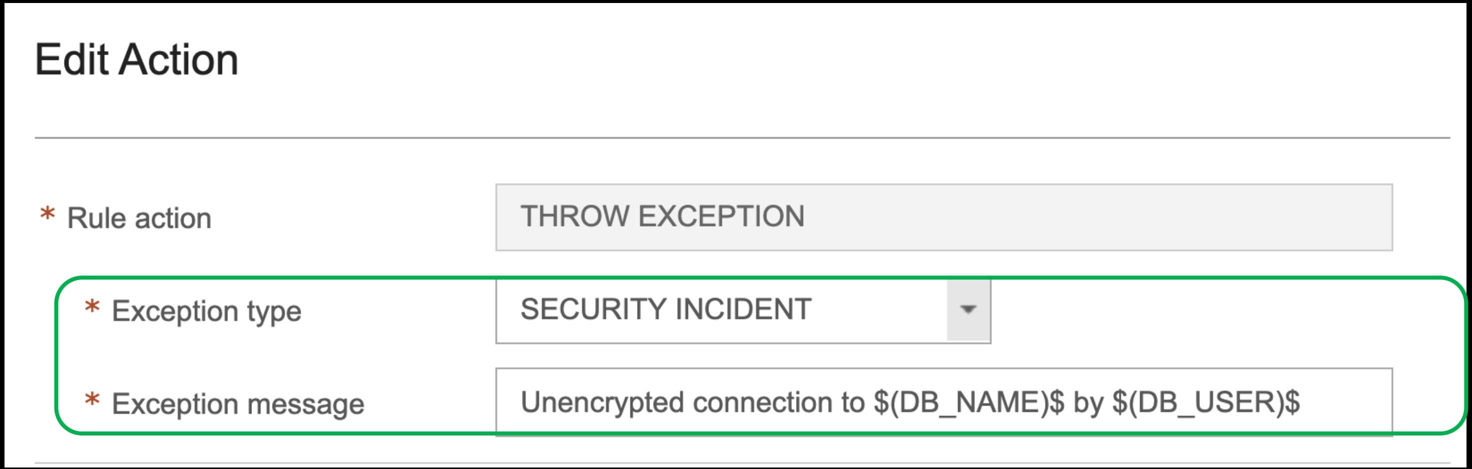
Session level criteria

Session	!=	ENCRYPTED
Database user	=	Admin

Rule action



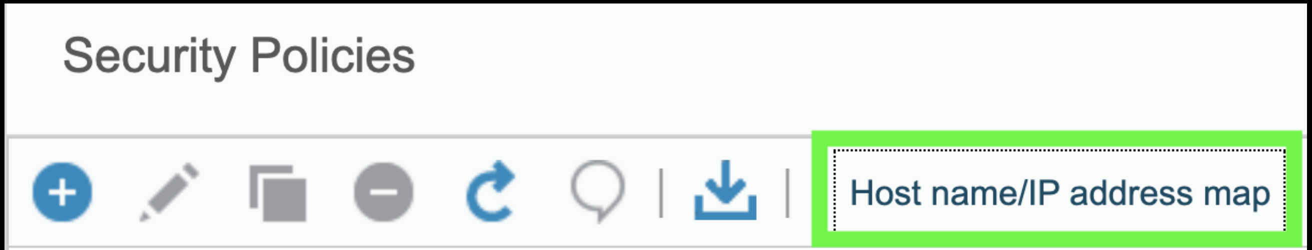
	Name
○	THROW EXCEPTION
○	S-GATE SESSION TERMINATE



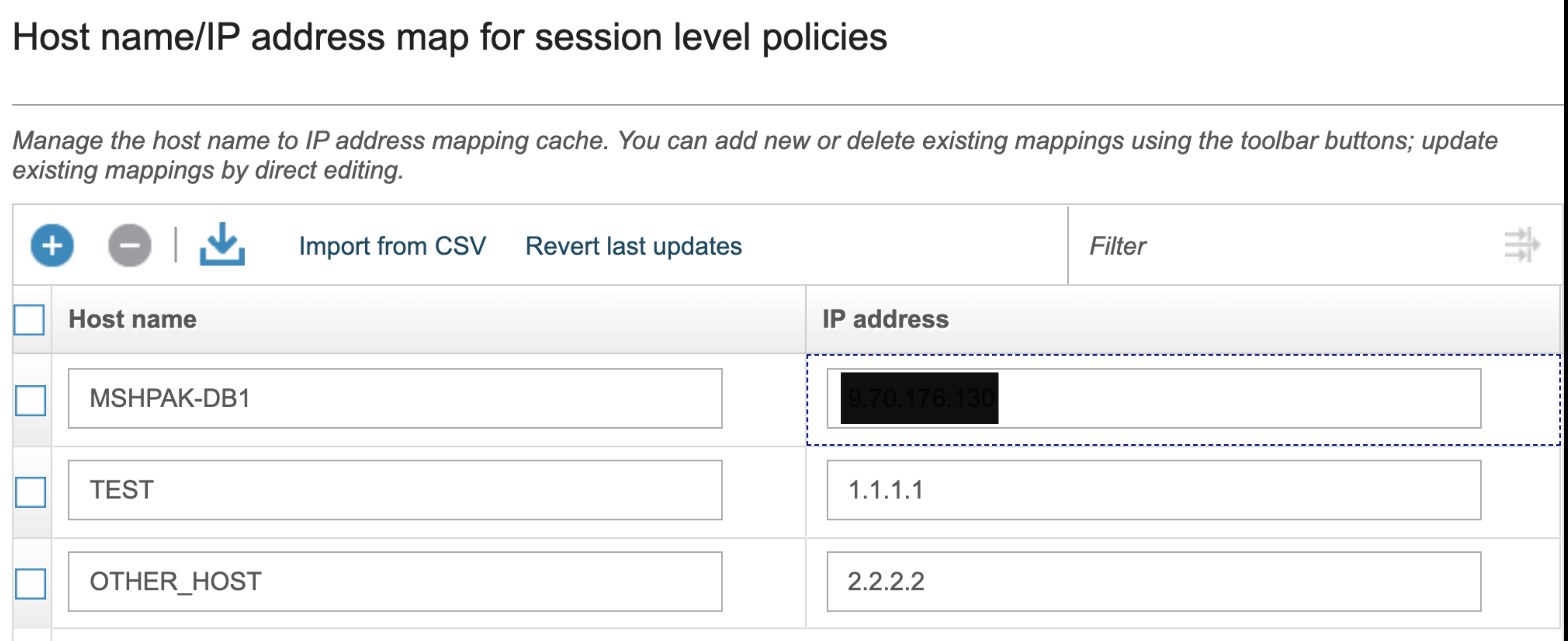
Edit Action

* Rule action	THROW EXCEPTION
* Exception type	SECURITY INCIDENT
* Exception message	Unencrypted connection to (DB_NAME) by (DB_USER)

Session Level Policy: Put your host name cache to work



Security Policies

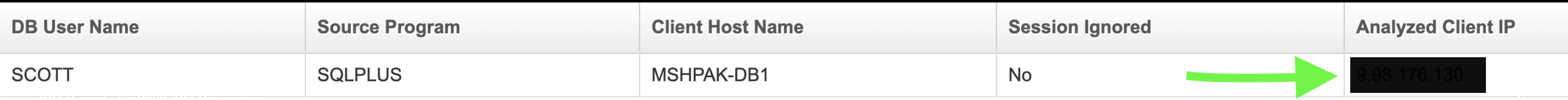


Host name/IP address map for session level policies

Manage the host name to IP address mapping cache. You can add new or delete existing mappings using the toolbar buttons; update existing mappings by direct editing.

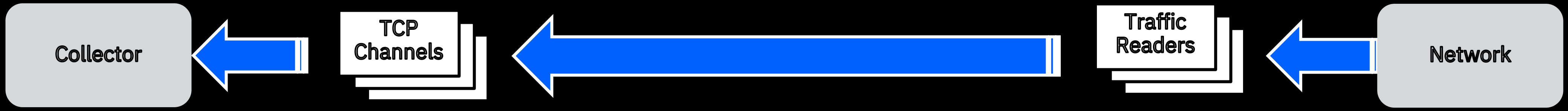
□	Host name	IP address
□	MSHPAK-DB1	[redacted]
□	TEST	1.1.1.1
□	OTHER_HOST	2.2.2.2

Result:



DB User Name	Source Program	Client Host Name	Session Ignored	Analyzed Client IP
SCOTT	SQLPLUS	MSHPAK-DB1	No	[redacted]

New Windows STAP (Protocol V8)



- Multiple Traffic Readers / TAP
- Re-engineered Dynamic Buffer Increase Algorithm
- Reduction in Buffer Copies
- Reduction in Lock Contention
- Reduction in CPU/Memory Usage
- Reduction in Firewall / Query Rewrite Latency

Windows STAP performance improvements

2X SQL/Sec

5X Less CPU

2X Less Memory

3X Sessions

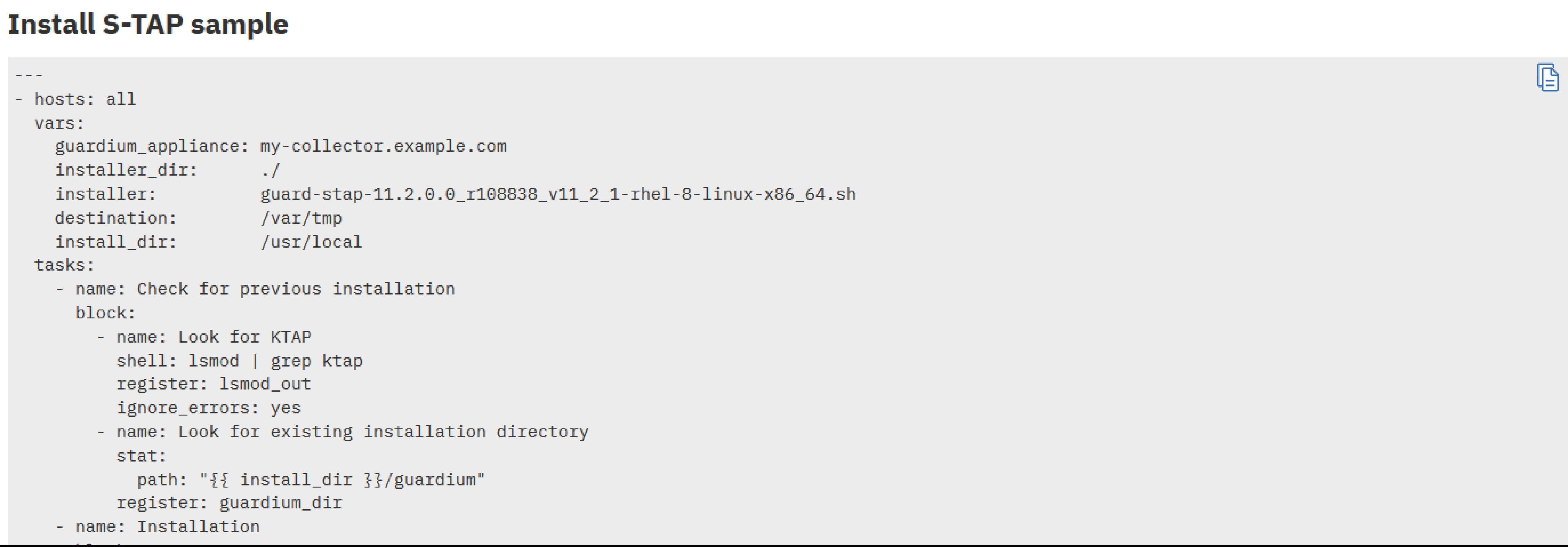
3X Less Network Overhead

Unix STAP Enhancements

- Using Ranger logs to monitor HDFS – No need for a kernel module
- ELB Rebalance to new collector w/o STAP restart – Prevent dropping buffers
- ATAP can now make decisions on ignoring response w/o going to KTAP – Reduce load on the server
- Better Control of custom modules upload from STAP to the appliance

Ansible Automation for STAP

- With Ansible auomation from Red Hat, you can now automate a lot of the STAP procedures to east day to day tasks

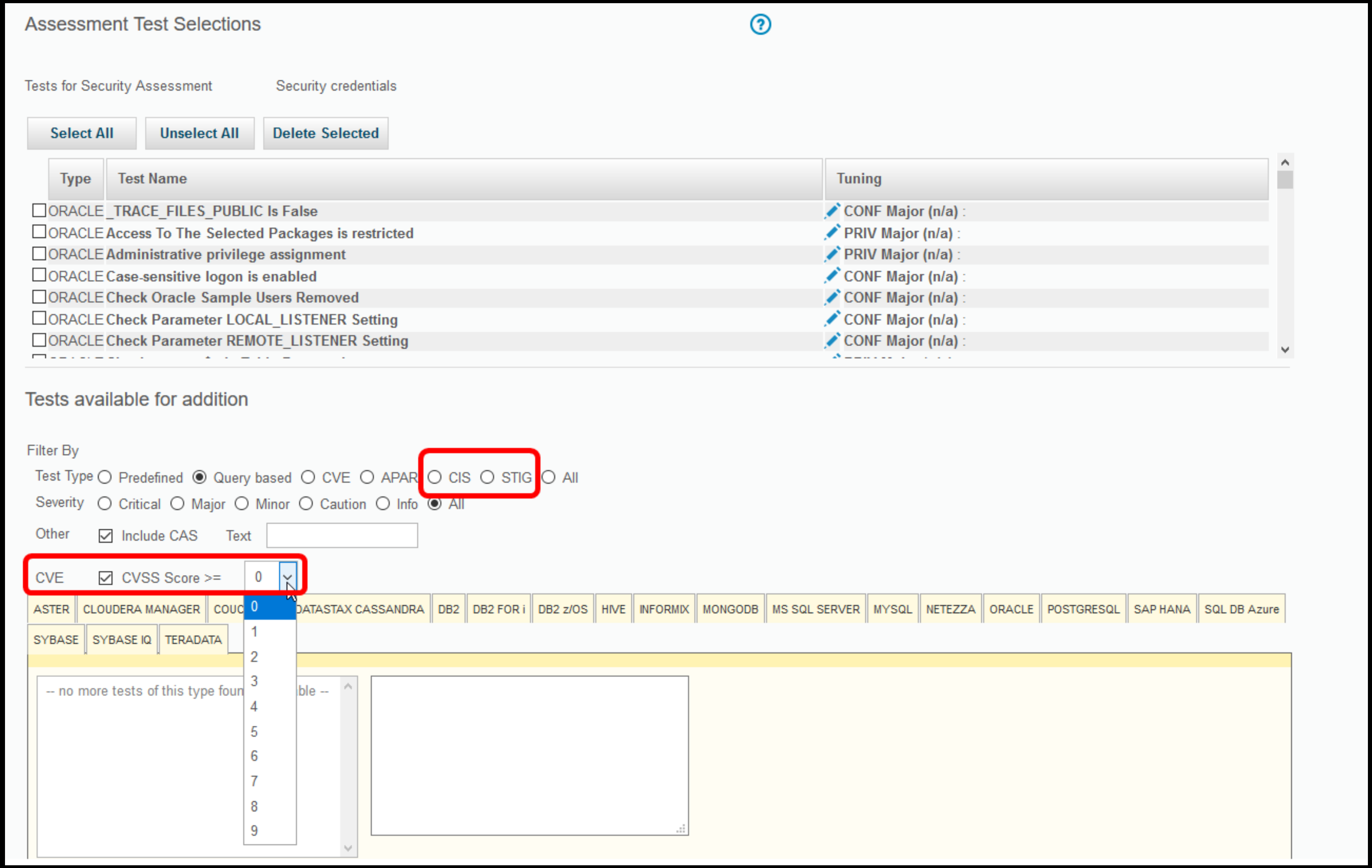


Install S-TAP sample

```
---
- hosts: all
  vars:
    guardium_appliance: my-collector.example.com
    installer_dir:      ./
    installer:          guard-stap-11.2.0.0_r108838_v11_2_1-rhel-8-linux-x86_64.sh
    destination:        /var/tmp
    install_dir:        /usr/local
  tasks:
    - name: Check for previous installation
      block:
        - name: Look for KTAP
          shell: lsmod | grep ktap
          register: lsmod_out
          ignore_errors: yes
        - name: Look for existing installation directory
          stat:
            path: "{{ install_dir }}/guardium"
          register: guardium_dir
    - name: Installation
```

VA Enhancements

- Now, you can now specifically choose tests that have external references for CIS or STIG.
- You can also choose to select CVE tests >= to a specific CVSS score
- Enhancements for Oracle weak password detection
- VA now supports Couchbase
- VA now support PostgresSQL 12 and it’s new CIS benchmark tests



Assessment Test Selections

Tests for Security Assessment   Security credentials

	Type	Test Name	Tuning
□	ORACLE	_TRACE_FILES_PUBLIC Is False	CONF Major (n/a) :
□	ORACLE	Access To The Selected Packages is restricted	PRIV Major (n/a) :
□	ORACLE	Administrative privilege assignment	PRIV Major (n/a) :
□	ORACLE	Case-sensitive logon is enabled	CONF Major (n/a) :
□	ORACLE	Check Oracle Sample Users Removed	CONF Major (n/a) :
□	ORACLE	Check Parameter LOCAL_LISTENER Setting	CONF Major (n/a) :
□	ORACLE	Check Parameter REMOTE_LISTENER Setting	CONF Major (n/a) :

Tests available for addition

Filter By

Test Type ○ Predefined ● Query based ○ CVE ○ APAR ○ CIS ○ STIG ○ All

Severity ○ Critical ○ Major ○ Minor ○ Caution ○ Info ● All

Other ☑ Include CAS Text

CVE ☑ CVSS Score >= 0

-- no more tests of this type foun[...]ble --

Couchbase

NoEQUAL

Odd and Ends

- You can now disable CLI acccounts that are not in used instead of having to change password all the time

- Automating Key Entry for Appliance Encryption – If you wish to encrypt the appliance disk, there is a way to automate the key entry at boot time

- Enhanced Security for existing DUO Integration

- Added Support for S3 Glacier for low cost long term backup

- Policy rule can now accept multiple subnet masks as a group

- You can now add Object Name attribute to alert message so you can easily query on them

Interact with Guardium Users/Experts

- Join the **Guardium Virtual Users Group** (VUG), an online monthly meeting for customers. To find out more and join: https://www.ibm.com/support/pages/node/597565

- Join the **IBM Security Community/Guardium**, to discuss all things Guardium, view resources and upcoming events and more: http://ibm.biz/SecurityCommunityGuardium

Thank you

Follow us on:

[ibm.com/security]

[securityintelligence.com]

[ibm.com/security/community]

[xforce.ibmcloud.com]

[@ibmsecurity]

[youtube.com/ibmsecurity]

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.