IBM Security

What’s new in Guardium 10.6

Shay Harel – Director of Engineering / Data Security

January 2019

Notices and disclaimers

- © 2018 International Business Machines Corporation. No part of this document may be reproduced or transmitted in any form without written permission from IBM.

- **U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.**

- Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

- IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

- **Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.**

- Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those

- customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

- References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

- Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

- It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Notices and disclaimers (continued)

- Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**

- The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

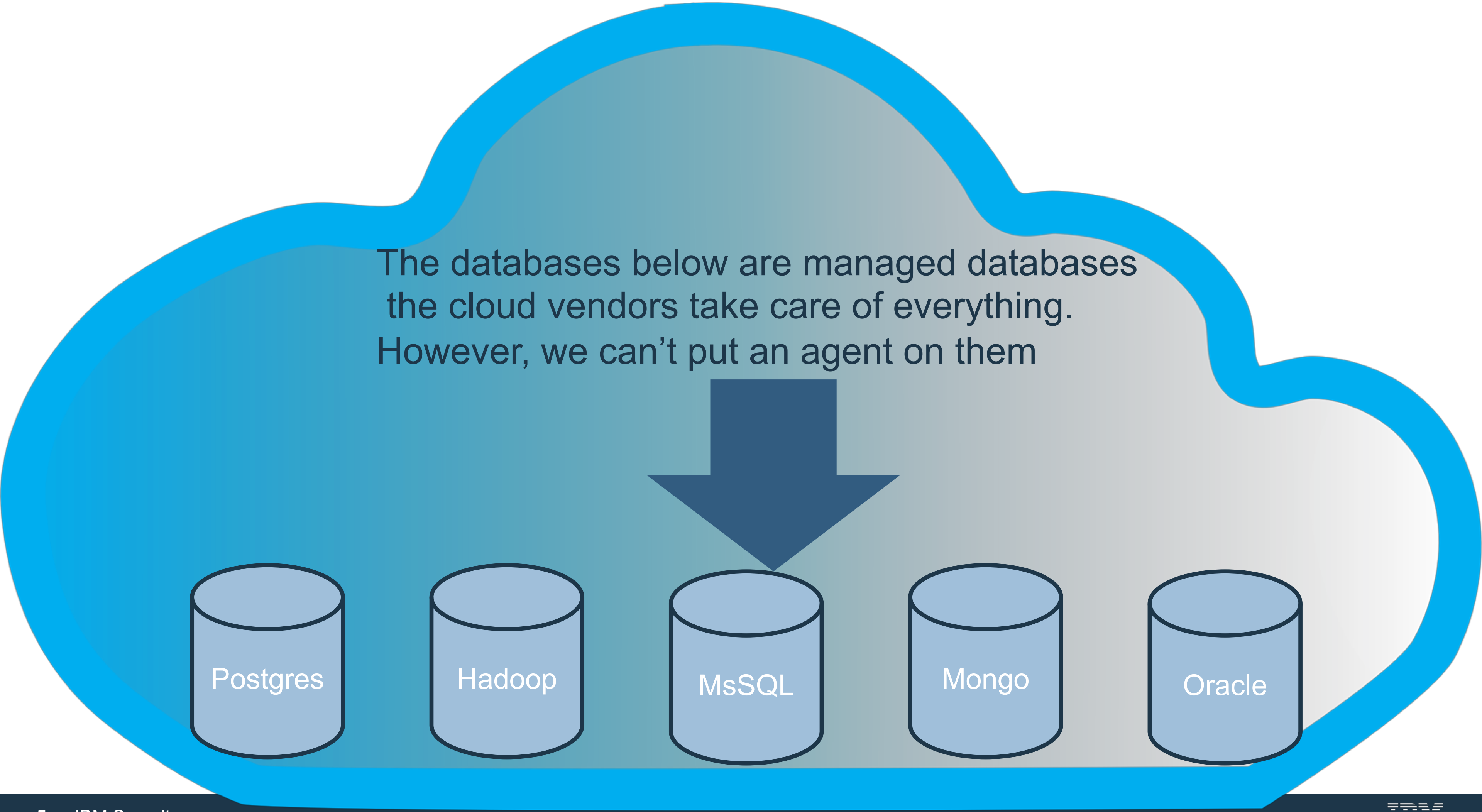
- IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.

- .

Today’s topics

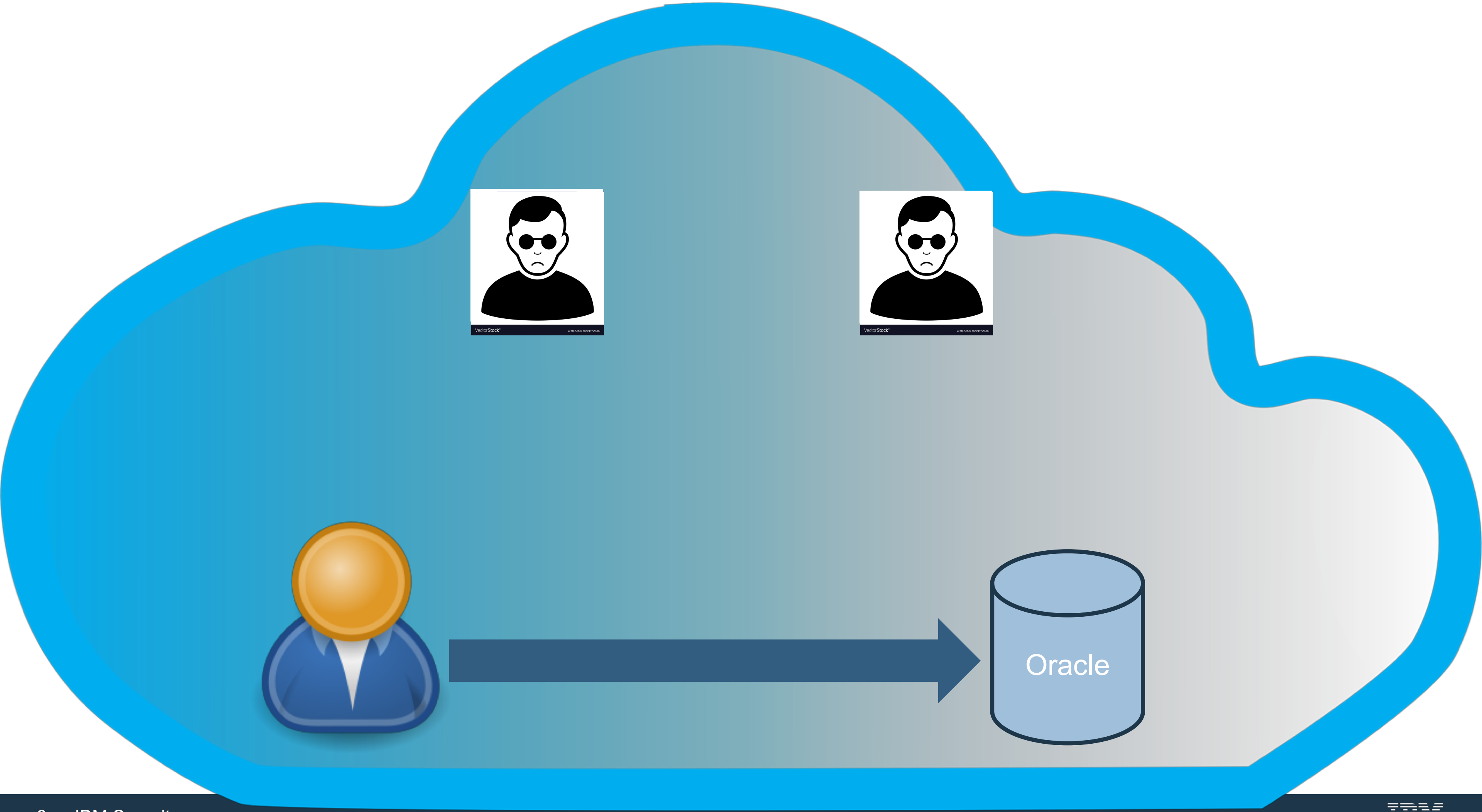
- External S-TAP
- New Policy Builder and new feature of Session Level Policy
- New Query/Report Builder
- Self monitoring of appliance disk to prevent disk full
- Unstructured data monitoring for SharePoint and NAS
- Updates and enhancements to GIM
- S-TAP, A-TAP Updates (Windows, Unix)
- Change to Classification
- Vulnerability Assessment (VA)
- Miscellaneous

External S-TAP

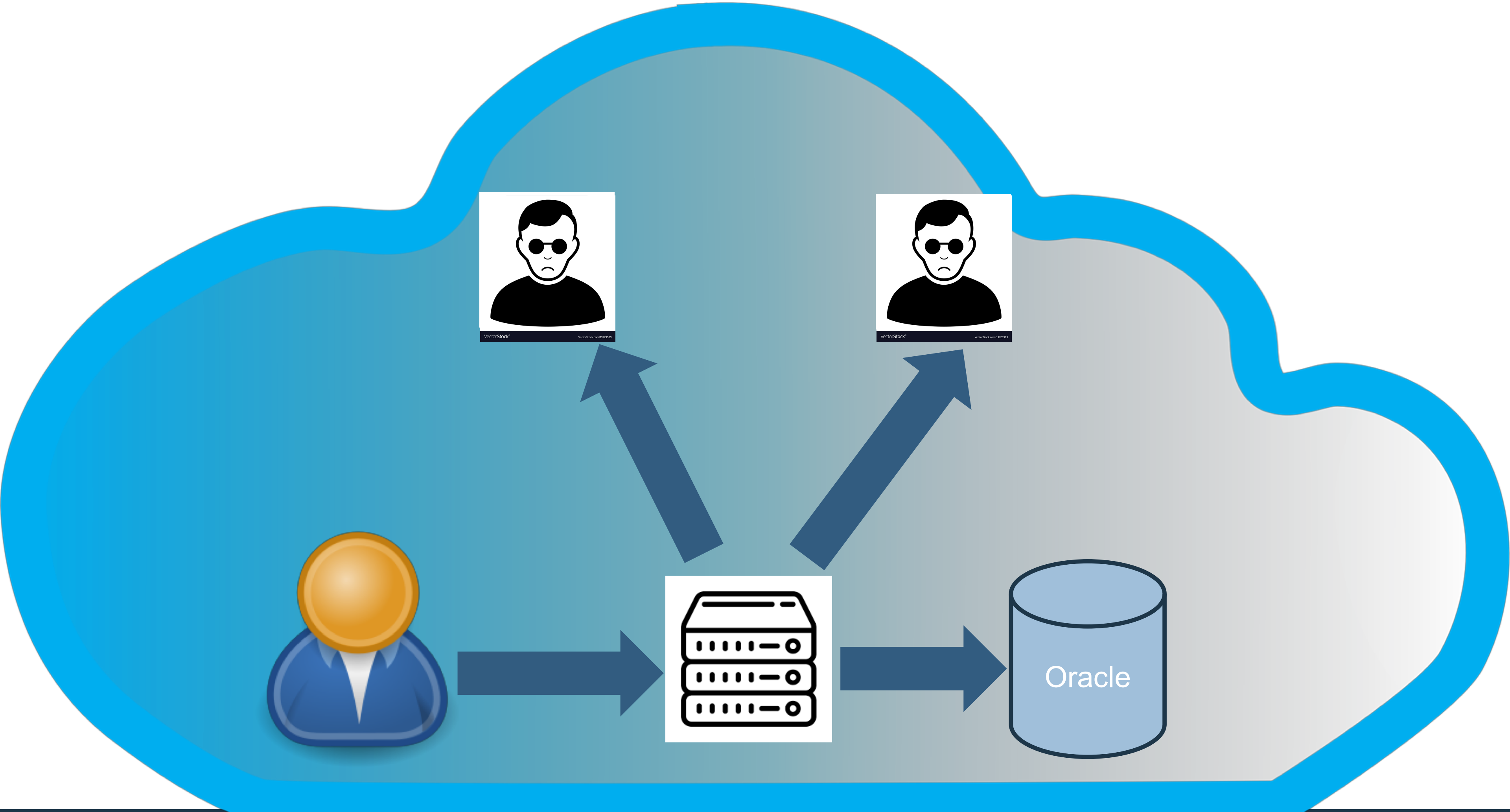


The databases below are managed databases the cloud vendors take care of everything. However, we can’t put an agent on them

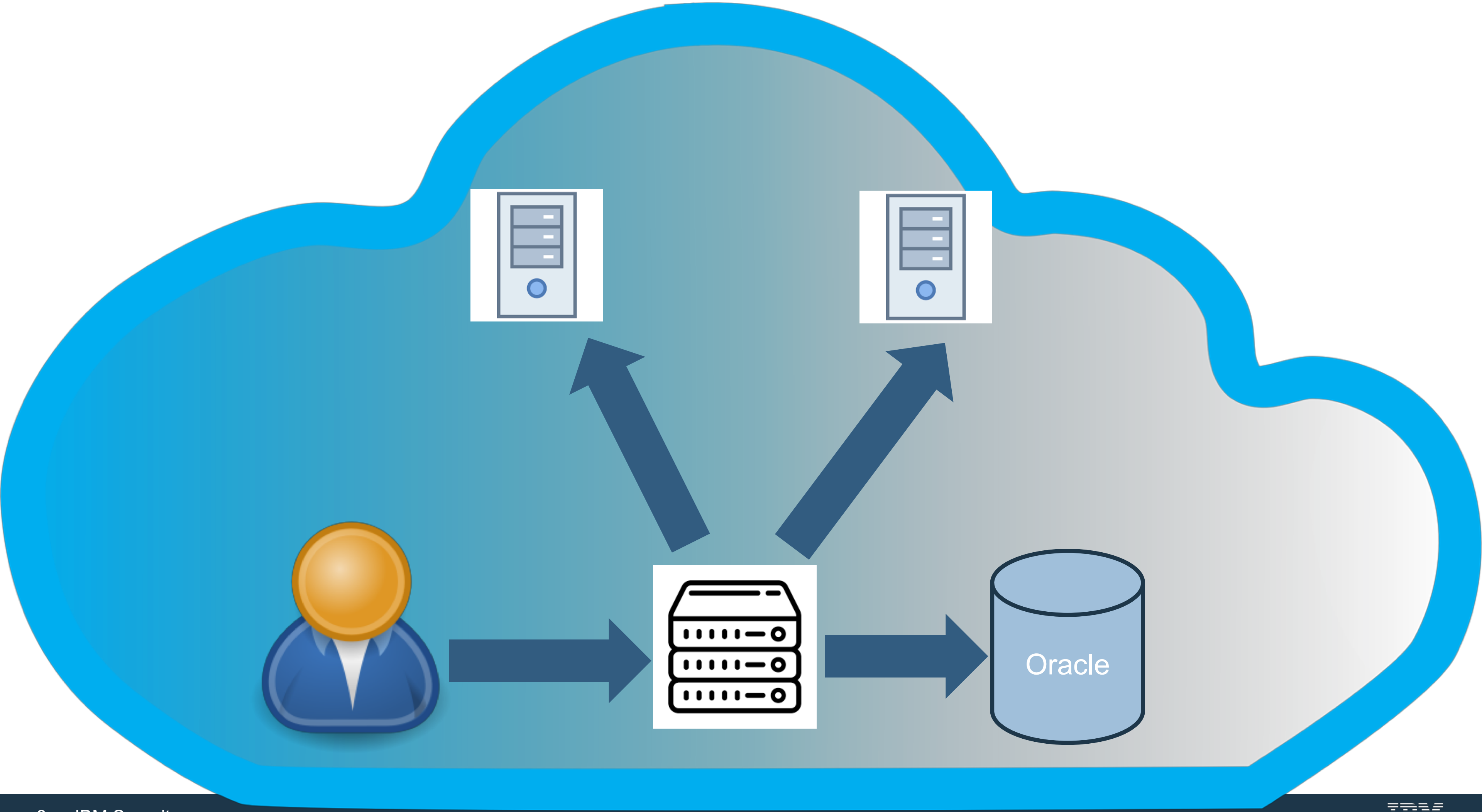
So now our collectors are blind ☹



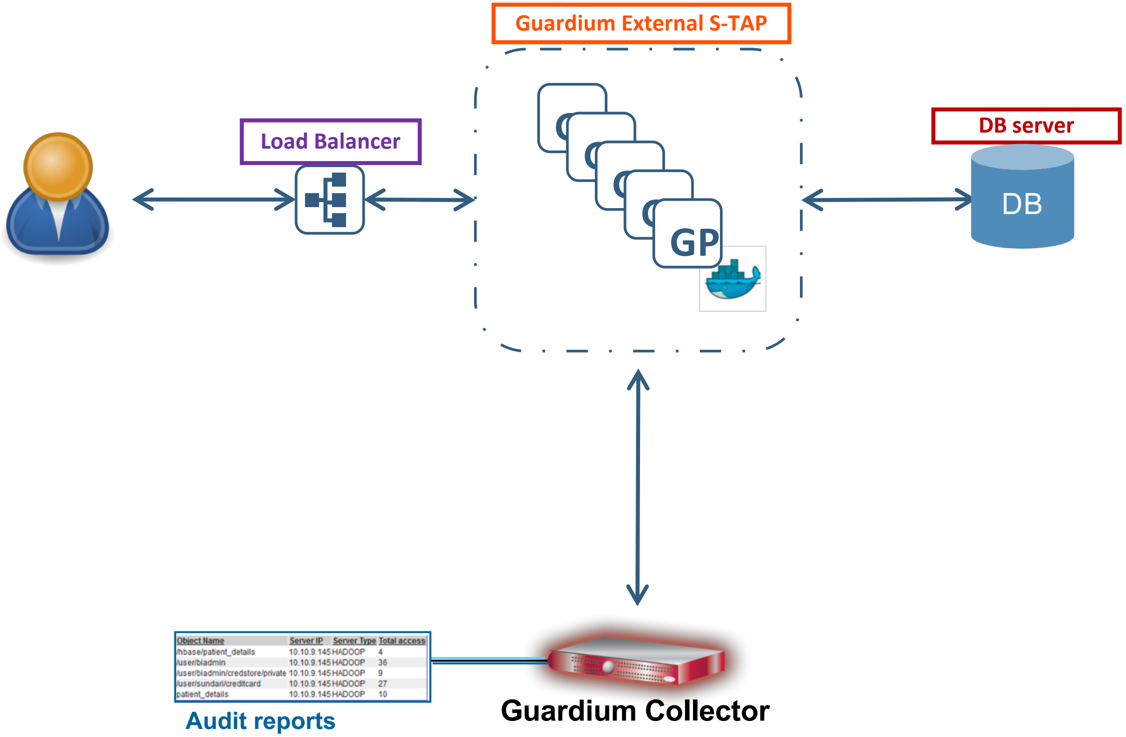
That’s where the external S-TAP comes into play



Now we can see traffic again even without an S-TAP



External S-TAP Architecture



Guardium External S-TAP

Load Balancer

DB server

Object Name	Server IP	Server Type	Total access
/hbase/patient_details	10.10.9.145	HADOOP	4
/user/biadmin	10.10.9.145	HADOOP	36
/user/biadmin/credstore/private	10.10.9.145	HADOOP	9
/user/sundari/creditcard	10.10.9.145	HADOOP	27
patient_details	10.10.9.145	HADOOP	10

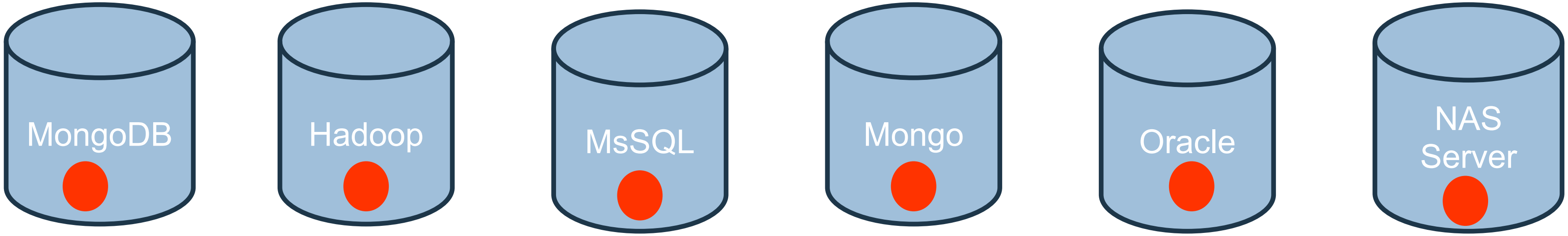
Audit reports

Guardium Collector

That's cool, any more applications for the external S-TAP?

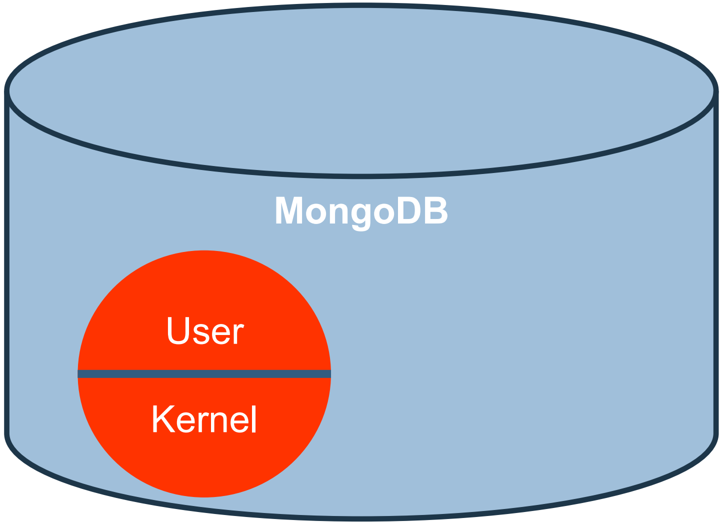
Let’s look at the typical data center

Let’s zoom in on one database



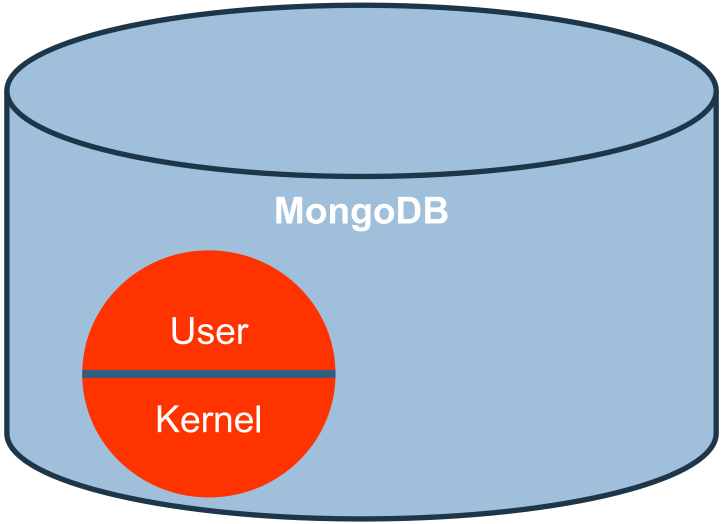
Remember this picture?

On the database server, the S-TAP has components located in user space and some deep inside the OS (Kernel)

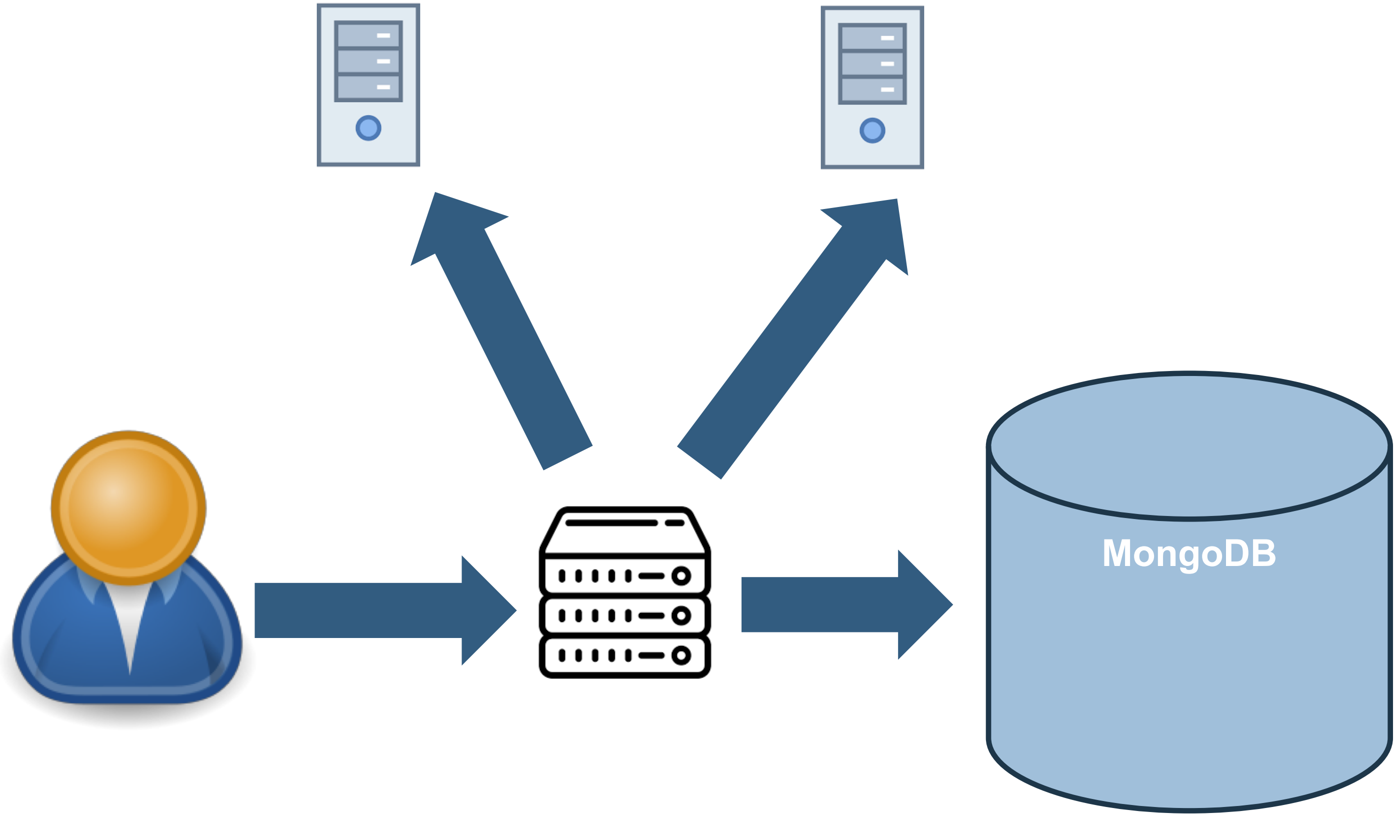


Remember this picture?

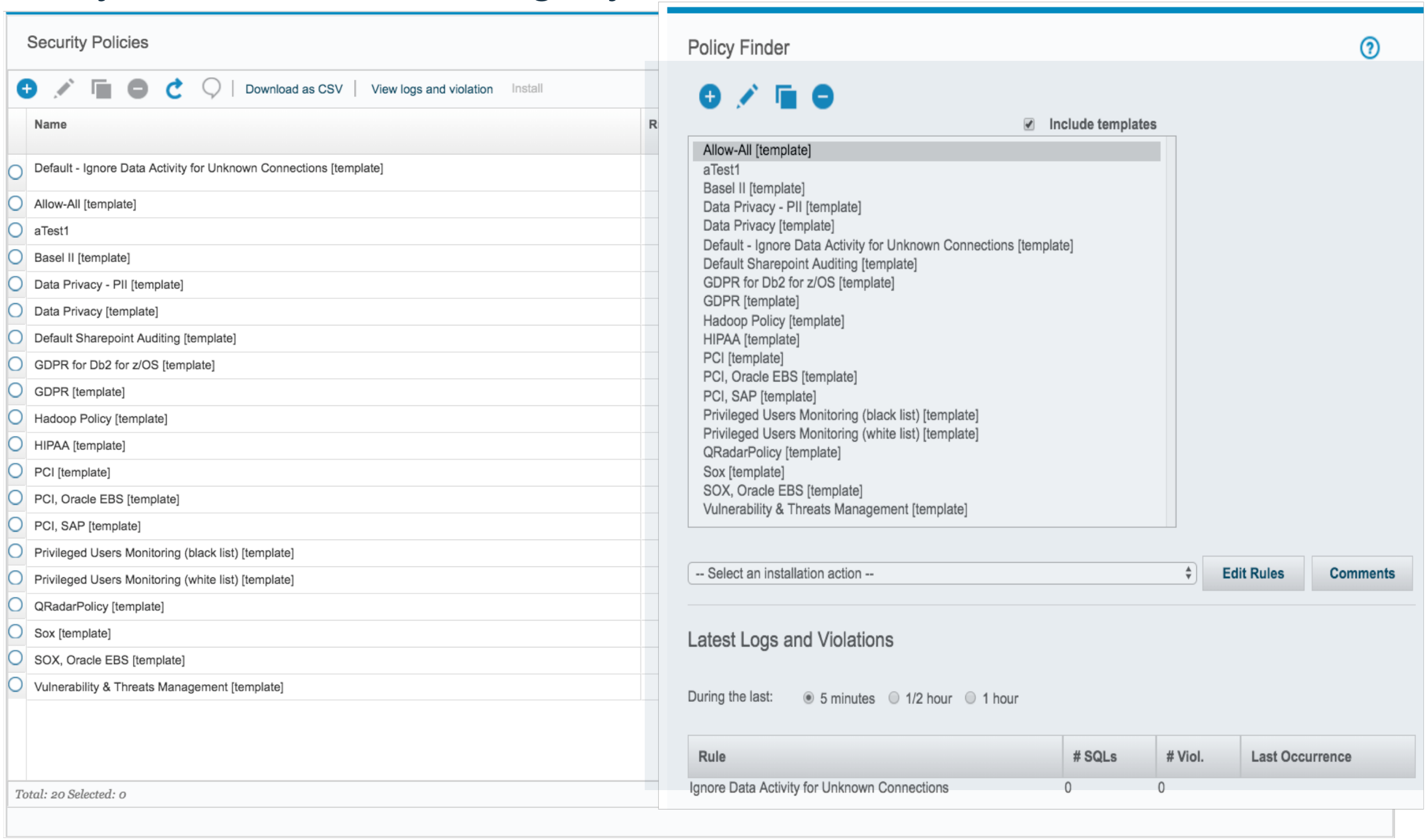
However, on database deployed in containers, there is no access to the kernel, hence we can't install an S-TAP, sounds familiar?



Once again, the external S-TAP comes to the rescue



Policy Builder - New vs legacy



Security Policies

	Name	R
○	Default - Ignore Data Activity for Unknown Connections [template]	
○	Allow-All [template]	
○	aTest1	
○	Basel II [template]	
○	Data Privacy - PII [template]	
○	Data Privacy [template]	
○	Default Sharepoint Auditing [template]	
○	GDPR for Db2 for z/OS [template]	
○	GDPR [template]	
○	Hadoop Policy [template]	
○	HIPAA [template]	
○	PCI [template]	
○	PCI, Oracle EBS [template]	
○	PCI, SAP [template]	
○	Privileged Users Monitoring (black list) [template]	
○	Privileged Users Monitoring (white list) [template]	
○	QRadarPolicy [template]	
○	Sox [template]	
○	SOX, Oracle EBS [template]	
○	Vulnerability & Threats Management [template]	

Total: 20 Selected: 0

Policy Finder

☑ Include templates

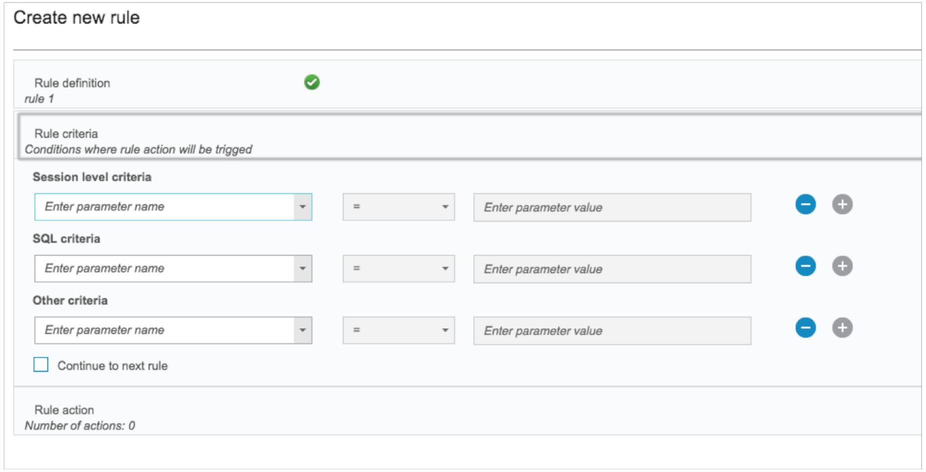
Allow-All [template]
aTest1
Basel II [template]
Data Privacy - PII [template]
Data Privacy [template]
Default - Ignore Data Activity for Unknown Connections [template]
Default Sharepoint Auditing [template]
GDPR for Db2 for z/OS [template]
GDPR [template]
Hadoop Policy [template]
HIPAA [template]
PCI [template]
PCI, Oracle EBS [template]
PCI, SAP [template]
Privileged Users Monitoring (black list) [template]
Privileged Users Monitoring (white list) [template]
QRadarPolicy [template]
Sox [template]
SOX, Oracle EBS [template]
Vulnerability & Threats Management [template]

Latest Logs and Violations

During the last: ● 5 minutes ○ 1/2 hour ○ 1 hour

Rule	# SQLs	# Viol.	Last Occurrence
Ignore Data Activity for Unknown Connections	0	0	

Rule criteria – new vs legacy



Create new rule

Rule definition ✓
rule 1

Rule criteria
Conditions where rule action will be trigged

Session level criteria

Enter parameter name | = | *Enter parameter value* ⊖ ⊕

SQL criteria

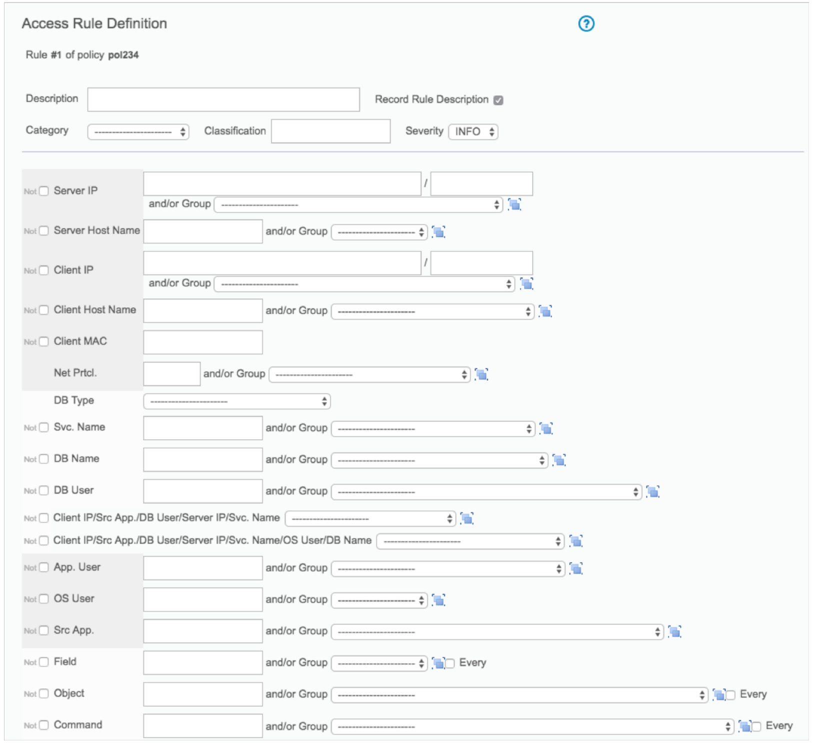
Enter parameter name | = | *Enter parameter value* ⊖ ⊕

Other criteria

Enter parameter name | = | *Enter parameter value* ⊖ ⊕

□ Continue to next rule

Rule action
Number of actions: 0



Access Rule Definition

Rule **#1** of policy **pol234**

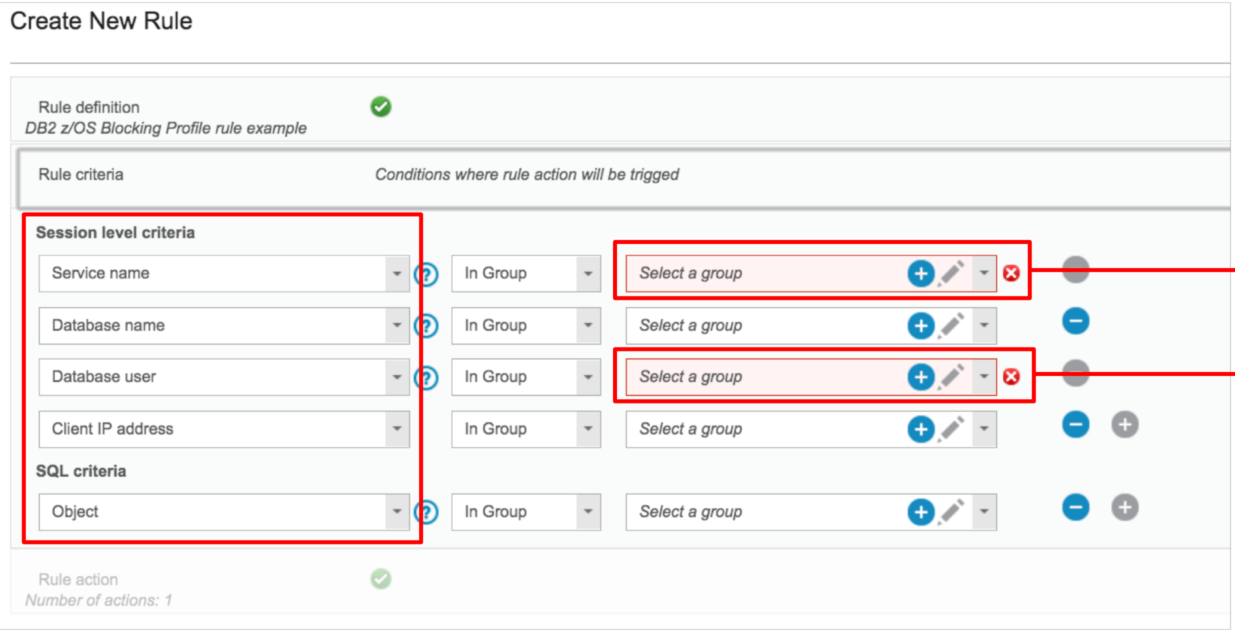
Description | Record Rule Description ☑

Category | Classification | Severity INFO

Not □ Server IP / and/or Group
Not □ Server Host Name and/or Group
Not □ Client IP / and/or Group
Not □ Client Host Name and/or Group
Not □ Client MAC
Net Prtcl. and/or Group
DB Type
Not □ Svc. Name and/or Group
Not □ DB Name and/or Group
Not □ DB User and/or Group
Not □ Client IP/Src App./DB User/Server IP/Svc. Name
Not □ Client IP/Src App./DB User/Server IP/Svc. Name/OS User/DB Name
Not □ App. User and/or Group
Not □ OS User and/or Group
Not □ Src App. and/or Group
Not □ Field and/or Group □ Every
Not □ Object and/or Group □ Every
Not □ Command and/or Group □ Every

- Removed cluttering UI
  - Allow user to add or delete parameter with '-' and '+' button
  - Indicates required parameter by showing red textbox
  - Some rule type has predefined criteria

Example of prepopulated criteria



Create New Rule

Rule definition ✓

DB2 z/OS Blocking Profile rule example

Rule criteria *Conditions where rule action will be trigged*

Session level criteria

Service name	In Group	*Select a group*
Database name	In Group	*Select a group*
Database user	In Group	*Select a group*
Client IP address	In Group	*Select a group*

SQL criteria

Object	In Group	*Select a group*

Rule action ✓

Number of actions: 1

Prepopulated criteria based on selected rule type

Required parameters will be displayed as red textbox

What is session level policy?

- New rule types introduced in 10.6 which define a policy based on session criteria
- Improved performance because validation occurs at beginning of sniffer processing
- The policies with session rule type will be installed before regular policies

What is it useful for?

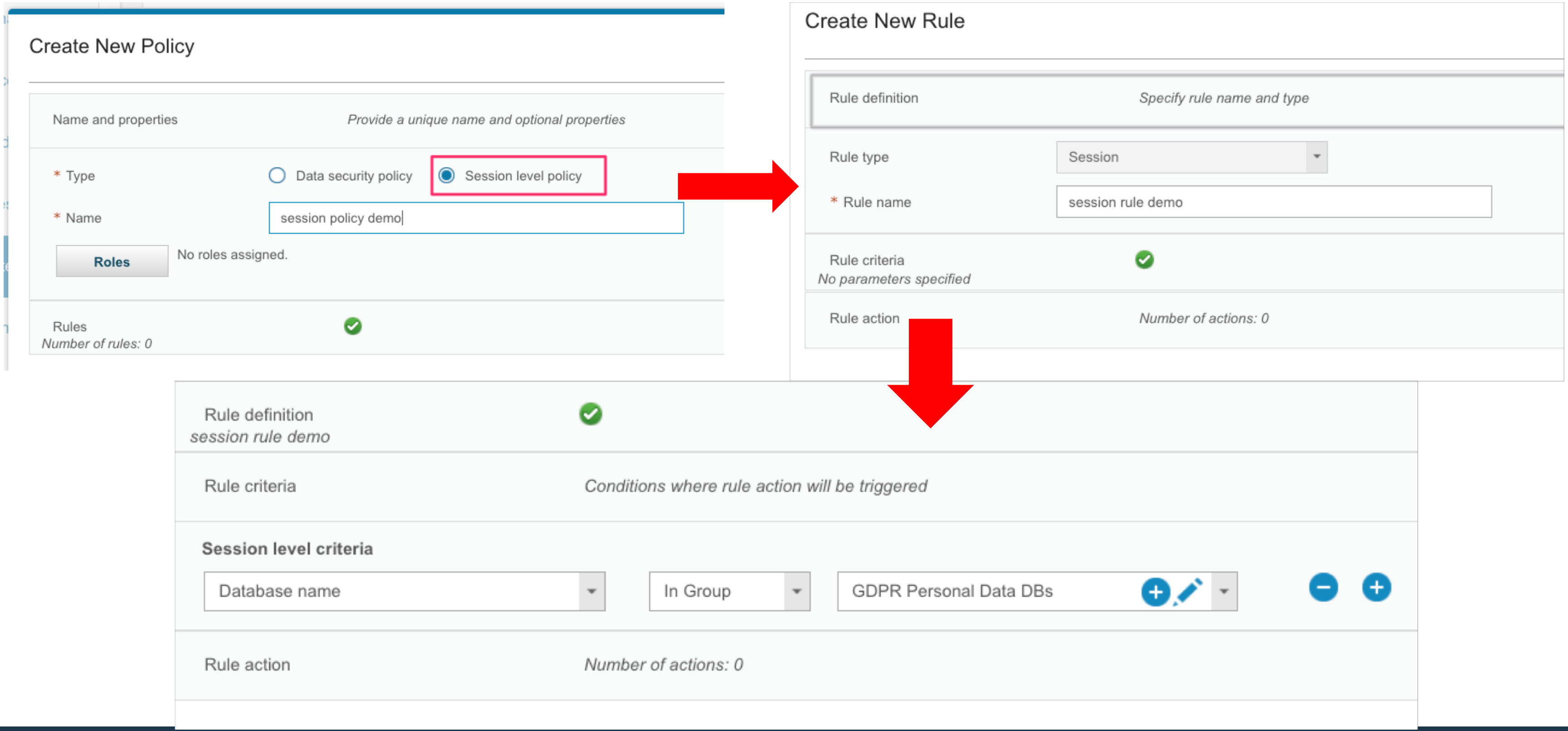
1. Decrease the load on collector
   - Trusted session scenario: policy rule to ignore sessions from certain IP address
   - Policy with rule to ignore non-privileged user S-TAP session

2. Optimizing firewall
   - Restrict database user from using a certain program by terminating session.
   - Restrict database user to access from certain IP addresses by terminating session.

   Without session level rules, reaction based on SQL requests which could do harm.

Flow of session level policy

- Once the policy is saved as ‘Session level policy’, it cannot be switched over to ‘Data security policy’
- Unlike access policy, it allows user to only define criteria based on session



Create New Policy

Name and properties — *Provide a unique name and optional properties*

* Type ○ Data security policy ● Session level policy

* Name: session policy demo

Roles — No roles assigned.

Rules ✓
Number of rules: 0

Create New Rule

Rule definition — *Specify rule name and type*

Rule type: Session

* Rule name: session rule demo

Rule criteria ✓
No parameters specified

Rule action — *Number of actions: 0*

Rule definition ✓
session rule demo

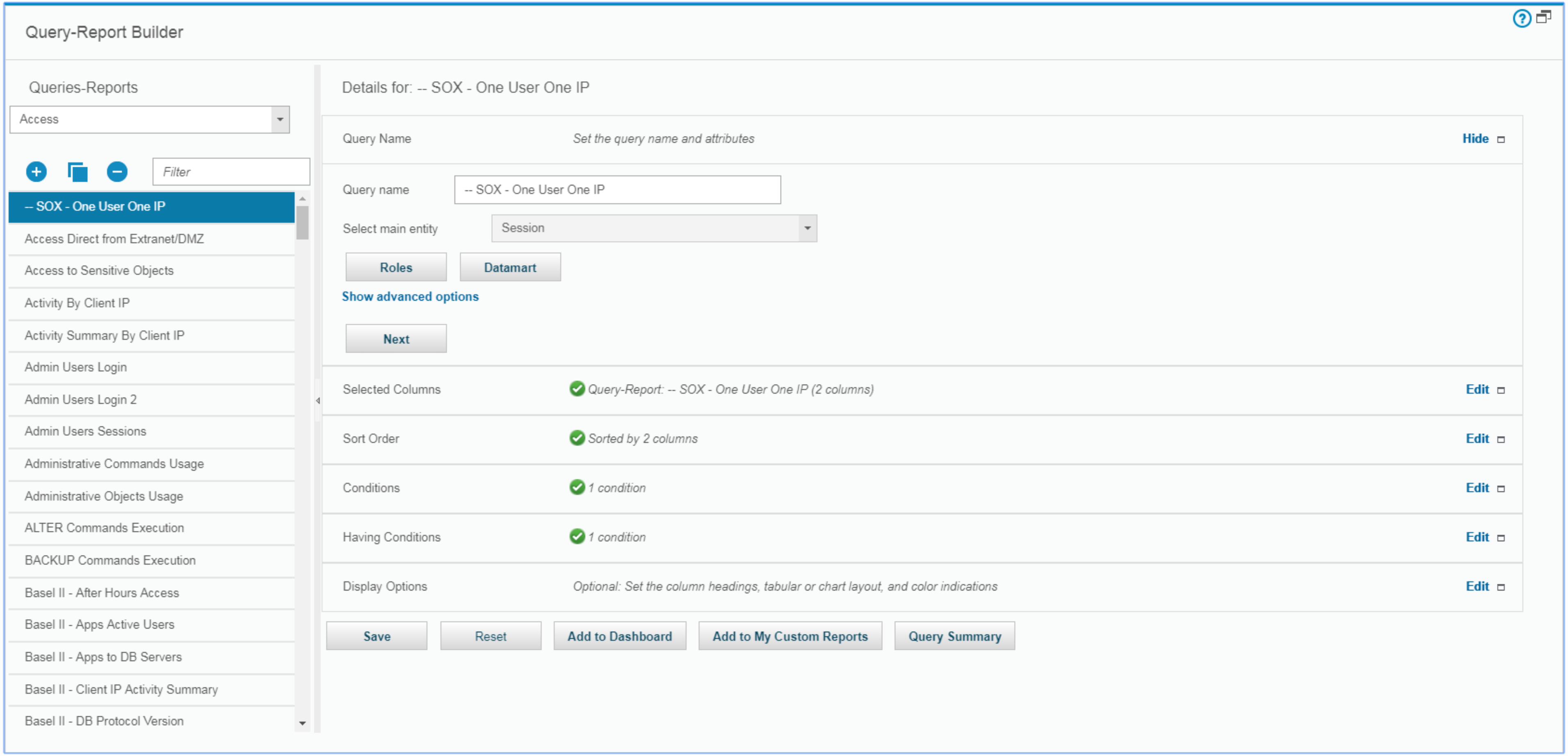
Rule criteria — *Conditions where rule action will be triggered*

Session level criteria

Database name | In Group | GDPR Personal Data DBs

Rule action — *Number of actions: 0*

New Query-Report Builder Screen Structure



Query-Report Builder

Queries-Reports

Access

Filter

- -- SOX - One User One IP
- Access Direct from Extranet/DMZ
- Access to Sensitive Objects
- Activity By Client IP
- Activity Summary By Client IP
- Admin Users Login
- Admin Users Login 2
- Admin Users Sessions
- Administrative Commands Usage
- Administrative Objects Usage
- ALTER Commands Execution
- BACKUP Commands Execution
- Basel II - After Hours Access
- Basel II - Apps Active Users
- Basel II - Apps to DB Servers
- Basel II - Client IP Activity Summary
- Basel II - DB Protocol Version

Details for: -- SOX - One User One IP

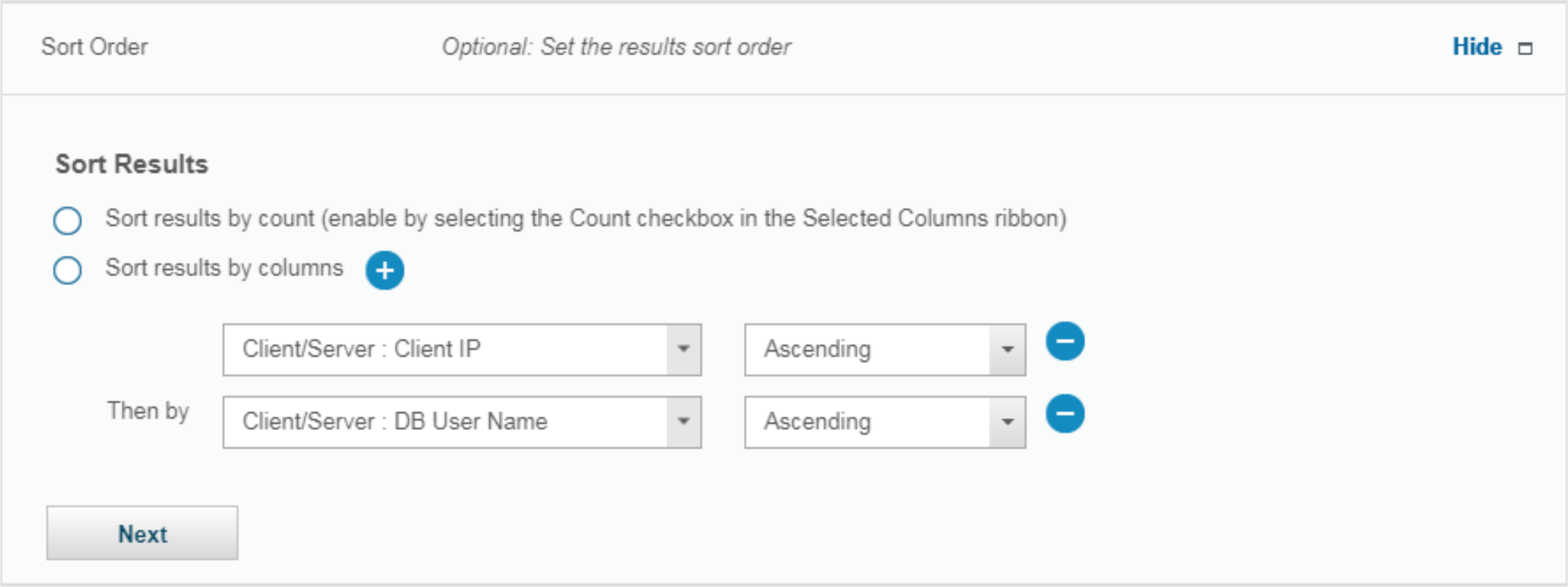
Query Name — *Set the query name and attributes* — Hide

Query name: -- SOX - One User One IP

Select main entity: Session

Selected Columns	✓ *Query-Report: -- SOX - One User One IP (2 columns)*	Edit
Sort Order	✓ *Sorted by 2 columns*	Edit
Conditions	✓ *1 condition*	Edit
Having Conditions	✓ *1 condition*	Edit
Display Options	*Optional: Set the column headings, tabular or chart layout, and color indications*	Edit

Sort Order



Sort Order *Optional: Set the results sort order* Hide

Sort Results

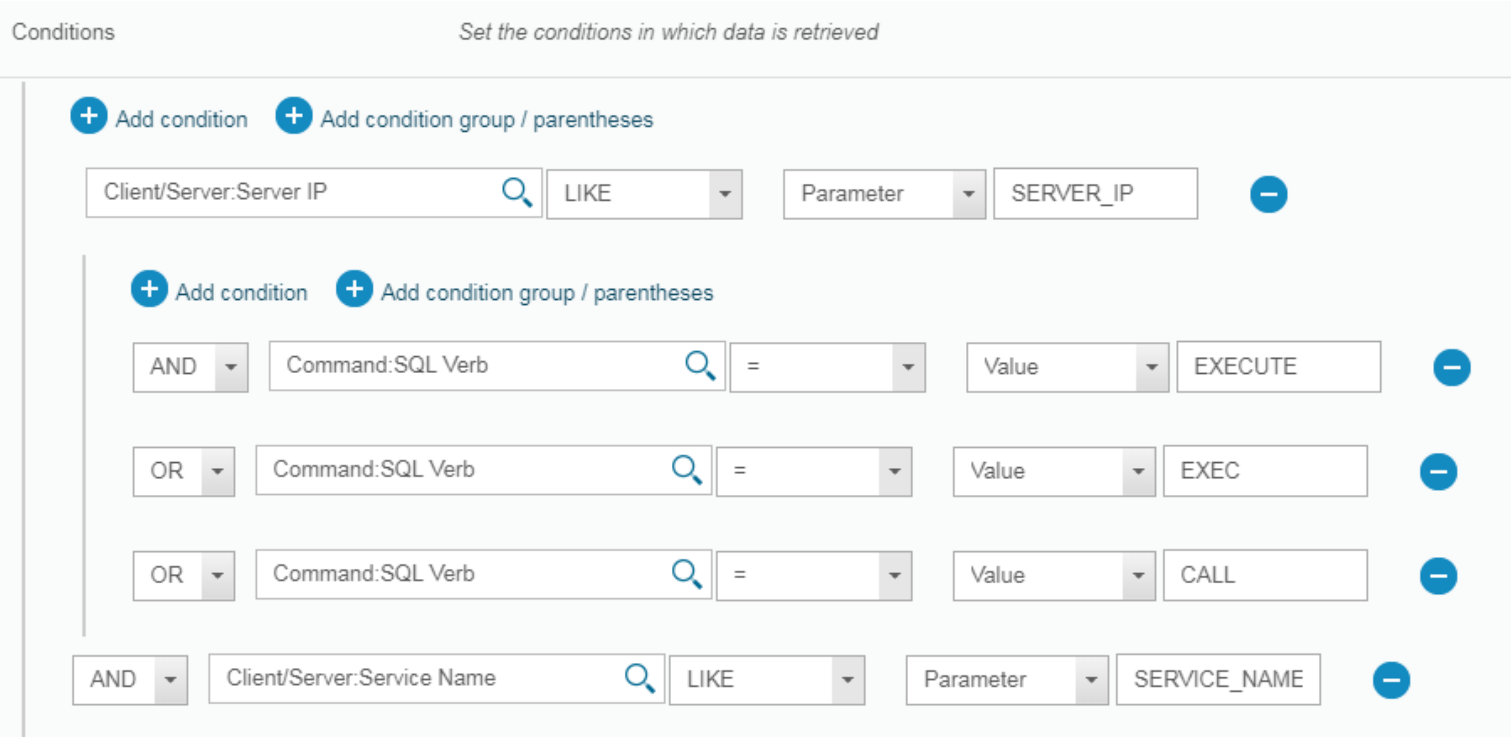
○ Sort results by count (enable by selecting the Count checkbox in the Selected Columns ribbon)

○ Sort results by columns

Client/Server : Client IP — Ascending

Then by Client/Server : DB User Name — Ascending

Complex Conditions – Condition Group


+ Add condition
+ Add condition group / parentheses
+ Add condition
+ Add condition group / parentheses

Conditions *Set the conditions in which data is retrieved*

Client/Server:Server IP LIKE Parameter SERVER_IP

AND Command:SQL Verb = Value EXECUTE

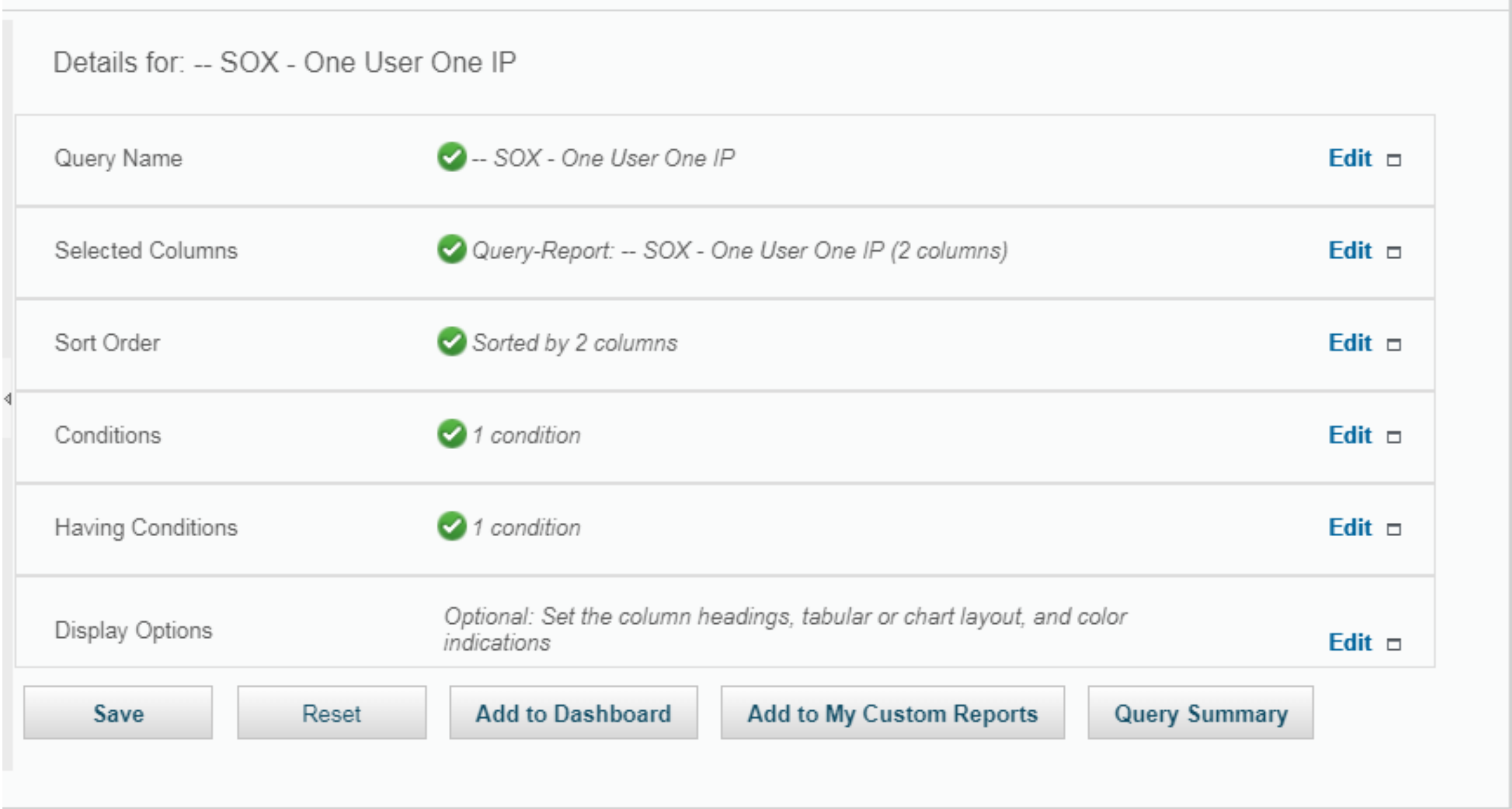
OR Command:SQL Verb = Value EXEC

OR Command:SQL Verb = Value CALL

AND Client/Server:Service Name LIKE Parameter SERVICE_NAME

Server IP like SERVER_IP AND (SQL Verb= ‘EXECUTE’ OR SQL Verb = ‘EXEC’ OR SQL Verb = ‘CALL) AND Service Name like SERVICE_NAME

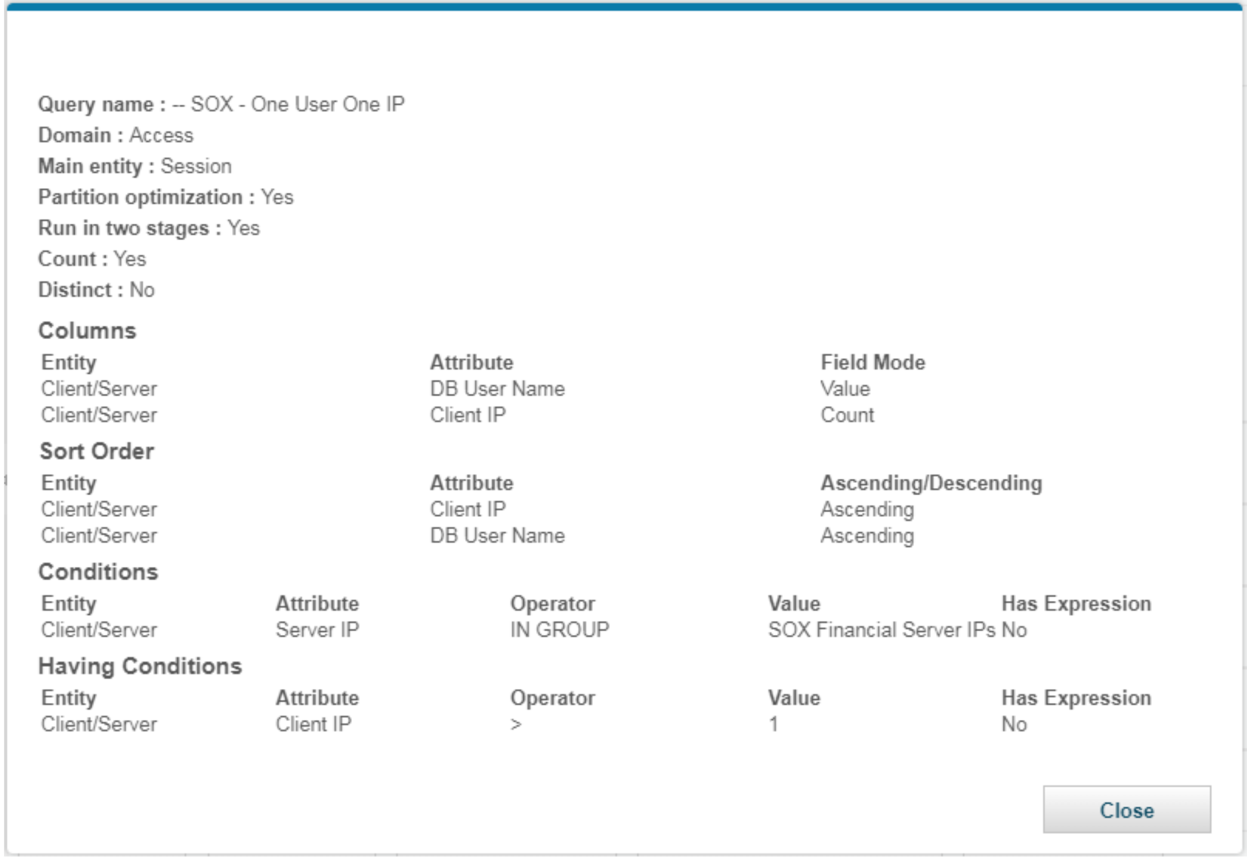
Screen Buttons



Details for: -- SOX - One User One IP

Query Name	✓ *-- SOX - One User One IP*	Edit □
Selected Columns	✓ *Query-Report: -- SOX - One User One IP (2 columns)*	Edit □
Sort Order	✓ *Sorted by 2 columns*	Edit □
Conditions	✓ *1 condition*	Edit □
Having Conditions	✓ *1 condition*	Edit □
Display Options	*Optional: Set the column headings, tabular or chart layout, and color indications*	Edit □

Query Summary



Query name : -- SOX - One User One IP
Domain : Access
Main entity : Session
Partition optimization : Yes
Run in two stages : Yes
Count : Yes
Distinct : No

Columns

Entity	Attribute	Field Mode
Client/Server	DB User Name	Value
Client/Server	Client IP	Count

Sort Order

Entity	Attribute	Ascending/Descending
Client/Server	Client IP	Ascending
Client/Server	DB User Name	Ascending

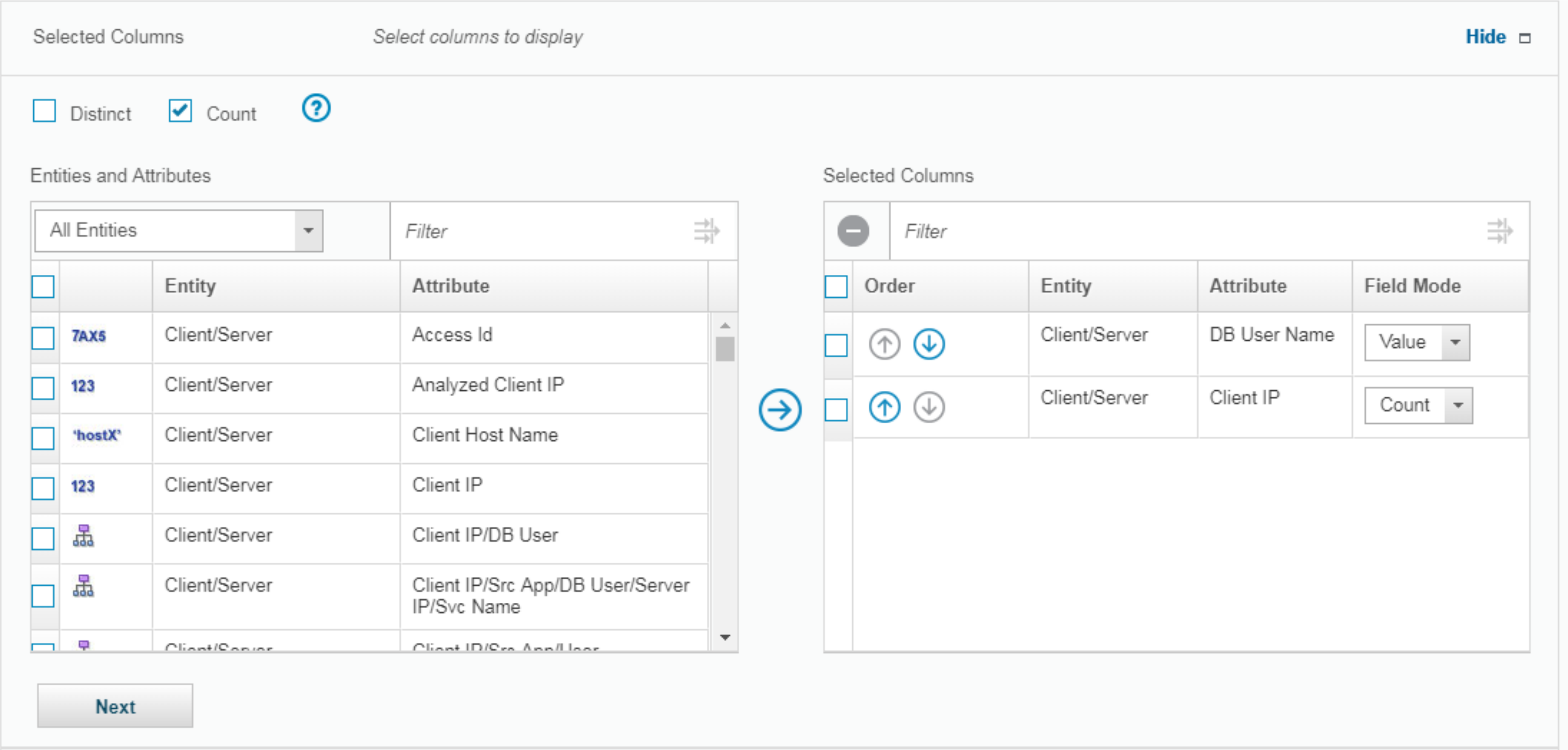
Conditions

Entity	Attribute	Operator	Value	Has Expression
Client/Server	Server IP	IN GROUP	SOX Financial Server IPs	No

Having Conditions

Entity	Attribute	Operator	Value	Has Expression
Client/Server	Client IP	>	1	No

Columns



Selected Columns *Select columns to display* **Hide**

□ Distinct ☑ Count ?

Entities and Attributes

All Entities ▾ | *Filter*

□		Entity	Attribute
□	7AX5	Client/Server	Access Id
□	123	Client/Server	Analyzed Client IP
□	'hostX'	Client/Server	Client Host Name
□	123	Client/Server	Client IP
□		Client/Server	Client IP/DB User
□		Client/Server	Client IP/Src App/DB User/Server IP/Svc Name
□		Client/Server	Client IP/Src App/User

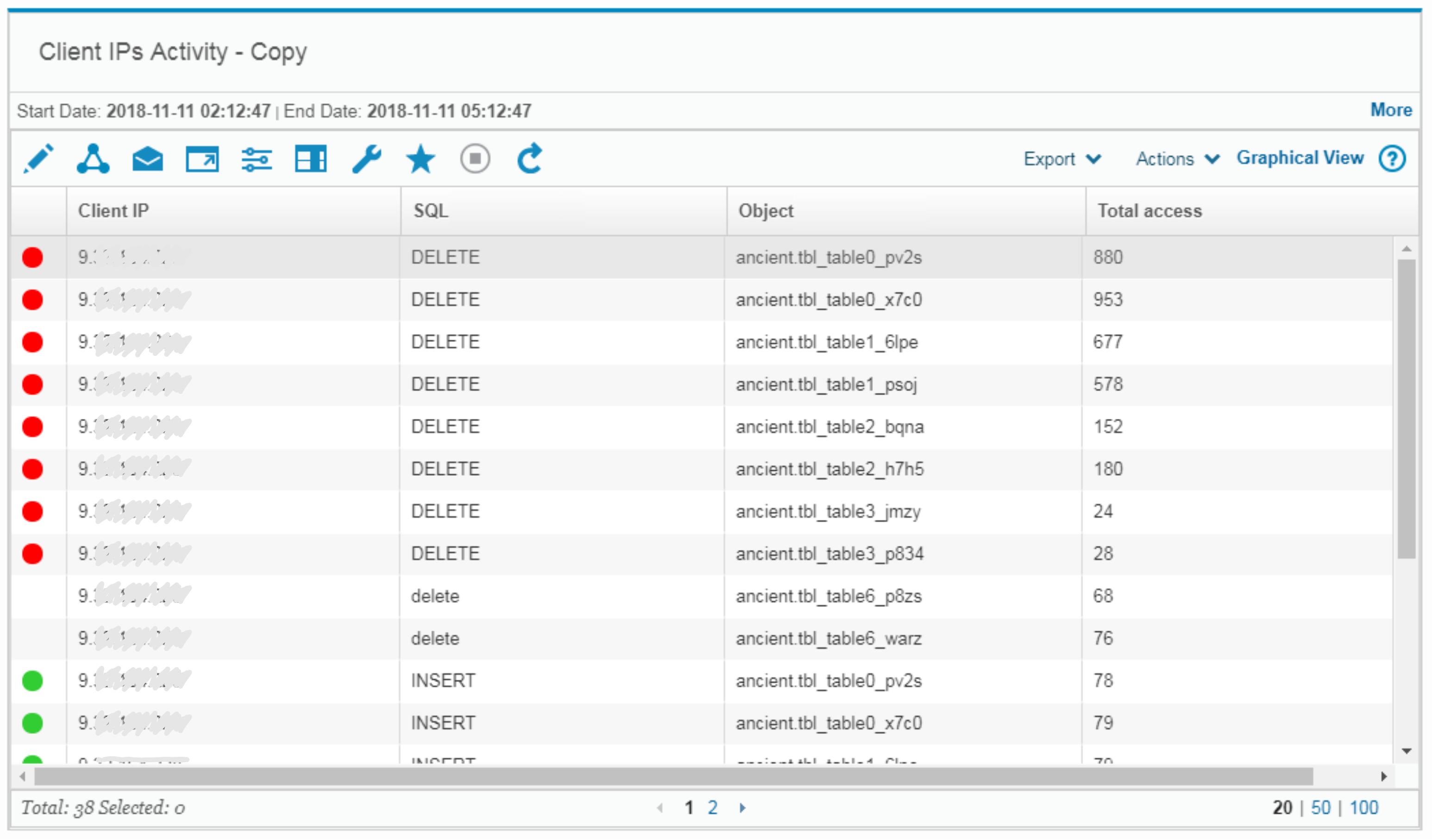
Selected Columns

Filter

□	Order	Entity	Attribute	Field Mode
□	↑ ↓	Client/Server	DB User Name	Value ▾
□	↑ ↓	Client/Server	Client IP	Count ▾

Next

Display Options – Tabular Report



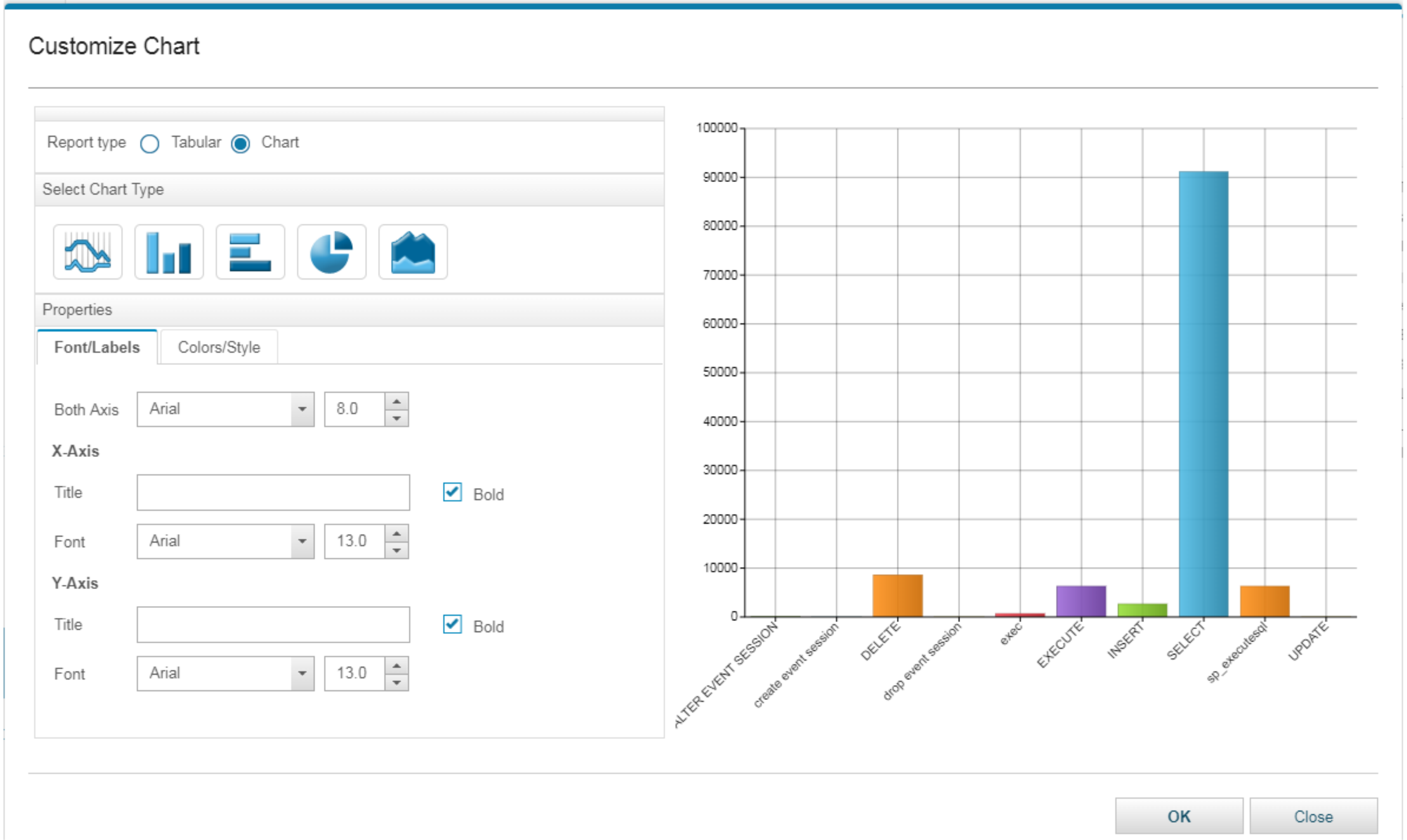
Client IPs Activity - Copy

Start Date: **2018-11-11 02:12:47** | End Date: **2018-11-11 05:12:47**

	Client IP	SQL	Object	Total access
●	9.[redacted]	DELETE	ancient.tbl_table0_pv2s	880
●	9.[redacted]	DELETE	ancient.tbl_table0_x7c0	953
●	9.[redacted]	DELETE	ancient.tbl_table1_6lpe	677
●	9.[redacted]	DELETE	ancient.tbl_table1_psoj	578
●	9.[redacted]	DELETE	ancient.tbl_table2_bqna	152
●	9.[redacted]	DELETE	ancient.tbl_table2_h7h5	180
●	9.[redacted]	DELETE	ancient.tbl_table3_jmzy	24
●	9.[redacted]	DELETE	ancient.tbl_table3_p834	28
	9.[redacted]	delete	ancient.tbl_table6_p8zs	68
	9.[redacted]	delete	ancient.tbl_table6_warz	76
●	9.[redacted]	INSERT	ancient.tbl_table0_pv2s	78
●	9.[redacted]	INSERT	ancient.tbl_table0_x7c0	79

Total: 38 Selected: 0

Display Options – Chart



Customize Chart

Report type ○ Tabular ● Chart

Select Chart Type

Properties

Font/Labels | Colors/Style

Both Axis: Arial 8.0

X-Axis

Title: ☑ Bold

Font: Arial 13.0

Y-Axis

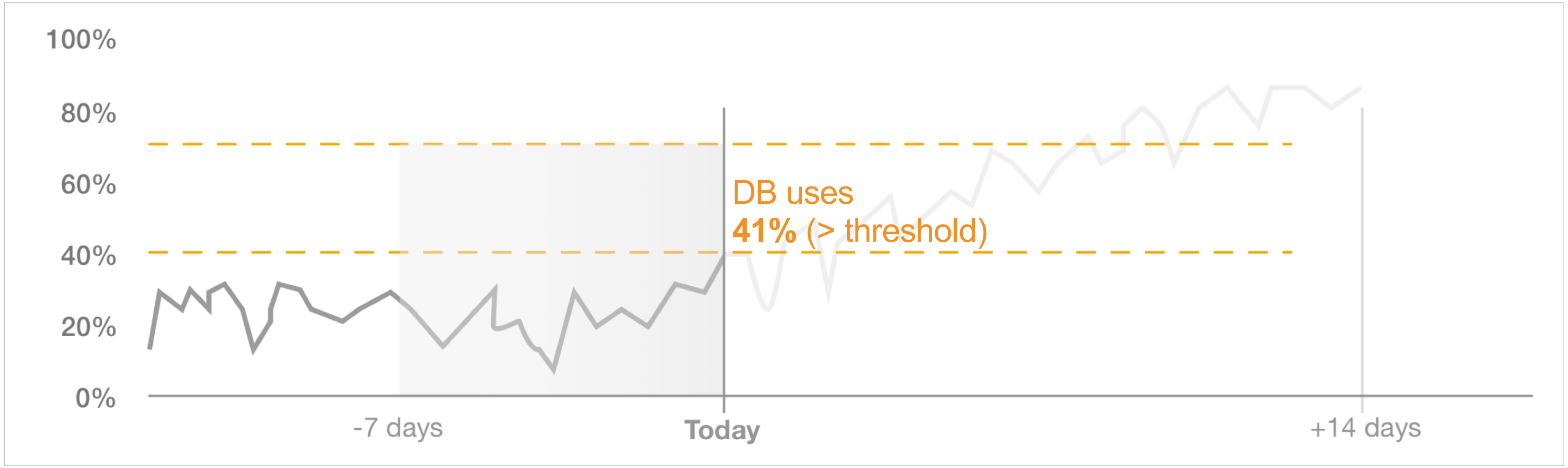
Title: ☑ Bold

Font: Arial 13.0

Disk Full prevention – Before 10.6

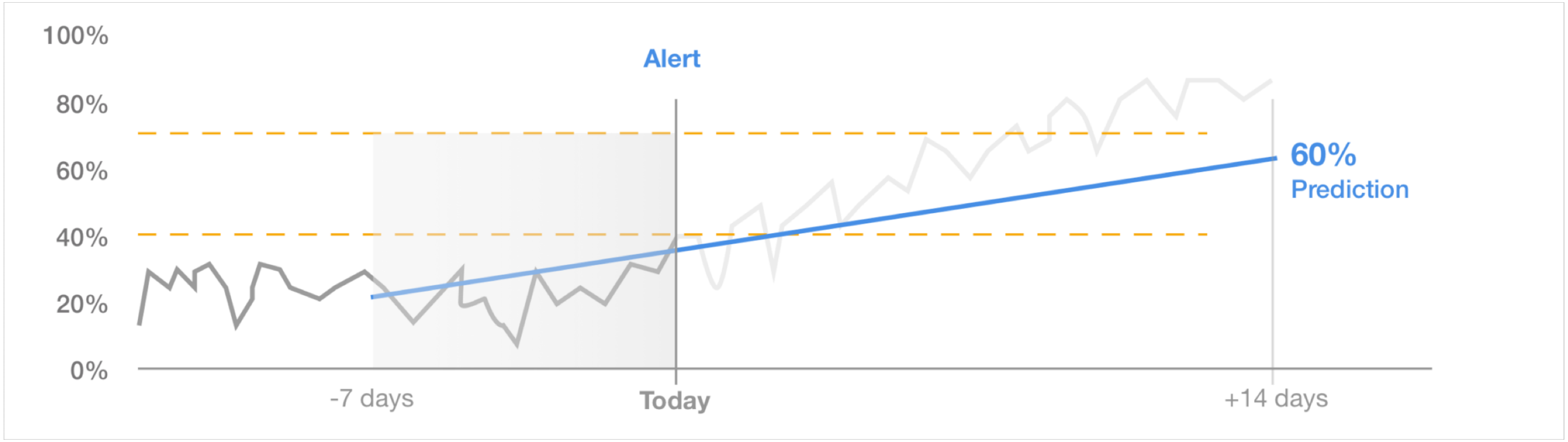
- Problem: Low disk space can lead to Guardium system failure.

- Solution before Guardium 10.6:
  Alert when disk or database usage > threshold 1 or threshold 2, or create custom correlation alert
  - Severity? Time left to no disk space?



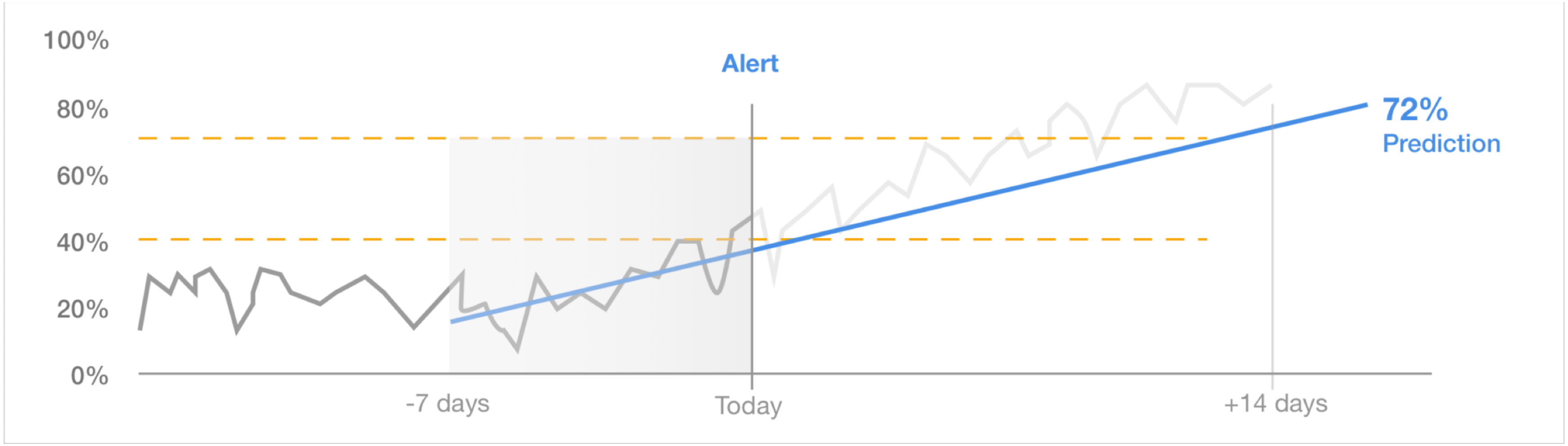
Disk Full prevention – New in 10.6

- **Disk & Database Health Analyzer triggers an alert ahead of time** if disk usage or database size are expected to reach over 50% within 2 weeks or less.
  - Daily alert; based on statistics from last 7 days.



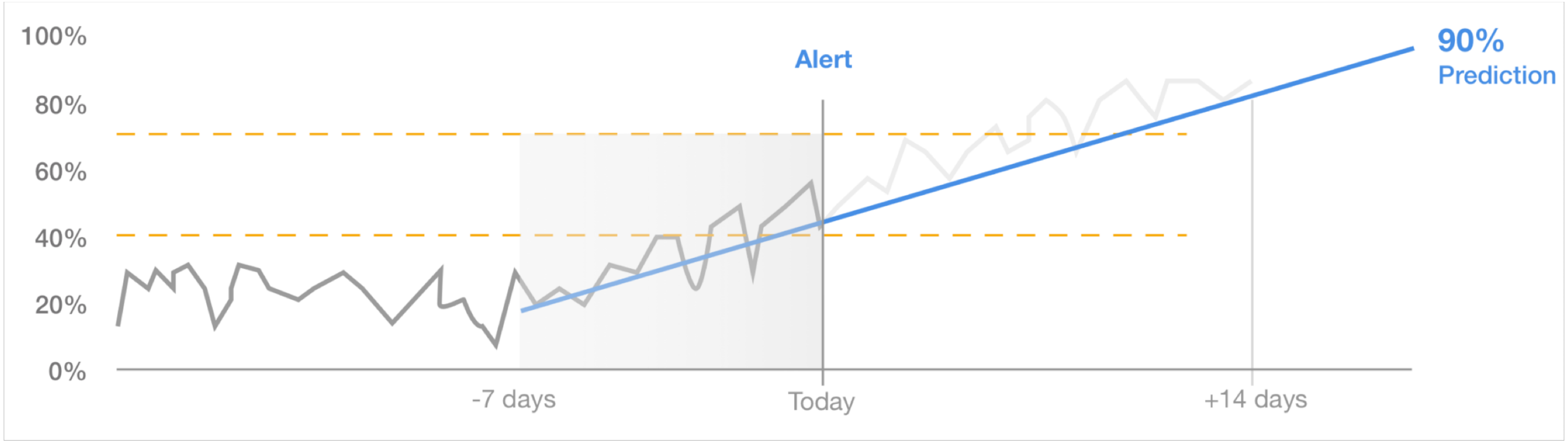
Disk Full prevention – New in 10.6

- If the problem persists, the predicted value will reflect it, the next day:



Disk Full prevention – New in 10.6

- If the problem persists, the predicted value will reflect it, the next day
- Alert details top files or table sizes
- In 10.6 this code runs on collectors only, post 10.6 we'll add to aggregators and CM



Database size alert (email)

From: DB Size alert

Subject: **Disk is getting full!**

DB size is estimated to exceed 50% of its recommended size in 14 days (reaching 63%), which may lead to space and stability problems.

Top tables:
GDM_EXCEPTION: +11 MB in last 24 hours; current size: 355 MB;
GDM_SESSION: +12 MB in last 24 hours; current size: 200 MB;
GDM_POLICY_VIOLATIONS_LOG: +2 MB in last 24 hours; current size: 5 MB;
…

For causes and actions you can take, see the Technote http://www-01.ibm.com/support/docview.wss?uid=swg21696497.

Disk space usage alert (email)

From: DB Size alert

Subject: **Disk is getting full!**

Disk space used in /var is estimated to exceed 50% in 14 days (reaching 74%), which may lead to space and stability problems.

Top files:

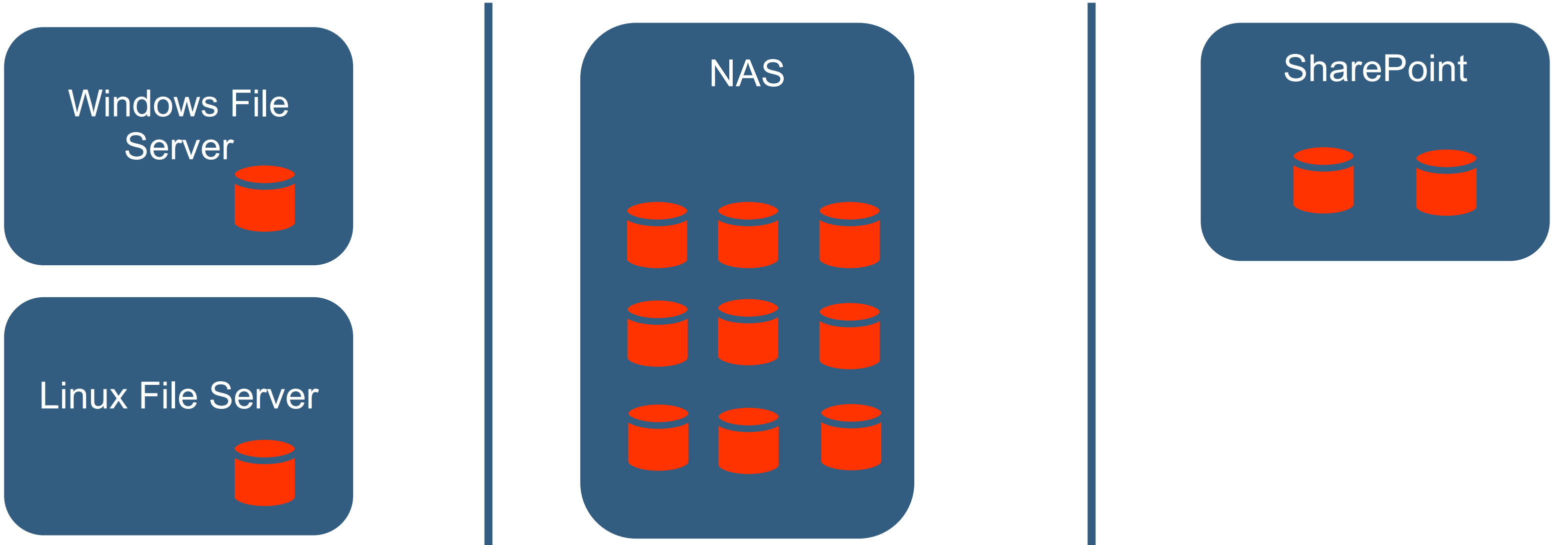
2304837875 Wed 25 Jul 2018 … /var/com/IBM/Guardium/…
190474334 Tue 24 Jul 2018 … /var/….log
190474334 Tue 24 Jul 2018 … /var/….log2

…

To find more and delete large files, see the Technote http://www-01.ibm.com/support/docview.wss?uid=swg21995197

What’s FAM

- **File Access Monitoring -**The discovery, classification and monitoring of unstructured data (files) as opposed to structured data which relies in databases
- **If it’s not on databases, where is the data?**



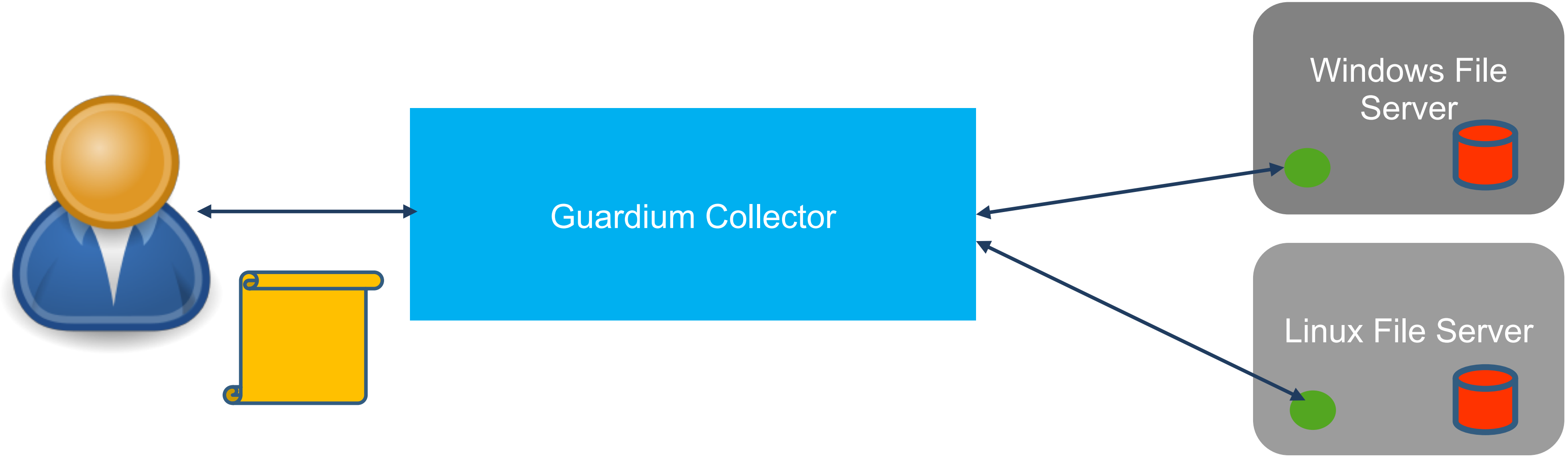
File server – A pizza box with internal or external disk

A Box attached to a storage array that exports several FS

File server with software to abstract and manage the files

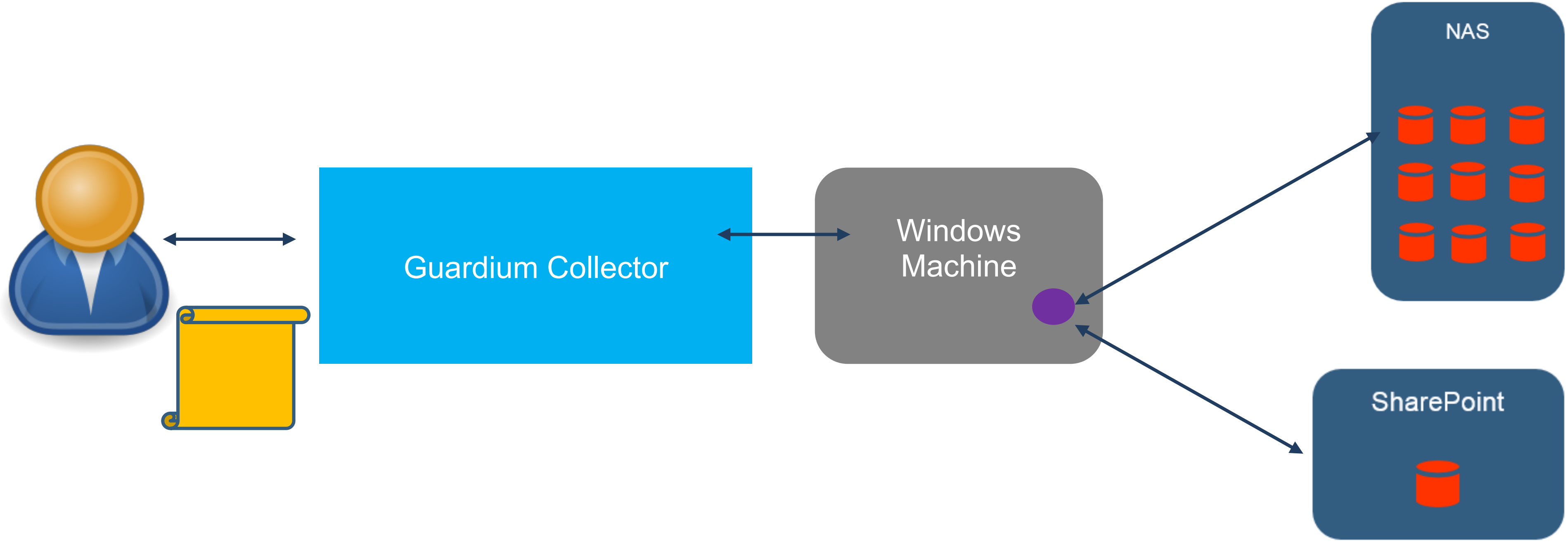
What does Guardium support natively?

- **File server –** An agent (like STAP) is sitting on a file server, crawls the file system and sends data to the collector about files it finds and it also classifies the data and monitor access (open/close/modify etc.) to the files

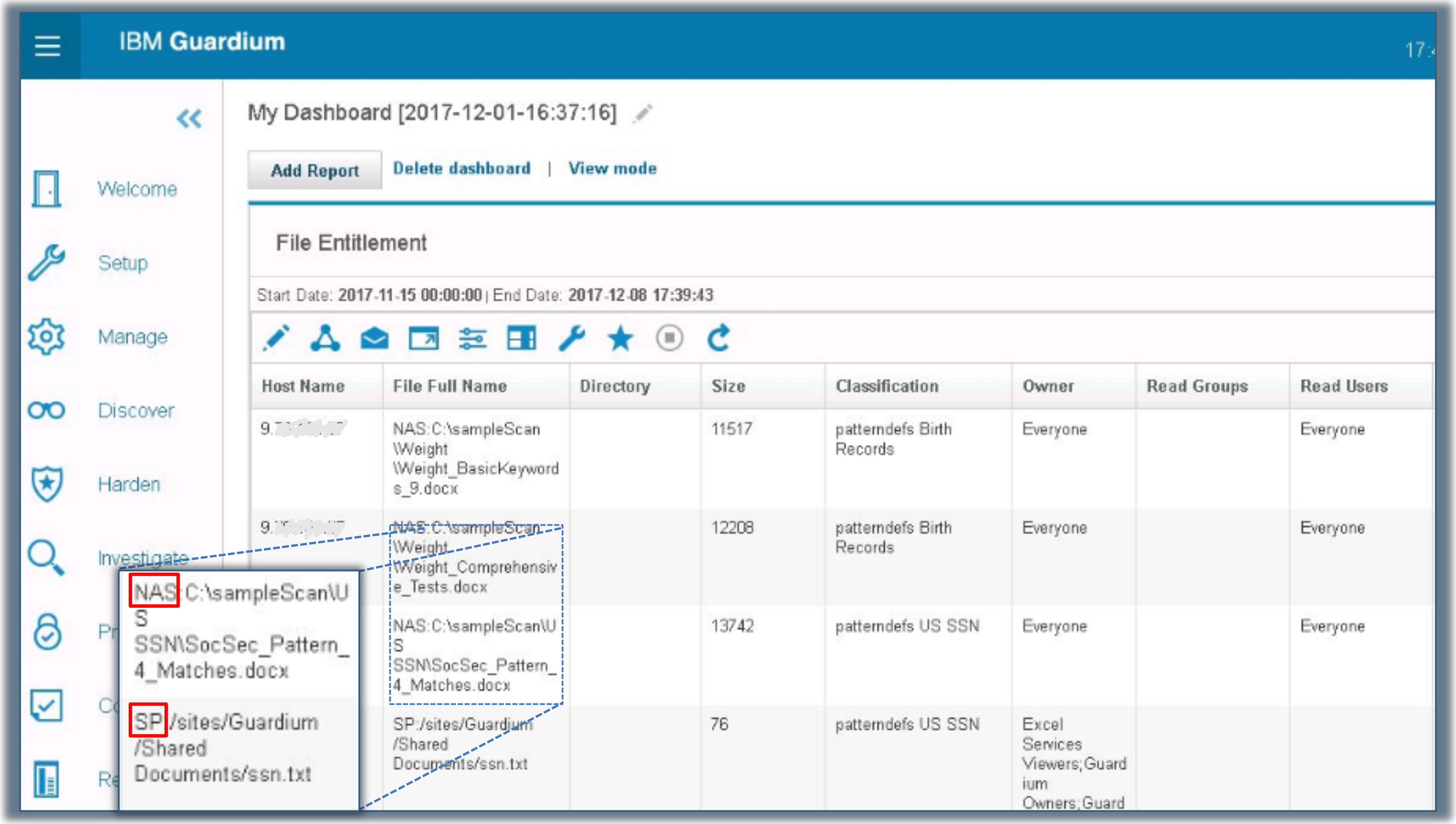


Partnering with Stealthbits

- **We use Stealthbits for Sharepoint and NAS** - A Stealthbits agent sits on a dedicated Windows box and scans Sharepoint servers and/or NAS servers and sends the results to the collector and from there everything works the same as the previous use case



FDEC Report: File Entitlement



My Dashboard [2017-12-01-16:37:16]

File Entitlement

Start Date: 2017-11-15 00:00:00 | End Date: 2017-12-08 17:39:43

Host Name	File Full Name	Directory	Size	Classification	Owner	Read Groups	Read Users
9.[redacted]	NAS:C:\sampleScan\Weight\Weight_BasicKeywords_9.docx		11517	patterndefs Birth Records	Everyone		Everyone
9.[redacted]	NAS:C:\sampleScan\Weight\Weight_Comprehensive_Tests.docx		12208	patterndefs Birth Records	Everyone		Everyone
	NAS:C:\sampleScan\US SSN\SocSec_Pattern_4_Matches.docx		13742	patterndefs US SSN	Everyone		Everyone
	SP:/sites/Guardium/Shared Documents/ssn.txt		76	patterndefs US SSN	Excel Services Viewers;Guardium Owners;Guard		

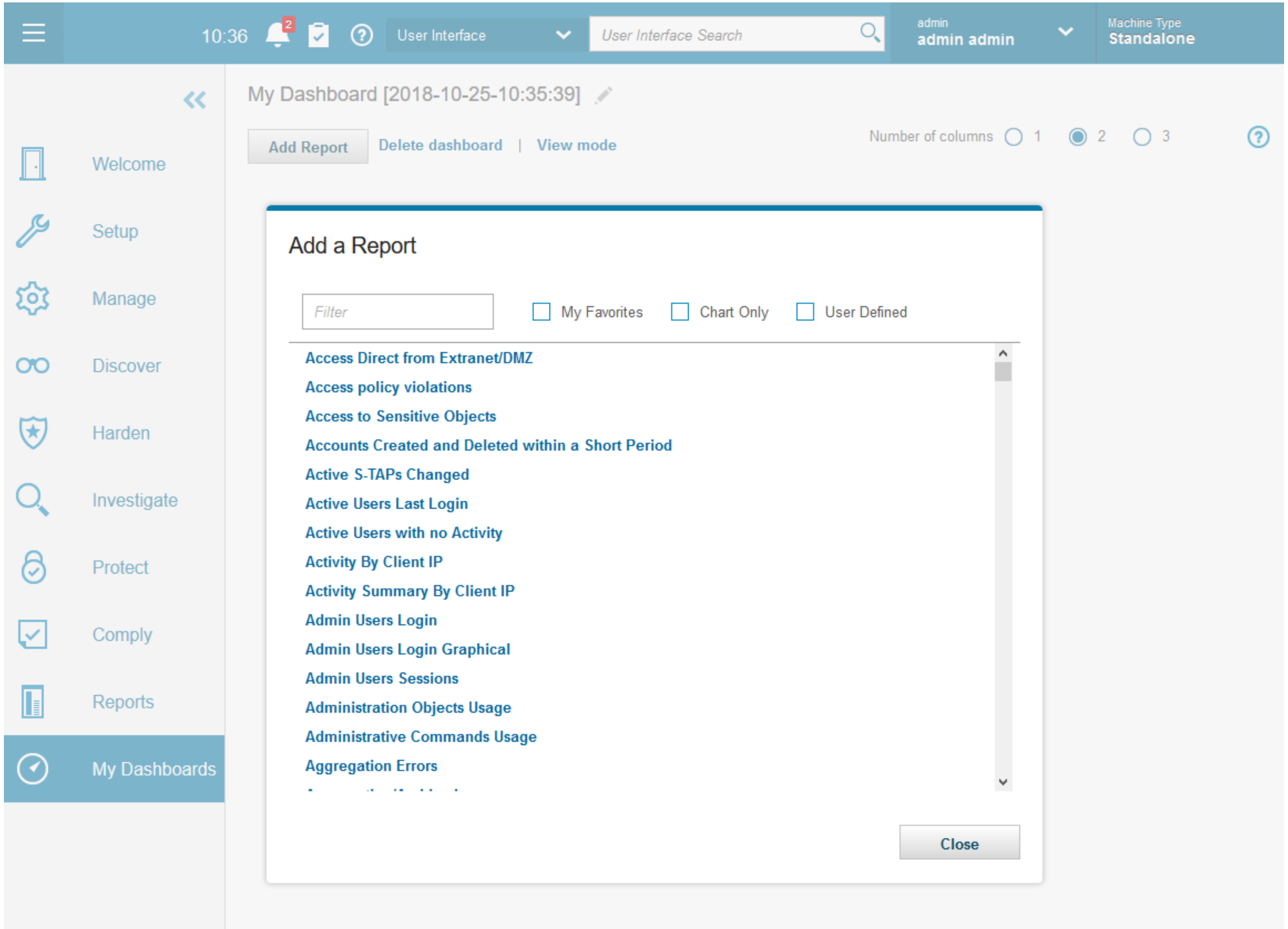
NAS C:\sampleScan\US SSN\SocSec_Pattern_4_Matches.docx

SP /sites/Guardium/Shared Documents/ssn.txt

But hold on, some of it was there in 10.5, right?

10.6 Now adds **monitoring** on top of the previous classification and entitlement capabilities

FAM: My Dashboard



My Dashboard [2018-10-25-10:35:39]

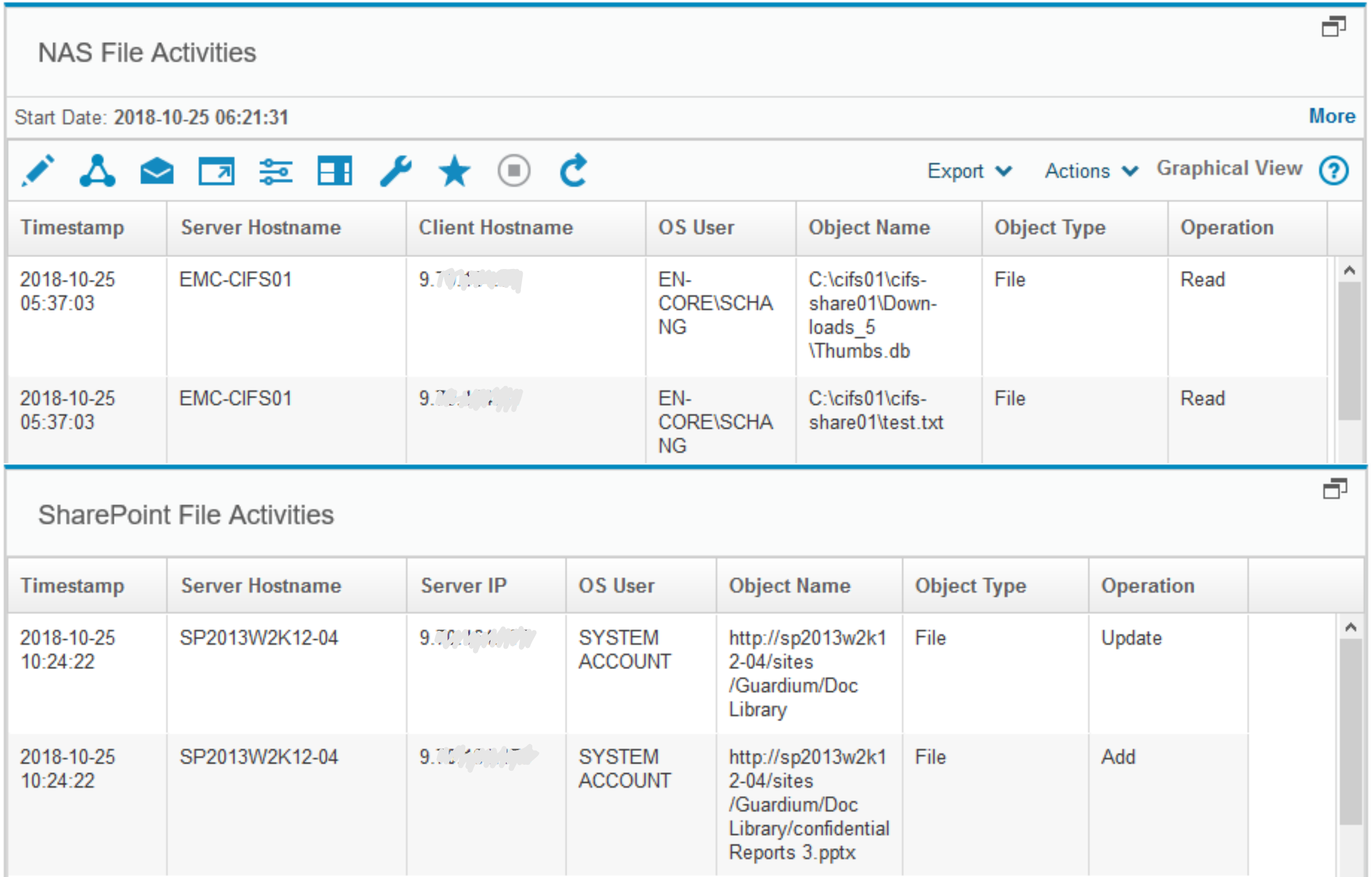
Number of columns ○ 1 ● 2 ○ 3

Add a Report

Filter ☐ My Favorites ☐ Chart Only ☐ User Defined

Access Direct from Extranet/DMZ
Access policy violations
Access to Sensitive Objects
Accounts Created and Deleted within a Short Period
Active S-TAPs Changed
Active Users Last Login
Active Users with no Activity
Activity By Client IP
Activity Summary By Client IP
Admin Users Login
Admin Users Login Graphical
Admin Users Sessions
Administration Objects Usage
Administrative Commands Usage
Aggregation Errors

FAM Reports



NAS File Activities

Start Date: **2018-10-25 06:21:31**

Timestamp	Server Hostname	Client Hostname	OS User	Object Name	Object Type	Operation
2018-10-25 05:37:03	EMC-CIFS01	9.[redacted]	EN-CORE\SCHANG	C:\cifs01\cifs-share01\Down-loads_5\Thumbs.db	File	Read
2018-10-25 05:37:03	EMC-CIFS01	9.[redacted]	EN-CORE\SCHANG	C:\cifs01\cifs-share01\test.txt	File	Read

SharePoint File Activities

Timestamp	Server Hostname	Server IP	OS User	Object Name	Object Type	Operation
2018-10-25 10:24:22	SP2013W2K12-04	9.[redacted]	SYSTEM ACCOUNT	http://sp2013w2k12-04/sites/Guardium/Doc Library	File	Update
2018-10-25 10:24:22	SP2013W2K12-04	9.[redacted]	SYSTEM ACCOUNT	http://sp2013w2k12-04/sites/Guardium/Doc Library/confidential Reports 3.pptx	File	Add

New GIM Enhancements Quick Summary

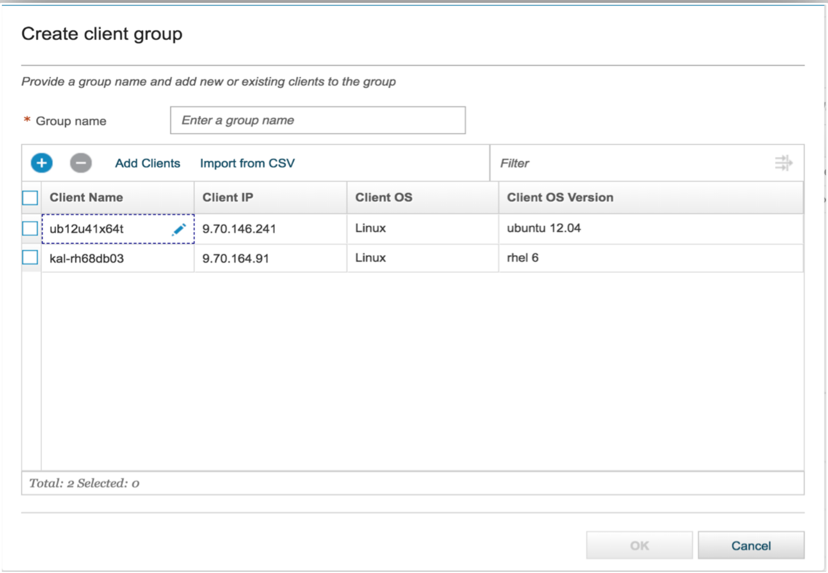
- Improved interaction for creating new client groups, including import from CSV
- Ability to view installed modules before selecting clients
  - A dialog which displays information cross client which is filterable and refreshable
- Notifying if GIM process is not running on some client
- Bundle action shown in configure clients
  - Provides Overall summary in one section rather than 2 sections for easier skimming and verification
- Displaying status for the module sent for installation/uninstallation
- Ability to generate Guard API across clients vs. only 1 client as in legacy UI

Note: All the enhancements are customer requests/pain points which have been gathered through various customer feedback sessions

GIM Group Builder

- Shows only the members of the group as compared to 10.5 behavior where it showed all the clients
- It has two new features, Add Clients and Import from CSV
- Through Add Clients, the user gets a list of non member client to select to add to the group
- The Import From CSV enables the user to import members from a CSV file

New UI



Create client group

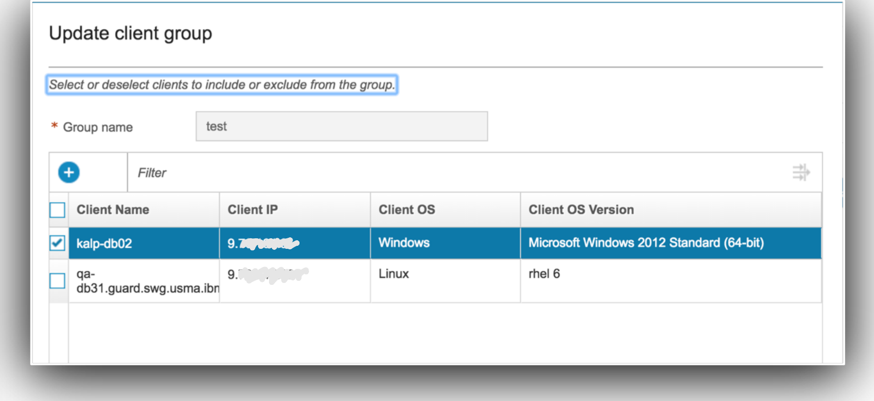
Provide a group name and add new or existing clients to the group

* Group name: *Enter a group name*

□	Client Name	Client IP	Client OS	Client OS Version
□	ub12u41x64t	9.70.146.241	Linux	ubuntu 12.04
□	kal-rh68db03	9.70.164.91	Linux	rhel 6

Total: 2 Selected: 0

10.5 UI



Update client group

Select or deselect clients to include or exclude from the group.

* Group name: test

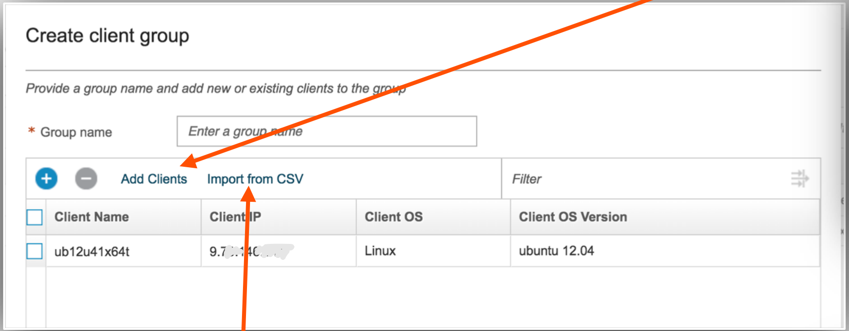
□	Client Name	Client IP	Client OS	Client OS Version
☑	kalp-db02	9.7[redacted]	Windows	Microsoft Windows 2012 Standard (64-bit)
□	qa-db31.guard.swg.usma.ibn	9.[redacted]	Linux	rhel 6

GIM Group Builder

New UI

Shows only the members of the group

The “Add Clients” Button displays all the clients which are not part of the group and allows you to add them as a part of the group.

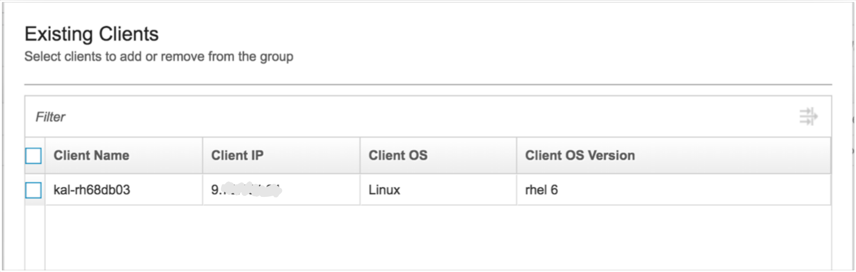


Create client group

Provide a group name and add new or existing clients to the group

* Group name *Enter a group name*

□	Client Name	Client IP	Client OS	Client OS Version
□	ub12u41x64t	9.7[redacted]	Linux	ubuntu 12.04



Existing Clients

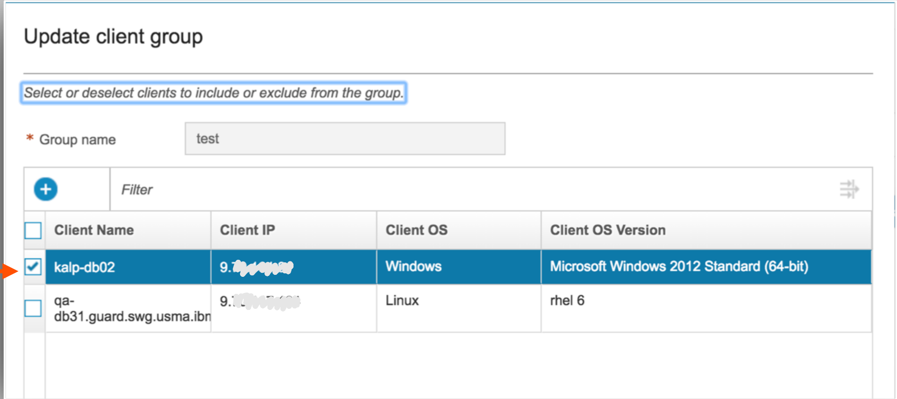
Select clients to add or remove from the group

□	Client Name	Client IP	Client OS	Client OS Version
□	kal-rh68db03	9.[redacted]	Linux	rhel 6

10.5 UI

“Import from CSV” allows you to import group members from a CSV file

10.5 UI showed all the clients and the members were auto selected to distinguish them as members



Update client group

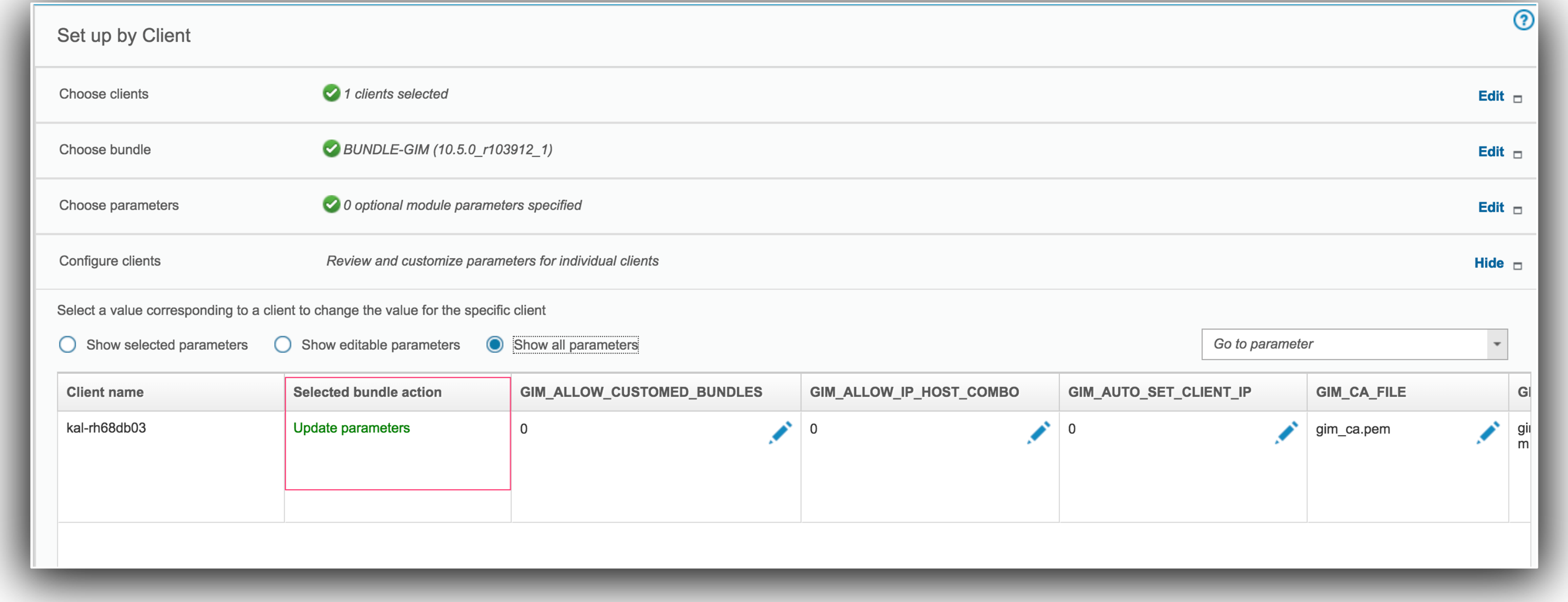
Select or deselect clients to include or exclude from the group.

* Group name test

□	Client Name	Client IP	Client OS	Client OS Version
☑	kalp-db02	9.[redacted]	Windows	Microsoft Windows 2012 Standard (64-bit)
□	qa-db31.guard.swg.usma.ibn	9.[redacted]	Linux	rhel 6

Configure clients

- The configure clients section now has a new column which displays the bundle action
- This enables the user to see all the important information in one section before performing the install/uninstall action



Set up by Client

Choose clients	✓ *1 clients selected*	Edit
Choose bundle	✓ *BUNDLE-GIM (10.5.0_r103912_1)*	Edit
Choose parameters	✓ *0 optional module parameters specified*	Edit
Configure clients	*Review and customize parameters for individual clients*	Hide

Select a value corresponding to a client to change the value for the specific client

○ Show selected parameters ○ Show editable parameters ● Show all parameters

Go to parameter

Client name	Selected bundle action	GIM_ALLOW_CUSTOMED_BUNDLES	GIM_ALLOW_IP_HOST_COMBO	GIM_AUTO_SET_CLIENT_IP	GIM_CA_FILE	GI
kal-rh68db03	Update parameters	0	0	0	gim_ca.pem	gi m

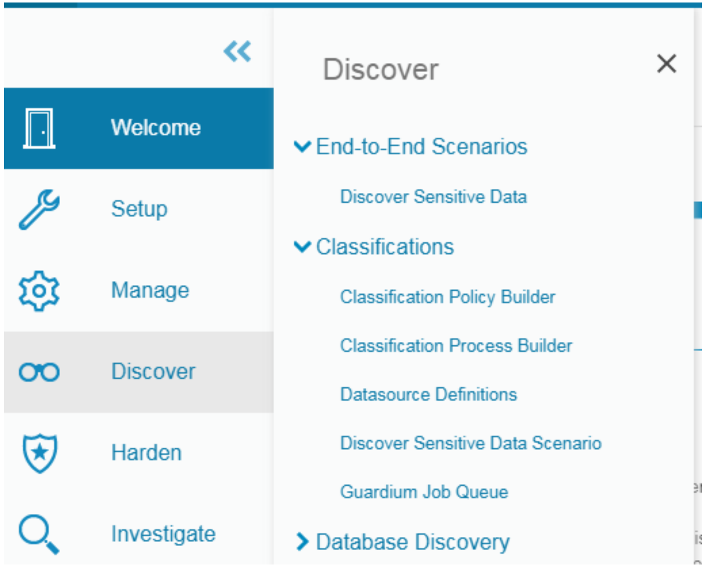
Unix STAP changes to support live update with EXIT

- This feature allows the upgrade of Guardium S-TAP while leaving databases running
- No loss of functionality or of data during S-TAP upgrade
- S-TAP upgrades can be done at any time
- Only works for EXIT - Another reason the EXIT mechanism is preferred over A-TAP
- During the period between S-TAP upgrade and all old database instances being restarted, there can be two sets of shared memory in use (so more memory consumed)
  - Only if shared memory layout changes
  - Returns to normal automatically when all old instances are shut down
- **Only shows benefit AFTER the 10.6.0.0 release!**
  - **Updating from anything before 10.6 is done the old way**

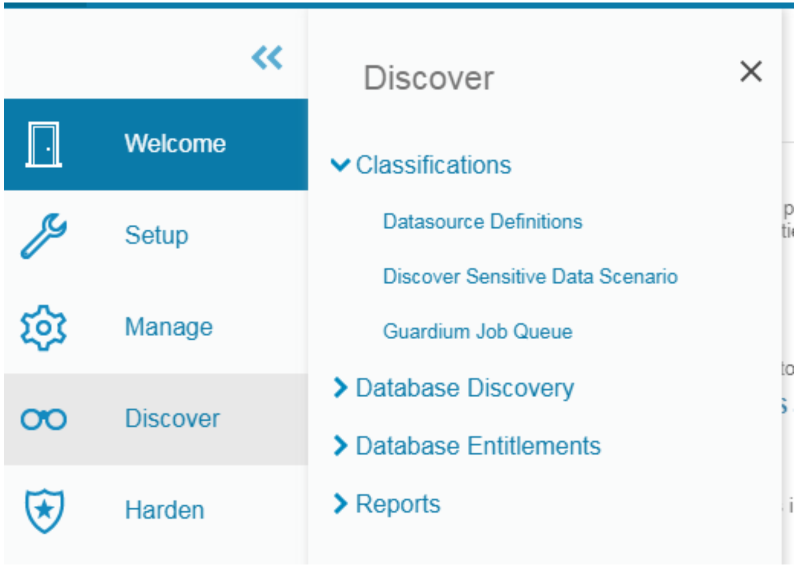
Discover Sensitive Data (AKA Classification)

- Enhancements have been made to Discover Sensitive Data (DSD) UI in 10.6 release to bring over all the functionality previously available in Classification Policy and Process builders.
- With these enhancements DSD became a complete replacement for classification policy and process builders. As a result, these builders were removed in 10.6.

10.5 Navigation Layout



10.6 Navigation Layout



VA (Vulnerability Assessment)

- VA and Classification are now **multi threaded** - Jobs can run in parallel, only limited by the CPU cores
  - (1<= N <=2* #CPU_Core and N<=100). **Execution time greatly reduced**
- New CIS benchmark for MySQL
- Support for Oracle 18c
- DB2 z/OS v12 support for VA

Miscellaneous

- Guardium can be now found in both AWS and Azure marketplace and you can use BYOL
- We now have options for better and stronger passwords so admins can force better security for the appliance. On top of that, there are more improvements to working with certificates
- We added more languages support to the UI and today Guardium can be deployed with 9 languages: Traditional Chinese, Simplified Chinese, Japanese, German, French, Spanish, Italian, Korean, Polish
- Outliers can now run on aggregators that aggregate data from more than one CM

The real fun is just starting.
Go to the backup slides for all the details

IBM Security

Thank You!

Useful Links

- What's new in 10.6: https://www.ibm.com/support/knowledgecenter/SSMPHH_10.6.0/com.ibm.guardium.doc/overview/whats_new.html

- External STAP:https://www.ibm.com/support/knowledgecenter/SSMPHH_10.6.0/com.ibm.guardium.doc.stap/proxy/proxy_overview.html

- Certificate docs: https://www.ibm.com/support/knowledgecenter/SSMPHH_10.6.0/com.ibm.guardium.doc.reference/cli_api/certificate_cli_commands.html

- Policy Builder: https://www.ibm.com/support/knowledgecenter/SSMPHH_10.6.0/com.ibm.guardium.doc/protect/building_policies.html

- Query Builder: https://www.ibm.com/support/knowledgecenter/SSMPHH_10.6.0/com.ibm.guardium.doc/reports/building_queries.html

- Great web site for overall Guardium usage: https://guardiumnotes.wordpress.com/2018/12/21/guardium-enhancements-review-10-1-3-10-6/

Videos/demos:

- Latest courses from IBM Security Learning Academy – see courses on the 10.6 **policy builder** and **query report builder**: http://ibm.biz/DataSecurityLatestCourses

IBM Security

Backup

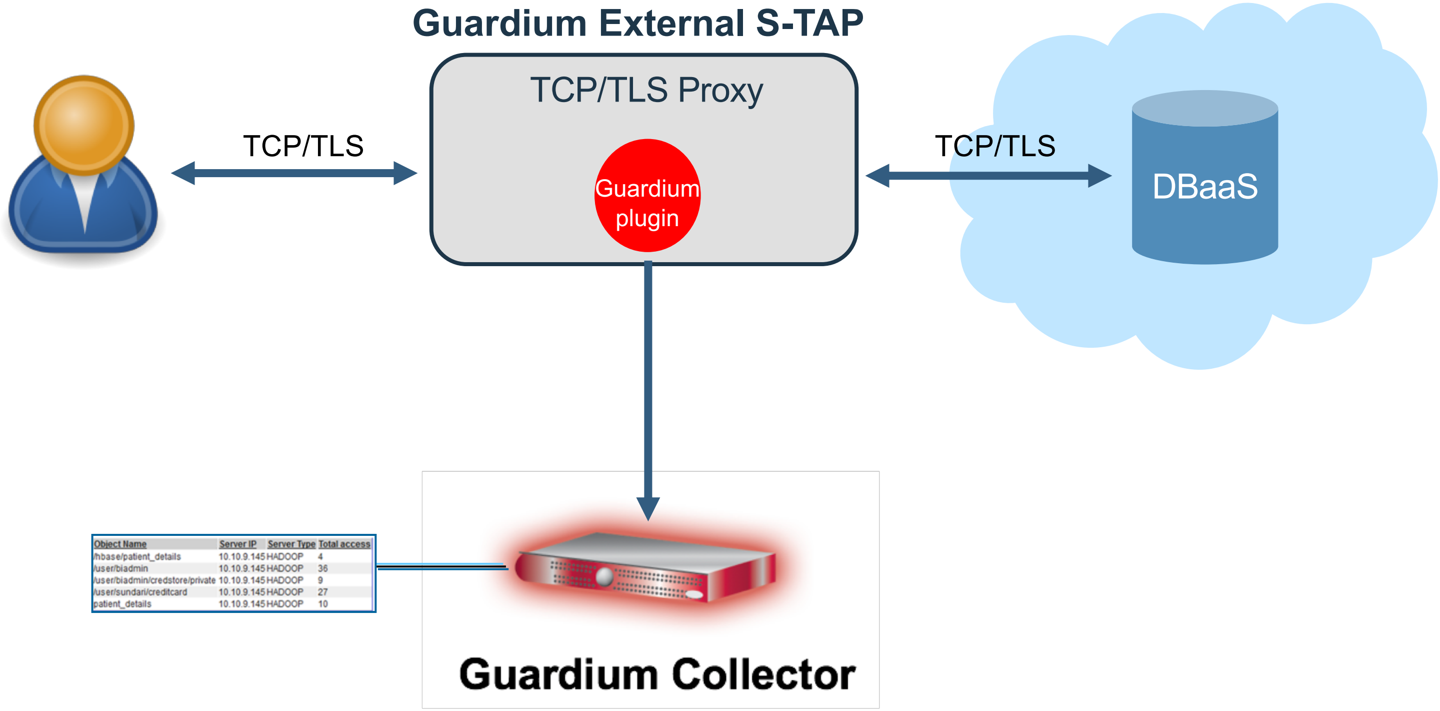
External S-TAP
FDEC
FAM
Policy Builder
On Rules (rule, actions, import)
Policy installation
Session level policy
Query Builder
Query conditions
Disk and database size alerts
GIM
Unix S-TAP
Masking, discovering sensitive data
Platform updates
GUI password
Certificates
MSSQL CIS
VA (Oracle 18c, multi-threading)
DB2 v10.5 LUW STIG
DB2 z/OS
Outliers

IBM Security

External S-TAP

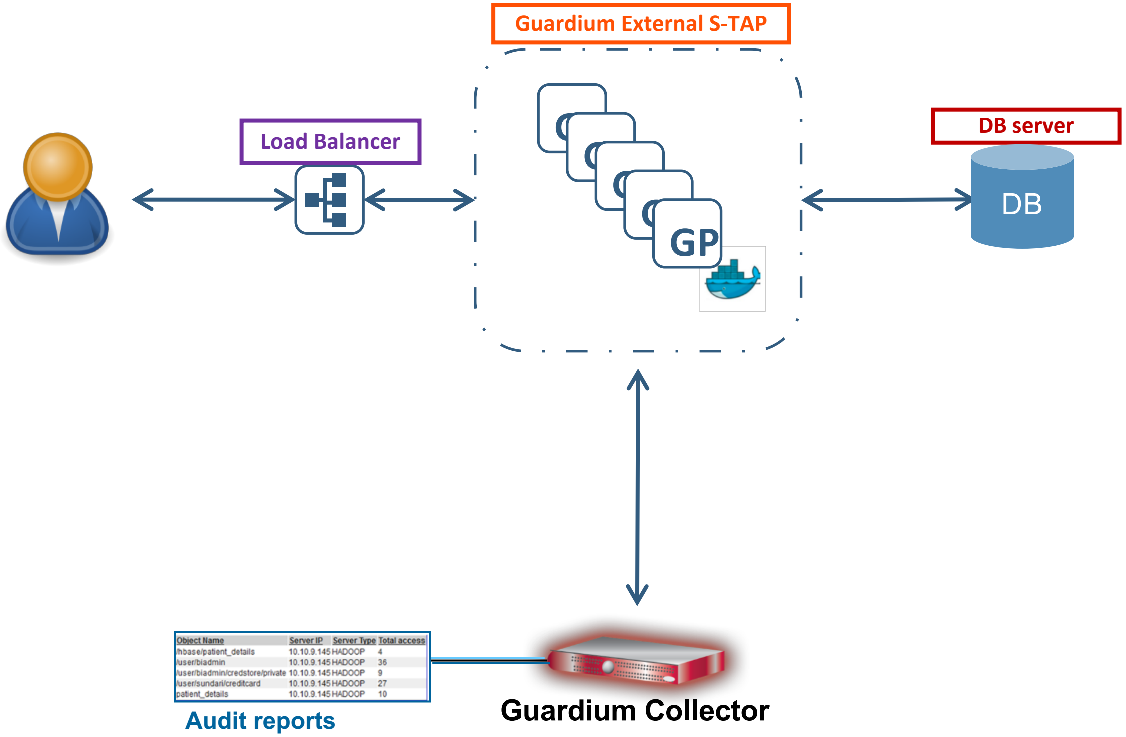
IBM

External S-TAP



Object Name	Server IP	Server Type	Total access
/hbase/patient_details	10.10.9.145	HADOOP	4
/user/biadmin	10.10.9.145	HADOOP	36
/user/biadmin/credstore/private	10.10.9.145	HADOOP	9
/user/sundari/creditcard	10.10.9.145	HADOOP	27
patient_details	10.10.9.145	HADOOP	10

Architecture

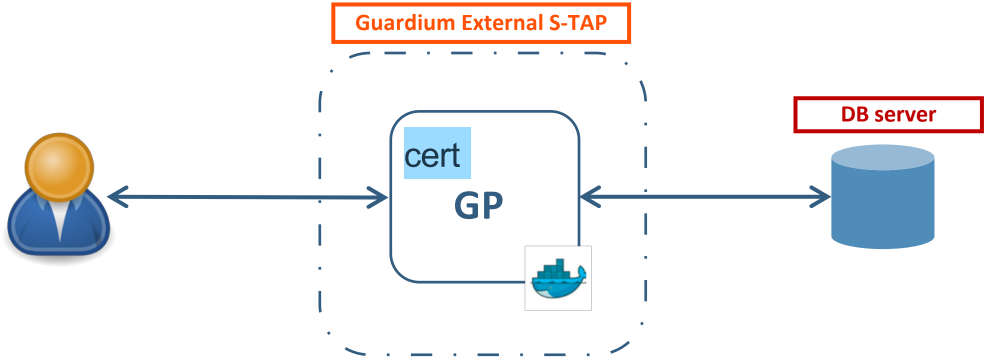


Object Name	Server IP	Server Type	Total access
/hbase/patient_details	10.10.9.145	HADOOP	4
/user/biadmin	10.10.9.145	HADOOP	36
/user/biadmin/credstore/private	10.10.9.145	HADOOP	9
/user/sundari/creditcard	10.10.9.145	HADOOP	27
patient_details	10.10.9.145	HADOOP	10

Requirements

- Point DB clients to Load Balancer instead of DB server
- Install certificates (for TLS)

TLS



To enable a TLS connection, a trusted certificate must be installed on each External S-TAP

New CLI (on CM)

- Creates CSR to be signed by a trusted CA
- Stores the signed certificate
- Distributes the certificate to appropriate External S-TAP instances

Use cases

External S-TAP provides Data Protection for DBs in the following scenarios

- DBaaS - 10.6
  - Oracle on RDS, SQLServer on Azure
- Encrypted DBs traffic
- Containerized DBs on-prem and in the cloud
  - Q1’19
- More DBs in 2019

Limitations

- SSL only
- No local traffic

- In this release
  - No client authentication
  - SSL version on client and server need to match

FDEC: File Discovery, Entitlement and Classification

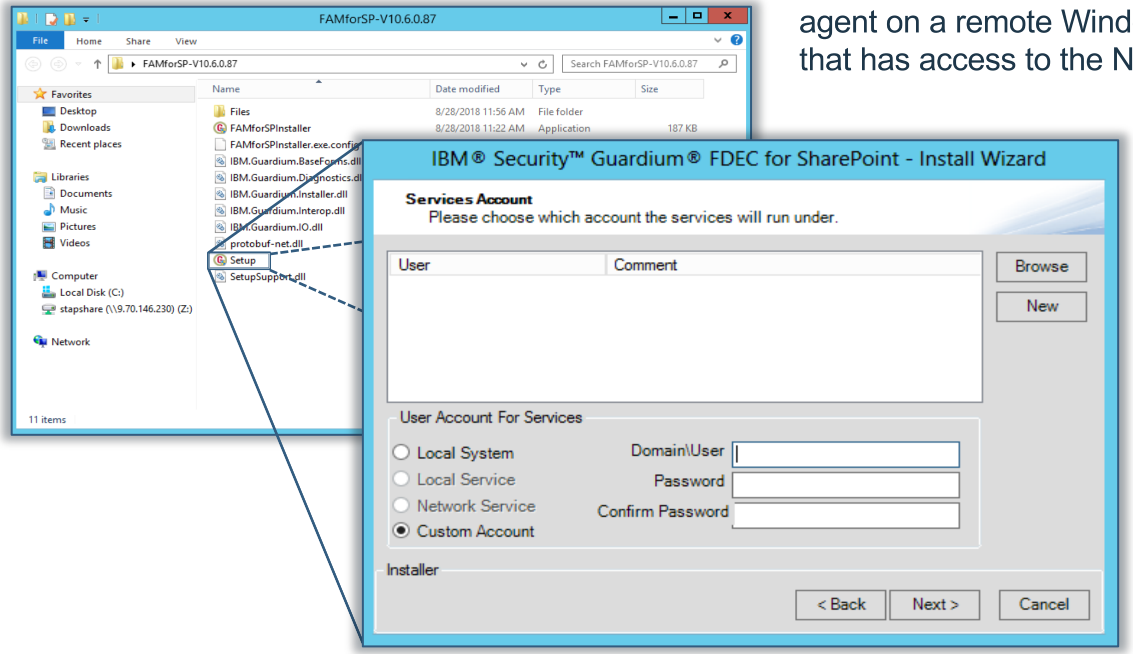
FDEC Use cases

- **Understand your sensitive data footprint**
  - Identify and classify the sensitive data on file shares such LUW(Linux, Unix and Windows) file systems, SharePoint, and NAS
  - Be able to identify and analyze the data, assess the impact on the business to decide on the right enforcement policies to protect and defend
  - Ability to use minimum skills thereby addressing the skills and technology gaps for end to end discovery and classification

- **Proactive Data Protection starts with Intelligent access management**
  - Need to understand real-world behavior based on who has access to what data and functions that contribute to the threats to the organization i.e. of the bottom line of the company
  - We can do this by allowing organizations to analyze document metadata and understand ownership
  - Have a view into the actors that have access to business critical data
  - Review entitlement reports to ensure access is always limited to just the users who need it
  - Remediate risks by implementing user controls for access systematically by integrating with existing identity governance processes

FDEC Installation

For SharePoint, install the agent on the application server of the SharePoint Farm. For NAS, install the agent on a remote Windows server that has access to the NAS device.



Name	Date modified	Type	Size
Files	8/28/2018 11:56 AM	File folder	
FAMforSPInstaller	8/28/2018 11:22 AM	Application	187 KB
FAMforSPInstaller.exe.config			
IBM.Guardium.BaseForms.dll			
IBM.Guardium.Diagnostics.dll			
IBM.Guardium.Installer.dll			
IBM.Guardium.Interop.dll			
IBM.Guardium.IO.dll			
protobuf-net.dll			
Setup			
SetupSupport.dll			

IBM® Security™ Guardium® FDEC for SharePoint - Install Wizard

Services Account
Please choose which account the services will run under.

User	Comment

User Account For Services

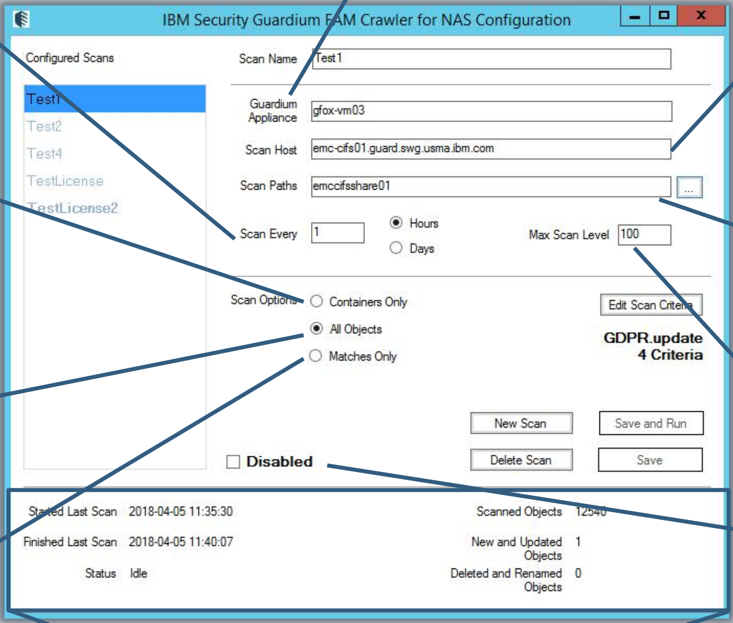
○ Local System
○ Local Service
○ Network Service
● Custom Account

Domain\User
Password
Confirm Password

Installer

https://www.ibm.com/support/knowledgecenter/SSMPHH_10.5.0/com.ibm.guardium.doc/discover/fam_for_nas_sp.html

FDEC Configuration: Main screen



IBM Security Guardium FAM Crawler for NAS Configuration

Configured Scans

- Test1
- Test2
- Test4
- TestLicense
- TestLicense2

Scan Name: Test1

Guardium Appliance: gfox-vm03

Scan Host: emc-cifs01.guard.swg.usma.ibm.com

Scan Paths: emccifsshare01 ...

Scan Every: 1 ● Hours ○ Days

Max Scan Level: 100

Scan Options: ○ Containers Only ● All Objects ○ Matches Only

Edit Scan Criteria

GDPR.update
4 Criteria

New Scan | Save and Run

Delete Scan | Save

□ **Disabled**

Started Last Scan 2018-04-05 11:35:30

Finished Last Scan 2018-04-05 11:40:07

Status Idle

Scanned Objects 12540

New and Updated Objects 1

Deleted and Renamed Objects 0

Guardium Appliance hostname or IP address

Frequency of the scan

Hostname of IP address of the device to be scanned. Localhost in case of SharePoint

Scan directories only and ignore the documents themselves. This will not trigger criteria and will not be classified

Name of Share

How deep into directory structure should the scan go

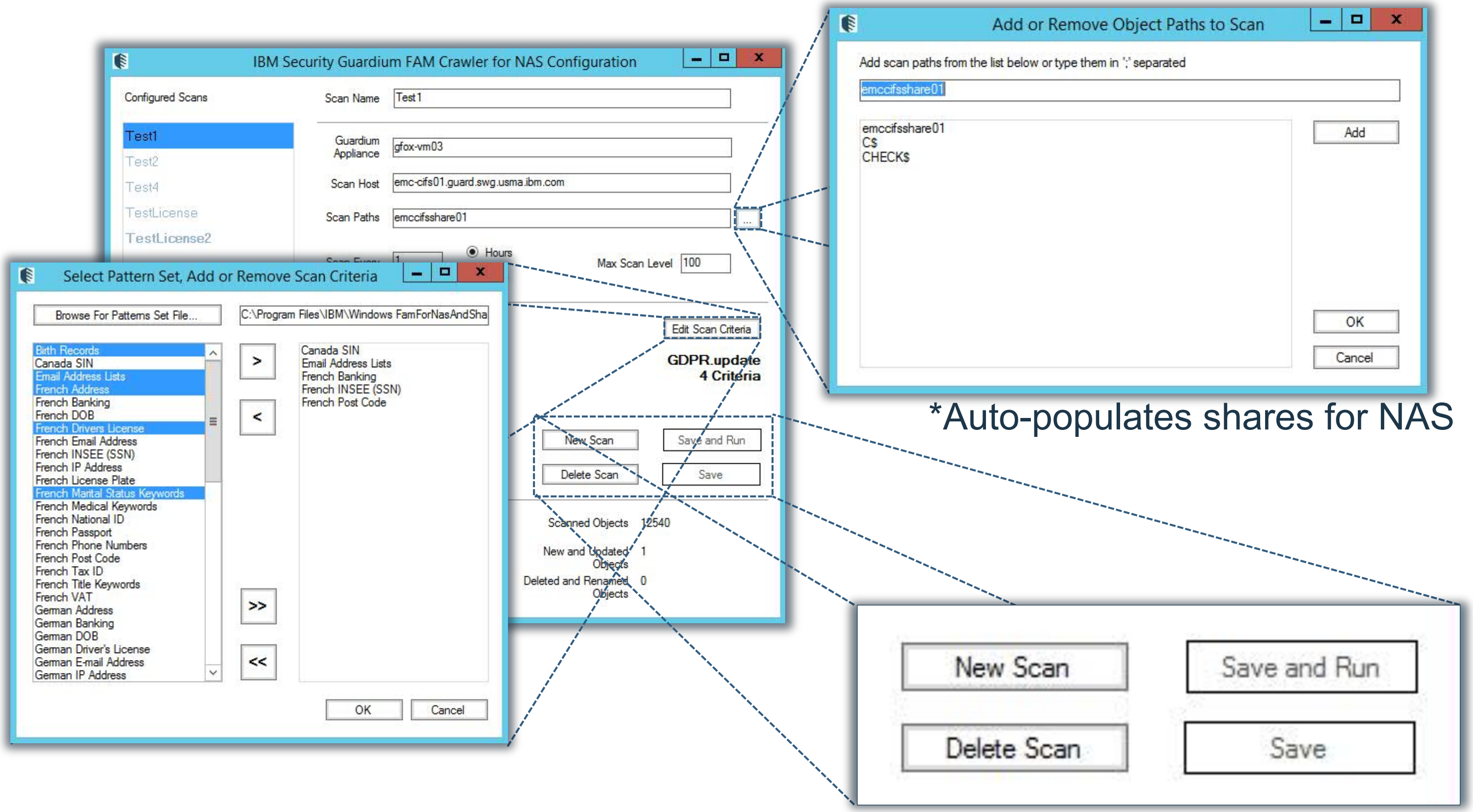
Scans everything including files and directory tree and will match to criteria

Enables or disable scanning

Only return records that trigger criteria

Scan Status

FDEC Configuration: Criteria selection and NAS share selection



IBM Security Guardium FAM Crawler for NAS Configuration

Configured Scans: Test1, Test2, Test4, TestLicense, TestLicense2

Scan Name: Test1

Guardium Appliance: gfox-vm03

Scan Host: emc-cifs01.guard.swg.usma.ibm.com

Scan Paths: emccifsshare01

● Hours

Max Scan Level: 100

GDPR.update
4 Criteria

Scanned Objects: 12540

New and Updated Objects: 1

Deleted and Renamed Objects: 0

Select Pattern Set, Add or Remove Scan Criteria

C:\Program Files\IBM\Windows FamForNasAndSha

Birth Records
Canada SIN
Email Address Lists
French Address
French Banking
French DOB
French Drivers License
French Email Address
French INSEE (SSN)
French IP Address
French License Plate
French Marital Status Keywords
French Medical Keywords
French National ID
French Passport
French Phone Numbers
French Post Code
French Tax ID
French Title Keywords
French VAT
German Address
German Banking
German DOB
German Driver's License
German E-mail Address
German IP Address

Canada SIN
Email Address Lists
French Banking
French INSEE (SSN)
French Post Code

Add or Remove Object Paths to Scan

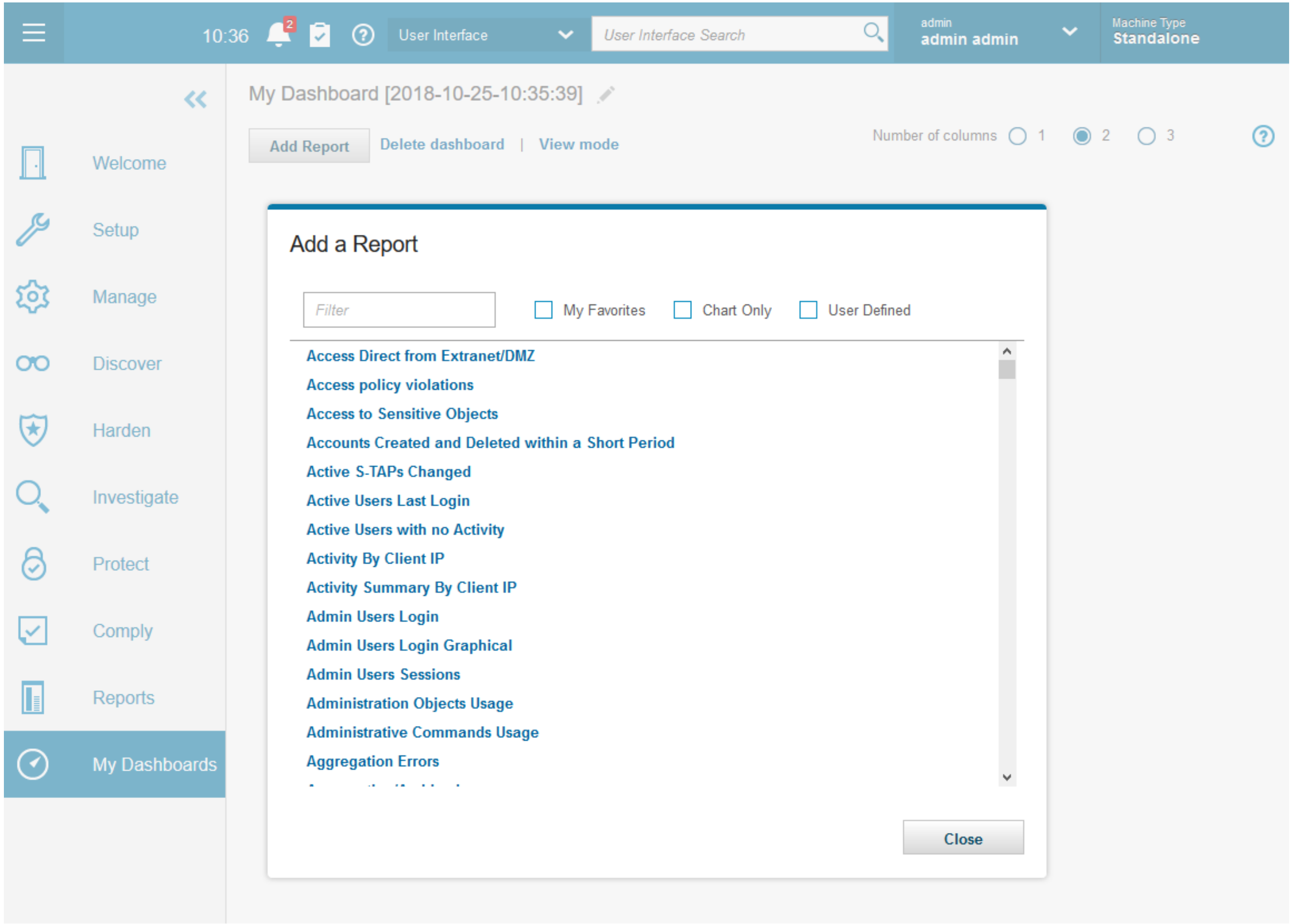
Add scan paths from the list below or type them in ';' separated

emccifsshare01

emccifsshare01
C$
CHECK$

*Auto-populates shares for NAS

FDEC: My Dashboard



My Dashboard [2018-10-25-10:35:39]

Add Report | Delete dashboard | View mode

Number of columns ○ 1 ● 2 ○ 3

Add a Report

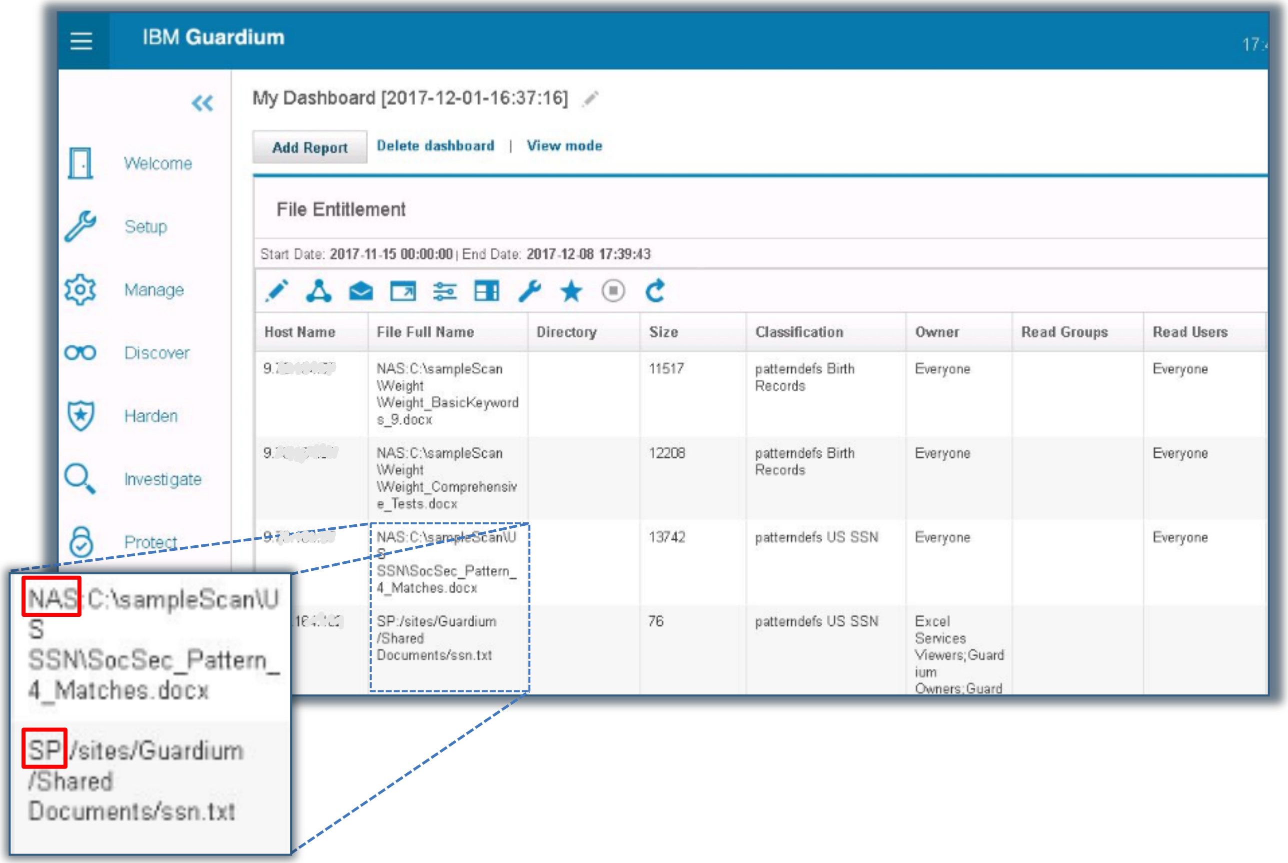
Filter

□ My Favorites □ Chart Only □ User Defined

- Access Direct from Extranet/DMZ
- Access policy violations
- Access to Sensitive Objects
- Accounts Created and Deleted within a Short Period
- Active S-TAPs Changed
- Active Users Last Login
- Active Users with no Activity
- Activity By Client IP
- Activity Summary By Client IP
- Admin Users Login
- Admin Users Login Graphical
- Admin Users Sessions
- Administration Objects Usage
- Administrative Commands Usage
- Aggregation Errors

Close

FDEC Report: File Entitlement



My Dashboard [2017-12-01-16:37:16]

File Entitlement

Start Date: 2017-11-15 00:00:00 | End Date: 2017-12-08 17:39:43

Host Name	File Full Name	Directory	Size	Classification	Owner	Read Groups	Read Users
9.[redacted]	NAS:C:\sampleScan\Weight\Weight_BasicKeywords_9.docx		11517	patterndefs Birth Records	Everyone		Everyone
9.[redacted]	NAS:C:\sampleScan\Weight\Weight_Comprehensive_Tests.docx		12208	patterndefs Birth Records	Everyone		Everyone
9.[redacted]	NAS:C:\sampleScan\US SSN\SocSec_Pattern_4_Matches.docx		13742	patterndefs US SSN	Everyone		Everyone
[redacted]	SP:/sites/Guardium/Shared Documents/ssn.txt		76	patterndefs US SSN	Excel Services Viewers;Guardium Owners;Guard		

NAS:C:\sampleScan\US SSN\SocSec_Pattern_4_Matches.docx

SP:/sites/Guardium/Shared Documents/ssn.txt

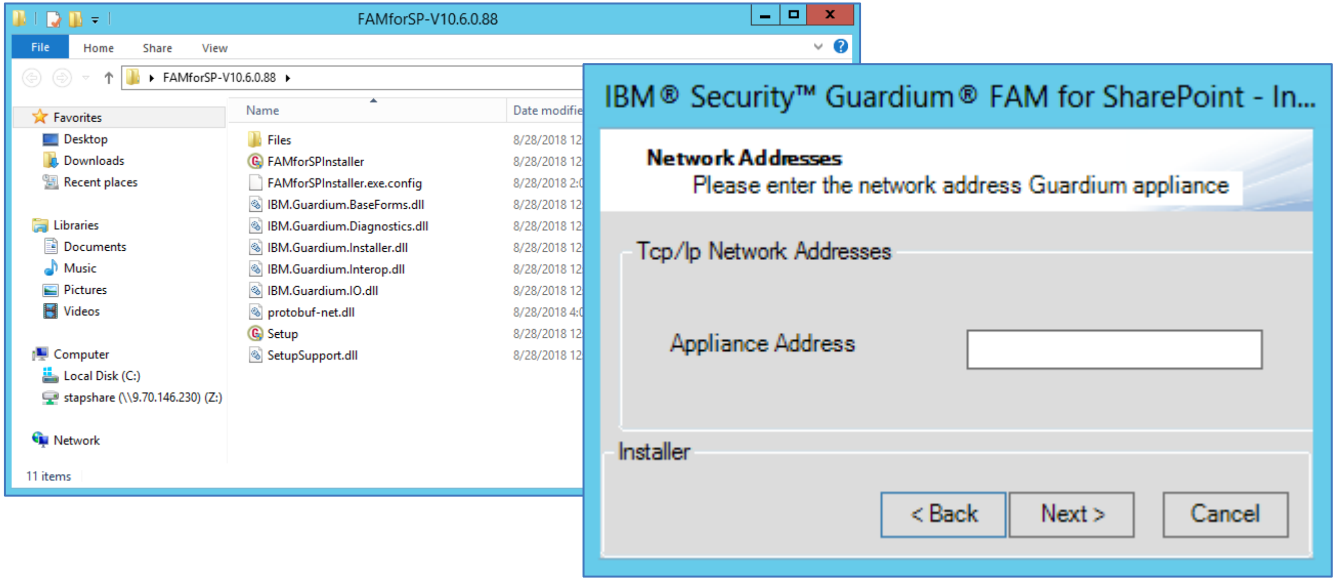
FAM: File Activity Monitoring

FAM Use cases

- **Data Protection Journey is not complete till organization know how to protect discovered data**
  - Empowering the workforce to be guardians of their own data
  - Able to use out-of-box polices to monitor and detect anomalous/malicious file access patterns
  - Get alerted or block when monitored sensitive files are accessed suspiciously
  - Have a single pane of glass for all file activities for investigative analysis & remediation
  - And finally, integrate insights with SIEM for enterprise-wide user behavioral analytics
  - Learn as you go
- **Minimize the cost of being "Not compliant"**
  - Generate audit reports for relevant activities
  - Prove compliance for PCI DSS, HIPAA, GDPR and SOX
  - Improve efficiency through compliance workflows
  - existing identity governance processes

FAM Installation

- For SharePoint, install the agent on the application server of the SharePoint Farm. For NAS, install the agent on a remote Windows server that has access to the NAS device.
- Download the FAM for NAS and SharePoint package from Fix Central (https://www-945.ibm.com/support/fixcentral/) and unzip this file.
- Navigate to the FAM package and find setup.exe
- Follow the prompts in the Wizard to complete the installation. You will have to provide the appliance address during the installation process.



FAMforSP-V10.6.0.88

FAMforSP-V10.6.0.88 ▸

Name	Date modifie
Files	8/28/2018 12
FAMforSPInstaller	8/28/2018 12
FAMforSPInstaller.exe.config	8/28/2018 2:0
IBM.Guardium.BaseForms.dll	8/28/2018 12
IBM.Guardium.Diagnostics.dll	8/28/2018 12
IBM.Guardium.Installer.dll	8/28/2018 12
IBM.Guardium.Interop.dll	8/28/2018 12
IBM.Guardium.IO.dll	8/28/2018 12
protobuf-net.dll	8/28/2018 4:0
Setup	8/28/2018 12
SetupSupport.dll	8/28/2018 12

11 items

IBM® Security™ Guardium® FAM for SharePoint - In...

Network Addresses

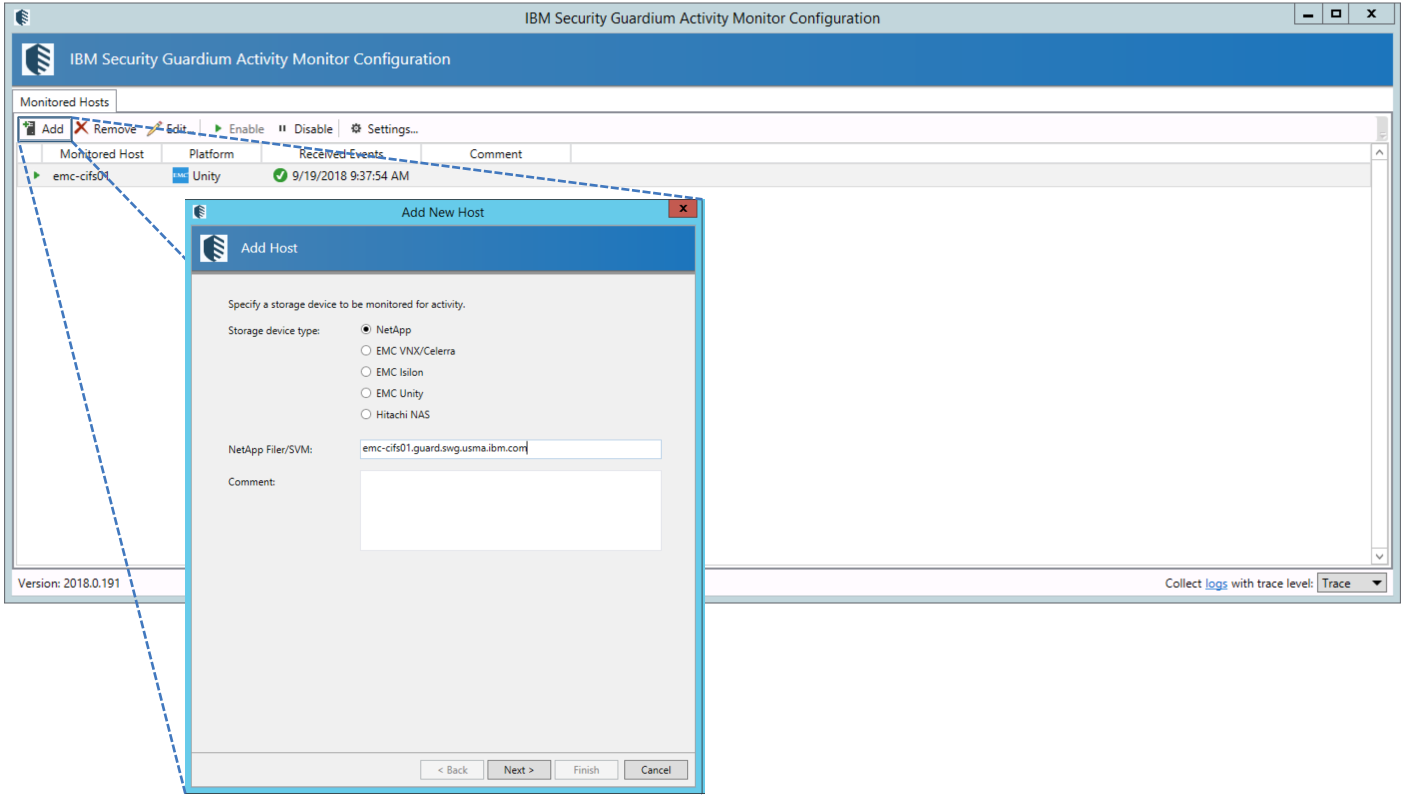
Please enter the network address Guardium appliance

Tcp/Ip Network Addresses

Appliance Address

Installer

Configuration: Adding NAS Host



IBM Security Guardium Activity Monitor Configuration

Monitored Hosts

Monitored Host	Platform	Received Events	Comment
emc-cifs01	Unity	✓ 9/19/2018 9:37:54 AM	

Version: 2018.0.191

Collect logs with trace level: Trace

Add New Host

Add Host

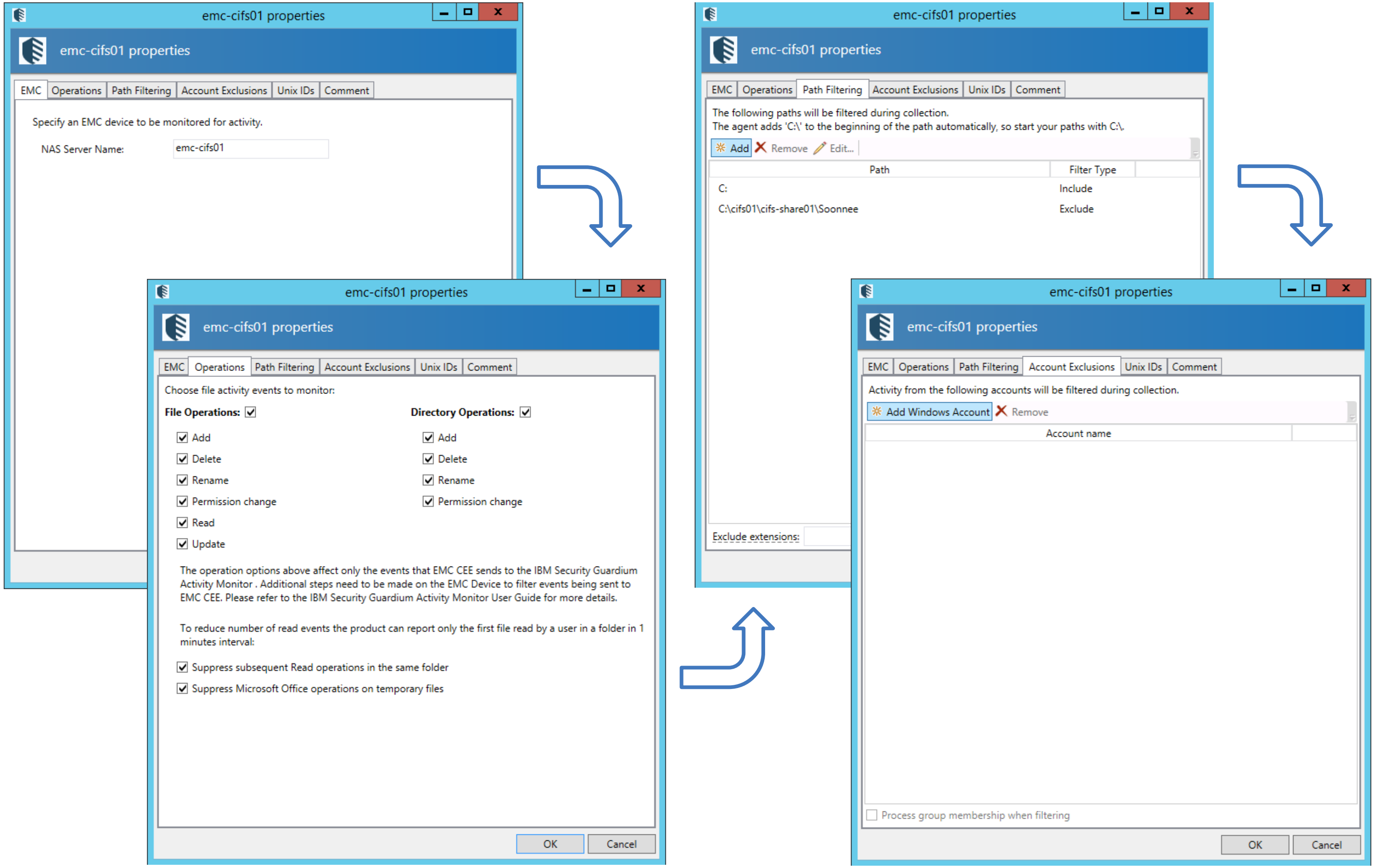
Specify a storage device to be monitored for activity.

Storage device type:
● NetApp
○ EMC VNX/Celerra
○ EMC Isilon
○ EMC Unity
○ Hitachi NAS

NetApp Filer/SVM: emc-cifs01.guard.swg.usma.ibm.com

Comment:

FAM Configuration: Editing NAS Configuration



emc-cifs01 properties

EMC | Operations | Path Filtering | Account Exclusions | Unix IDs | Comment

Specify an EMC device to be monitored for activity.

NAS Server Name: emc-cifs01

emc-cifs01 properties

EMC | Operations | Path Filtering | Account Exclusions | Unix IDs | Comment

Choose file activity events to monitor:

File Operations: ☑

☑ Add
☑ Delete
☑ Rename
☑ Permission change
☑ Read
☑ Update

Directory Operations: ☑

☑ Add
☑ Delete
☑ Rename
☑ Permission change

The operation options above affect only the events that EMC CEE sends to the IBM Security Guardium Activity Monitor . Additional steps need to be made on the EMC Device to filter events being sent to EMC CEE. Please refer to the IBM Security Guardium Activity Monitor User Guide for more details.

To reduce number of read events the product can report only the first file read by a user in a folder in 1 minutes interval:

☑ Suppress subsequent Read operations in the same folder
☑ Suppress Microsoft Office operations on temporary files

OK | Cancel

emc-cifs01 properties

EMC | Operations | Path Filtering | Account Exclusions | Unix IDs | Comment

The following paths will be filtered during collection.
The agent adds 'C:\' to the beginning of the path automatically, so start your paths with C:\.

Add | Remove | Edit...

Path	Filter Type
C:	Include
C:\cifs01\cifs-share01\Soonnee	Exclude

Exclude extensions:

emc-cifs01 properties

EMC | Operations | Path Filtering | Account Exclusions | Unix IDs | Comment

Activity from the following accounts will be filtered during collection.

Add Windows Account | Remove

Account name

□ Process group membership when filtering

OK | Cancel

FAM Configuration: NAS Options

Selected NAS Device

On the selected NAS device tab, use the text field to provide the name of the NAS server.

Operations

Select the activity events to monitor. These operations can relate to file or directory activity.

Path Filtering

This tab, on a host’s properties window, allows users to add collection scope filters for file paths. Specified paths can be included in or excluded from being monitored.

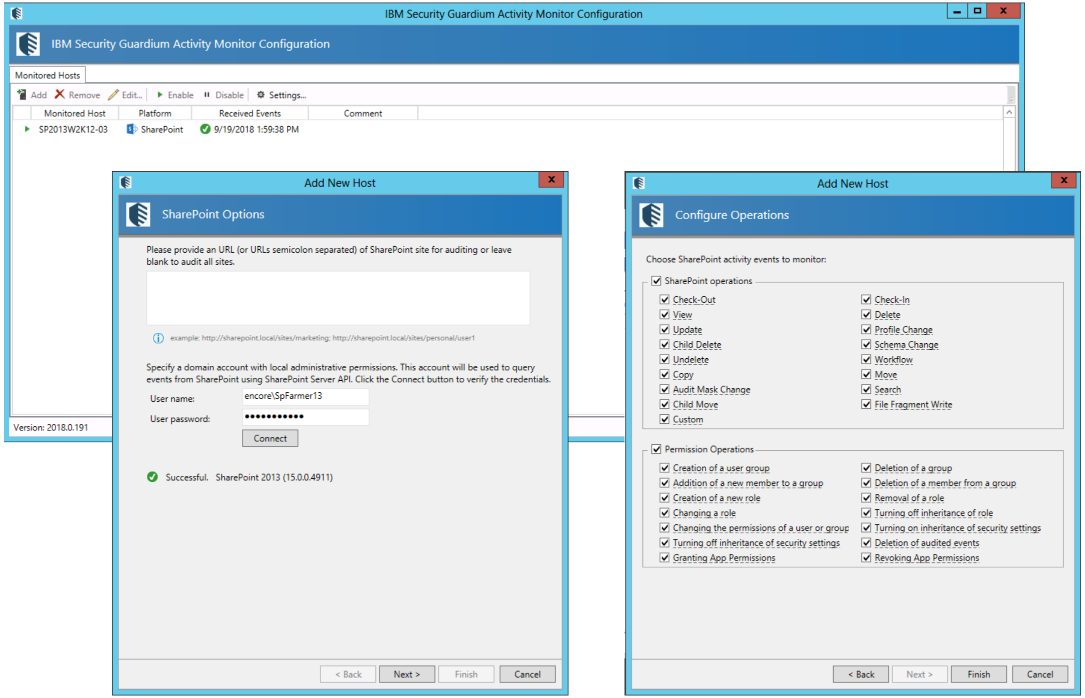
Account Exclusions

The accounts added here will be excluded from being monitored for file system activity. File Activity Monitor for NAS and SharePoint **5**

Unix IDs

This tab provides configuration options to translate Unix IDs (UID) to Windows SIDs. This applies only to NetApp devices and EMC devices, When there is an activity on a NAS device, UIDs are returned for that activity event. Depending on the operating system, the UID can be mapped to Active Directory accounts using the uidNumber attribute in Active Directory. The activity agent resolves the Active Directory SID based on the UID from the activity event.

FAM Configuration: Adding SharePoint Host


IBM Security Guardium Activity Monitor Configuration
IBM Security Guardium Activity Monitor Configuration
Monitored Hosts
Add
Remove
Edit...
Enable
Disable
Settings...

Monitored Host	Platform	Received Events	Comment
SP2013W2K12-03	SharePoint	✓ 9/19/2018 1:59:38 PM	

Version: 2018.0.191

Add New Host
SharePoint Options

Please provide an URL (or URLs semicolon separated) of SharePoint site for auditing or leave blank to audit all sites.

example: http://sharepoint.local/sites/marketing; http://sharepoint.local/sites/personal/user1

Specify a domain account with local administrative permissions. This account will be used to query events from SharePoint using SharePoint Server API. Click the Connect button to verify the credentials.

User name: encore\SpFarmer13

User password: ●●●●●●●●●●●

✓ Successful. SharePoint 2013 (15.0.0.4911)

Choose SharePoint activity events to monitor:

☑ SharePoint operations

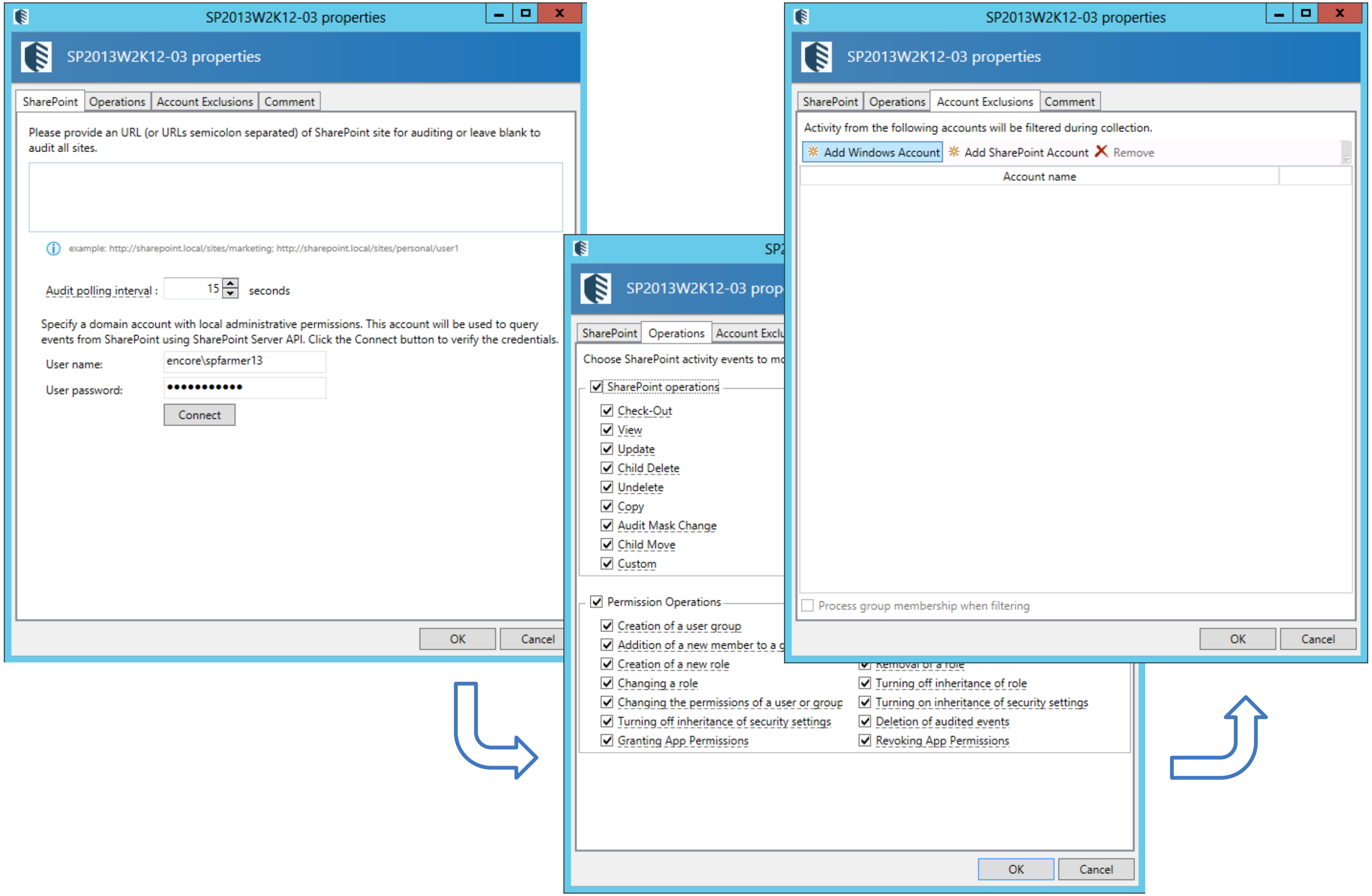
☑ Check-Out
☑ View
☑ Update
☑ Child Delete
☑ Undelete
☑ Copy
☑ Audit Mask Change
☑ Child Move
☑ Custom
☑ Check-In
☑ Delete
☑ Profile Change
☑ Schema Change
☑ Workflow
☑ Move
☑ Search
☑ File Fragment Write

☑ Permission Operations

☑ Creation of a user group
☑ Addition of a new member to a group
☑ Creation of a new role
☑ Changing a role
☑ Changing the permissions of a user or group
☑ Turning off inheritance of security settings
☑ Granting App Permissions
☑ Deletion of a group
☑ Deletion of a member from a group
☑ Removal of a role
☑ Turning off inheritance of role
☑ Turning on inheritance of security settings
☑ Deletion of audited events
☑ Revoking App Permissions

- **Monitored Host is automatically configured as it is the local host**
- **Only one host can be added at a time for SharePoint**
- **Must Apply credentials and click Connect**

FAM Configuration: Editing SharePoint Configuration



Please provide an URL (or URLs semicolon separated) of SharePoint site for auditing or leave blank to audit all sites.

example: http://sharepoint.local/sites/marketing; http://sharepoint.local/sites/personal/user1

Audit polling interval : 15 seconds

Specify a domain account with local administrative permissions. This account will be used to query events from SharePoint using SharePoint Server API. Click the Connect button to verify the credentials.

User name: encore\spfarmer13

User password: ●●●●●●●●●●●

Choose SharePoint activity events to mo

☑ SharePoint operations

☑ Check-Out
☑ View
☑ Update
☑ Child Delete
☑ Undelete
☑ Copy
☑ Audit Mask Change
☑ Child Move
☑ Custom

☑ Permission Operations

☑ Creation of a user group
☑ Addition of a new member to a g
☑ Creation of a new role
☑ Changing a role
☑ Changing the permissions of a user or group
☑ Turning off inheritance of security settings
☑ Granting App Permissions
☑ Removal of a role
☑ Turning off inheritance of role
☑ Turning on inheritance of security settings
☑ Deletion of audited events
☑ Revoking App Permissions

Activity from the following accounts will be filtered during collection.

□ Process group membership when filtering

FAM Configuration: SharePoint Options

SharePoint

Provide credentials that have administrative privileges on both the local system as well as SharePoint. Then click on **Connect**.

Path Filtering

This tab, on a host’s properties window, allows users to add collection scope filters for file paths. Specified paths can be included in or excluded from being monitored.

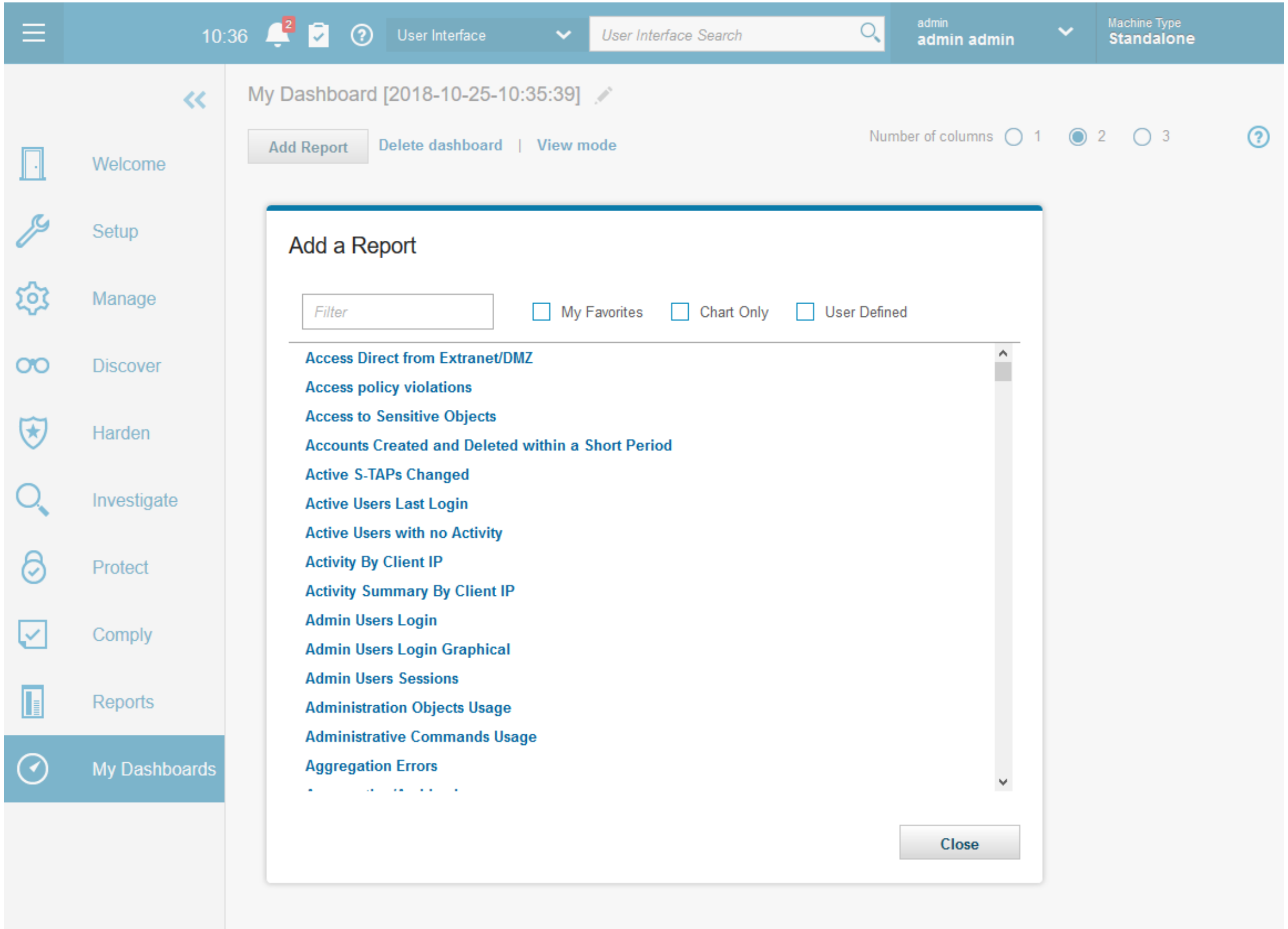
Operations

Select the SharePoint operations and Permission operations to monitor.

Account Exclusions

The accounts added here will be excluded from being monitored for SharePoint activity.

FAM: My Dashboard



My Dashboard [2018-10-25-10:35:39]

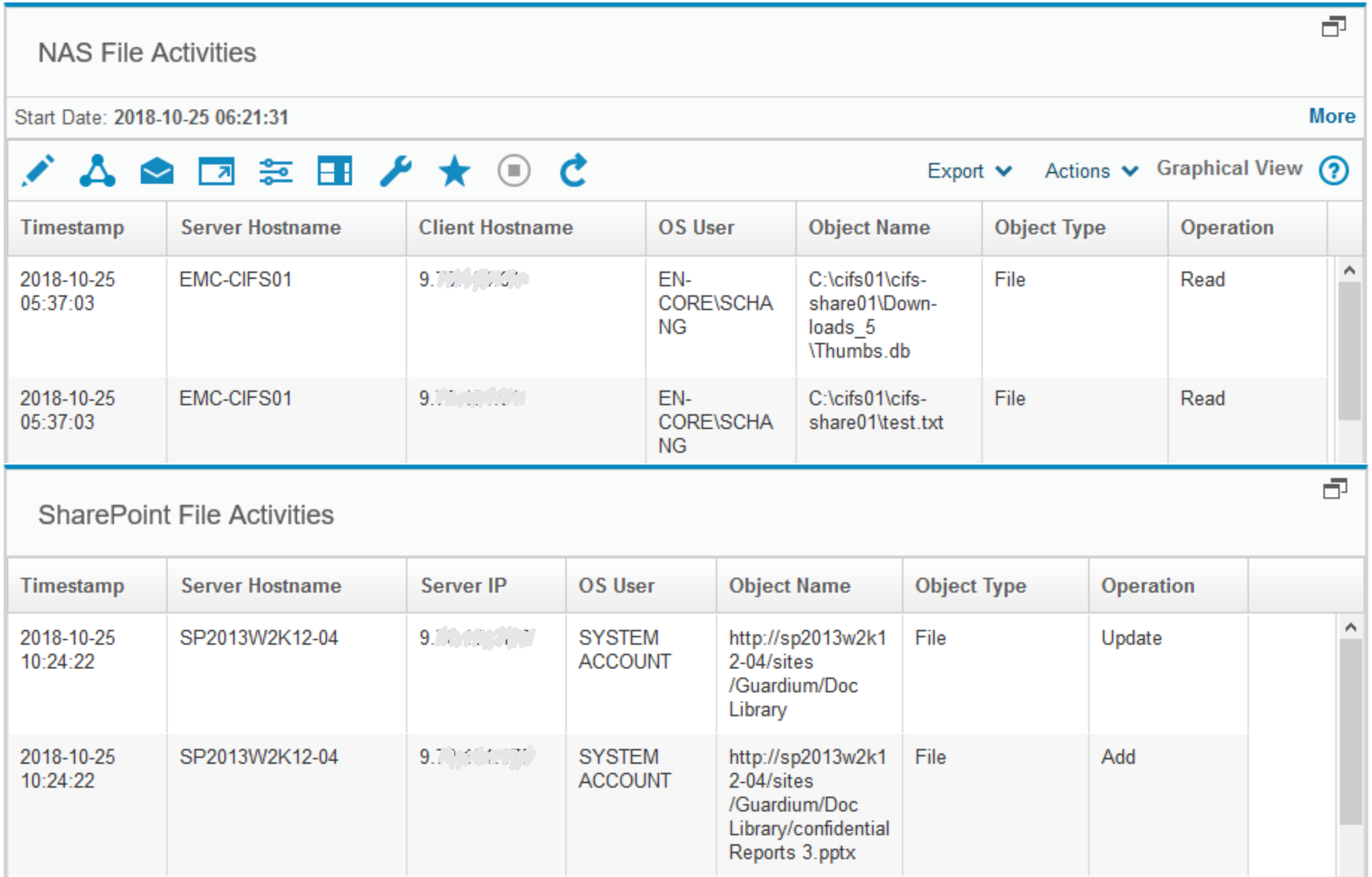
Number of columns ○ 1 ● 2 ○ 3

Add a Report

Filter □ My Favorites □ Chart Only □ User Defined

Access Direct from Extranet/DMZ
Access policy violations
Access to Sensitive Objects
Accounts Created and Deleted within a Short Period
Active S-TAPs Changed
Active Users Last Login
Active Users with no Activity
Activity By Client IP
Activity Summary By Client IP
Admin Users Login
Admin Users Login Graphical
Admin Users Sessions
Administration Objects Usage
Administrative Commands Usage
Aggregation Errors

FAM Reports



NAS File Activities

Start Date: **2018-10-25 06:21:31**

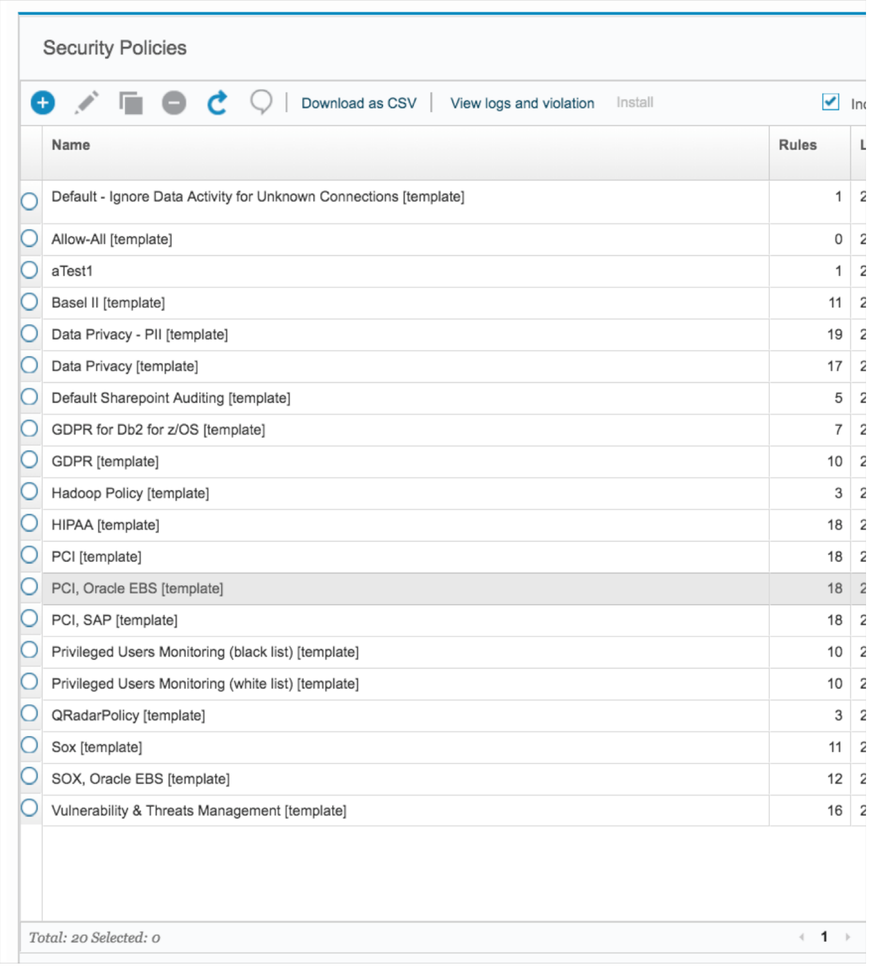
Timestamp	Server Hostname	Client Hostname	OS User	Object Name	Object Type	Operation
2018-10-25 05:37:03	EMC-CIFS01	9.[redacted]	EN-CORE\SCHANG	C:\cifs01\cifs-share01\Down-loads_5\Thumbs.db	File	Read
2018-10-25 05:37:03	EMC-CIFS01	9.[redacted]	EN-CORE\SCHANG	C:\cifs01\cifs-share01\test.txt	File	Read

SharePoint File Activities

Timestamp	Server Hostname	Server IP	OS User	Object Name	Object Type	Operation
2018-10-25 10:24:22	SP2013W2K12-04	9.[redacted]	SYSTEM ACCOUNT	http://sp2013w2k12-04/sites/Guardium/Doc Library	File	Update
2018-10-25 10:24:22	SP2013W2K12-04	9.[redacted]	SYSTEM ACCOUNT	http://sp2013w2k12-04/sites/Guardium/Doc Library/confidential Reports 3.pptx	File	Add

New Policy Builder

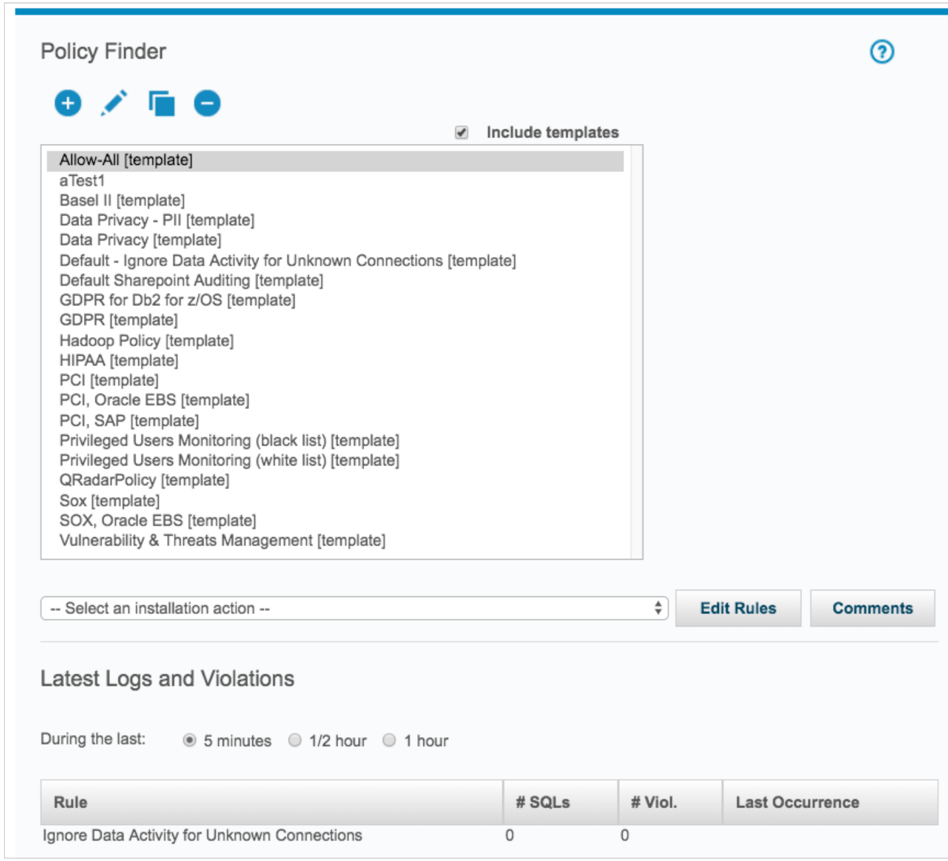
New vs legacy



Security Policies

	Name	Rules	L
○	Default - Ignore Data Activity for Unknown Connections [template]	1	2
○	Allow-All [template]	0	2
○	aTest1	1	2
○	Basel II [template]	11	2
○	Data Privacy - PII [template]	19	2
○	Data Privacy [template]	17	2
○	Default Sharepoint Auditing [template]	5	2
○	GDPR for Db2 for z/OS [template]	7	2
○	GDPR [template]	10	2
○	Hadoop Policy [template]	3	2
○	HIPAA [template]	18	2
○	PCI [template]	18	2
○	PCI, Oracle EBS [template]	18	2
○	PCI, SAP [template]	18	2
○	Privileged Users Monitoring (black list) [template]	10	2
○	Privileged Users Monitoring (white list) [template]	10	2
○	QRadarPolicy [template]	3	2
○	Sox [template]	11	2
○	SOX, Oracle EBS [template]	12	2
○	Vulnerability & Threats Management [template]	16	2

Total: 20 Selected: 0



Policy Finder

☑ Include templates

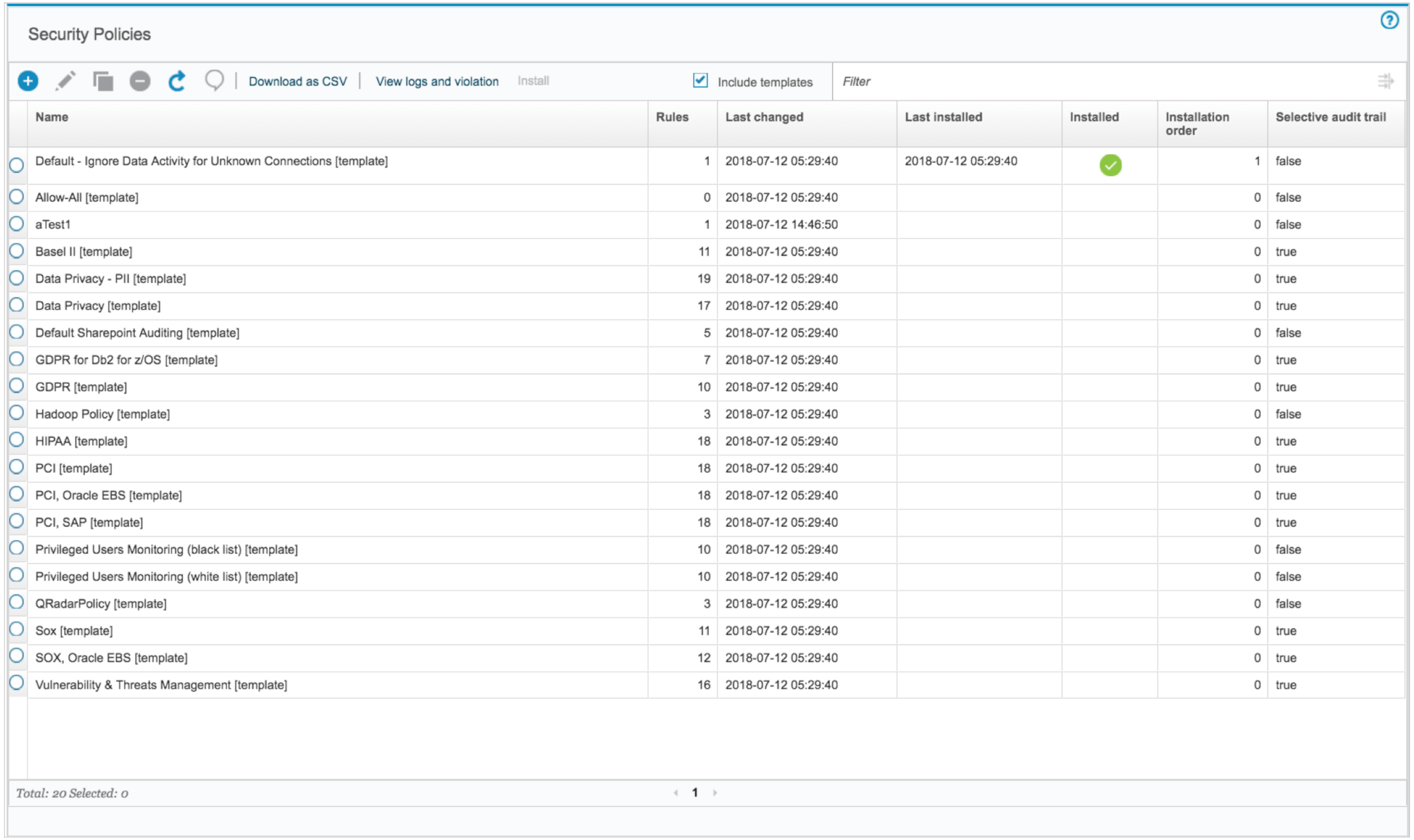
Allow-All [template]
aTest1
Basel II [template]
Data Privacy - PII [template]
Data Privacy [template]
Default - Ignore Data Activity for Unknown Connections [template]
Default Sharepoint Auditing [template]
GDPR for Db2 for z/OS [template]
GDPR [template]
Hadoop Policy [template]
HIPAA [template]
PCI [template]
PCI, Oracle EBS [template]
PCI, SAP [template]
Privileged Users Monitoring (black list) [template]
Privileged Users Monitoring (white list) [template]
QRadarPolicy [template]
Sox [template]
SOX, Oracle EBS [template]
Vulnerability & Threats Management [template]

Latest Logs and Violations

During the last: ● 5 minutes ○ 1/2 hour ○ 1 hour

Rule	# SQLs	# Viol.	Last Occurrence
Ignore Data Activity for Unknown Connections	0	0	

Full look of new Policy builder



Security Policies

○	Name	Rules	Last changed	Last installed	Installed	Installation order	Selective audit trail
○	Default - Ignore Data Activity for Unknown Connections [template]	1	2018-07-12 05:29:40	2018-07-12 05:29:40	✓	1	false
○	Allow-All [template]	0	2018-07-12 05:29:40			0	false
○	aTest1	1	2018-07-12 14:46:50			0	false
○	Basel II [template]	11	2018-07-12 05:29:40			0	true
○	Data Privacy - PII [template]	19	2018-07-12 05:29:40			0	true
○	Data Privacy [template]	17	2018-07-12 05:29:40			0	true
○	Default Sharepoint Auditing [template]	5	2018-07-12 05:29:40			0	false
○	GDPR for Db2 for z/OS [template]	7	2018-07-12 05:29:40			0	true
○	GDPR [template]	10	2018-07-12 05:29:40			0	true
○	Hadoop Policy [template]	3	2018-07-12 05:29:40			0	false
○	HIPAA [template]	18	2018-07-12 05:29:40			0	true
○	PCI [template]	18	2018-07-12 05:29:40			0	true
○	PCI, Oracle EBS [template]	18	2018-07-12 05:29:40			0	true
○	PCI, SAP [template]	18	2018-07-12 05:29:40			0	true
○	Privileged Users Monitoring (black list) [template]	10	2018-07-12 05:29:40			0	false
○	Privileged Users Monitoring (white list) [template]	10	2018-07-12 05:29:40			0	false
○	QRadarPolicy [template]	3	2018-07-12 05:29:40			0	false
○	Sox [template]	11	2018-07-12 05:29:40			0	true
○	SOX, Oracle EBS [template]	12	2018-07-12 05:29:40			0	true
○	Vulnerability & Threats Management [template]	16	2018-07-12 05:29:40			0	true

Total: 20 Selected: 0

‹ 1 ›

Full look of new Policy builder

Edit / View policy
* Template policies can only be viewed

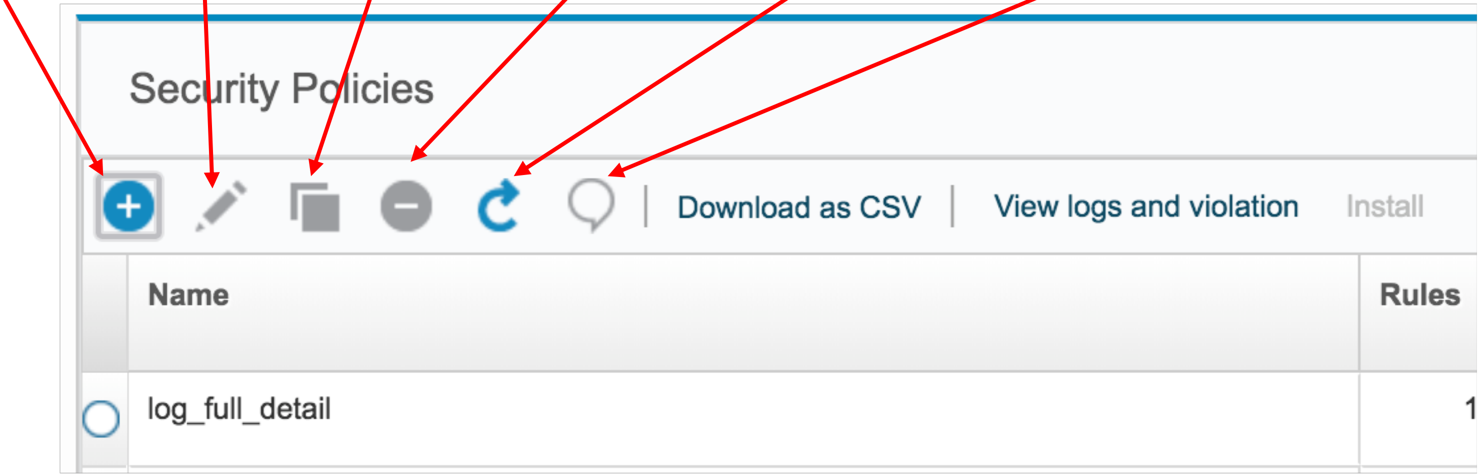
Delete selected policy
*Template policies cannot be deleted

Refresh grid

Create new policy

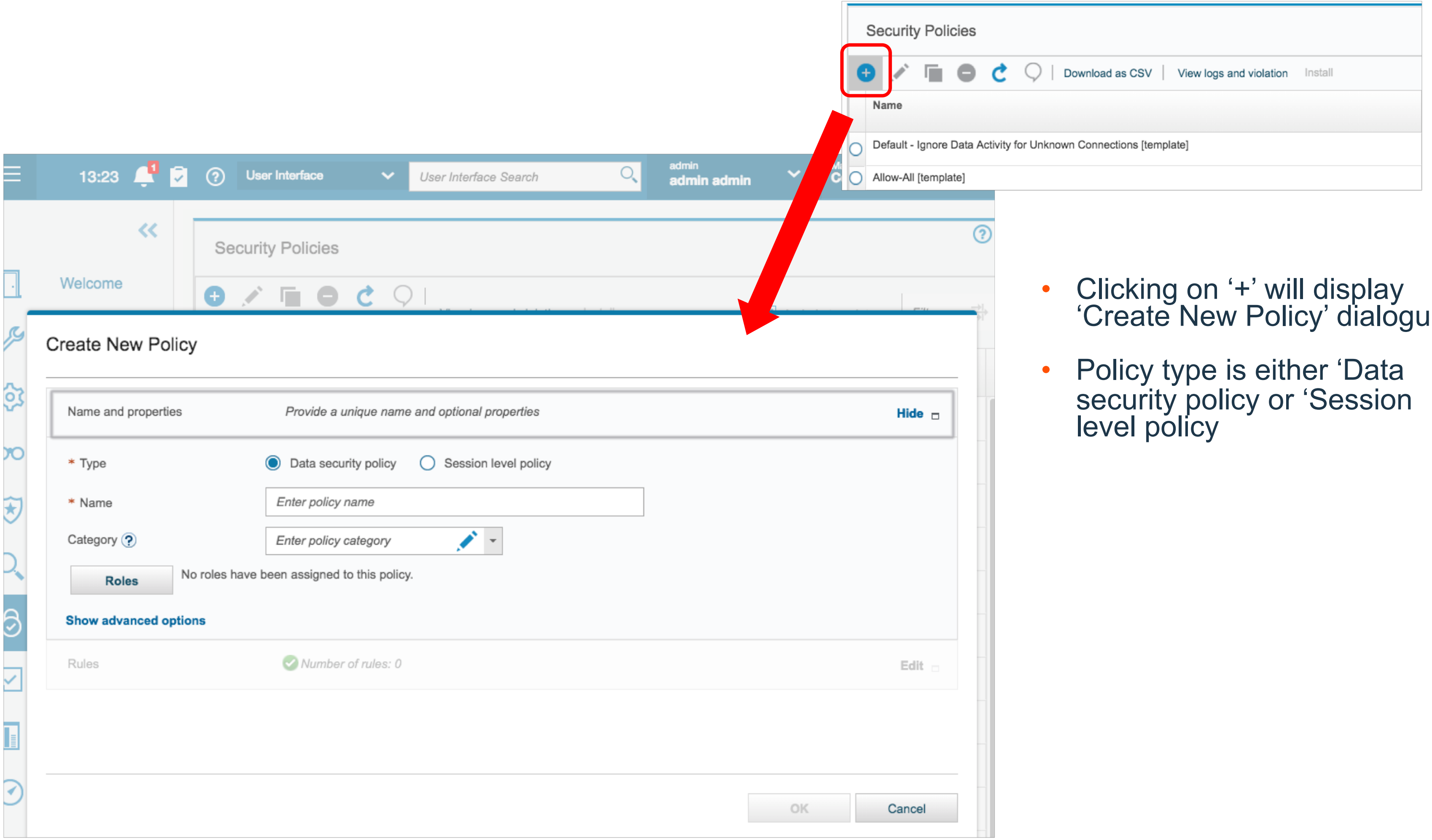
Clone selected policy

Comment on selected policy



	Name	Rules
○	log_full_detail	1

Opening ‘Create New Policy’ window



Security Policies

Download as CSV | View logs and violation | Install

Name
○ Default - Ignore Data Activity for Unknown Connections [template]
○ Allow-All [template]

Create New Policy

Name and properties — *Provide a unique name and optional properties* — Hide

* Type: ● Data security policy ○ Session level policy

* Name: *Enter policy name*

Category: *Enter policy category*

Roles — No roles have been assigned to this policy.

Show advanced options

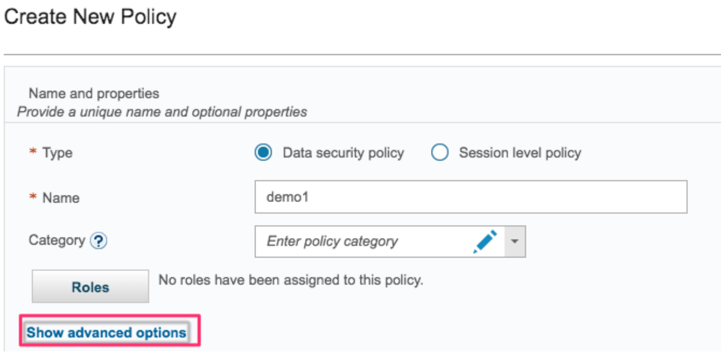
Rules — *Number of rules: 0* — Edit

OK | Cancel

- Clicking on ‘+’ will display ‘Create New Policy’ dialogue
- Policy type is either ‘Data security policy or ‘Session level policy

Advanced options

Advanced options will allow user to define the policy as ‘Log flat’ or ‘Rule on flat’ or ‘Selective audit trail’.



Create New Policy

Name and properties
Provide a unique name and optional properties

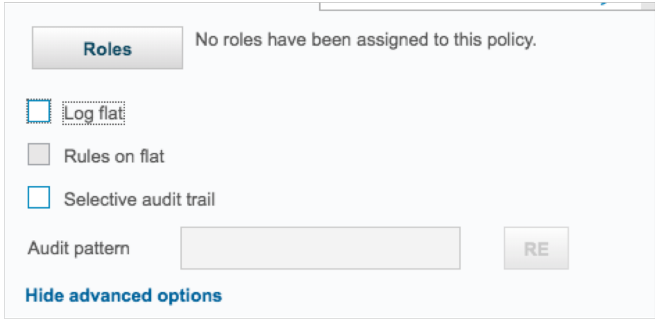
* Type ● Data security policy ○ Session level policy

* Name demo1

Category ? *Enter policy category*

Roles No roles have been assigned to this policy.

Show advanced options



Roles No roles have been assigned to this policy.

□ Log flat

□ Rules on flat

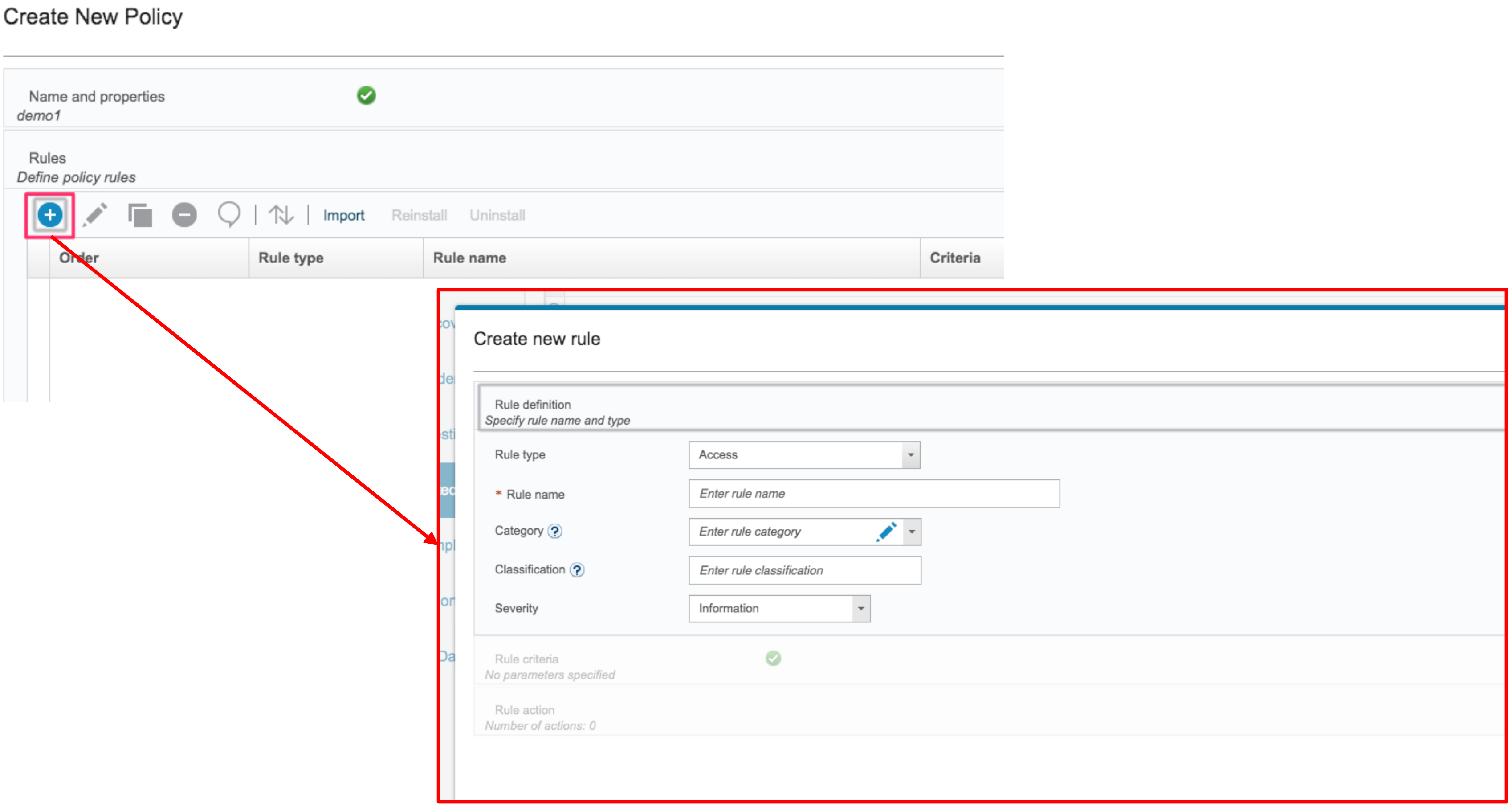
□ Selective audit trail

Audit pattern RE

Hide advanced options

Rule

Creating new rule



Create New Policy

Name and properties ✓
demo1

Rules
Define policy rules

Order	Rule type	Rule name	Criteria

Create new rule

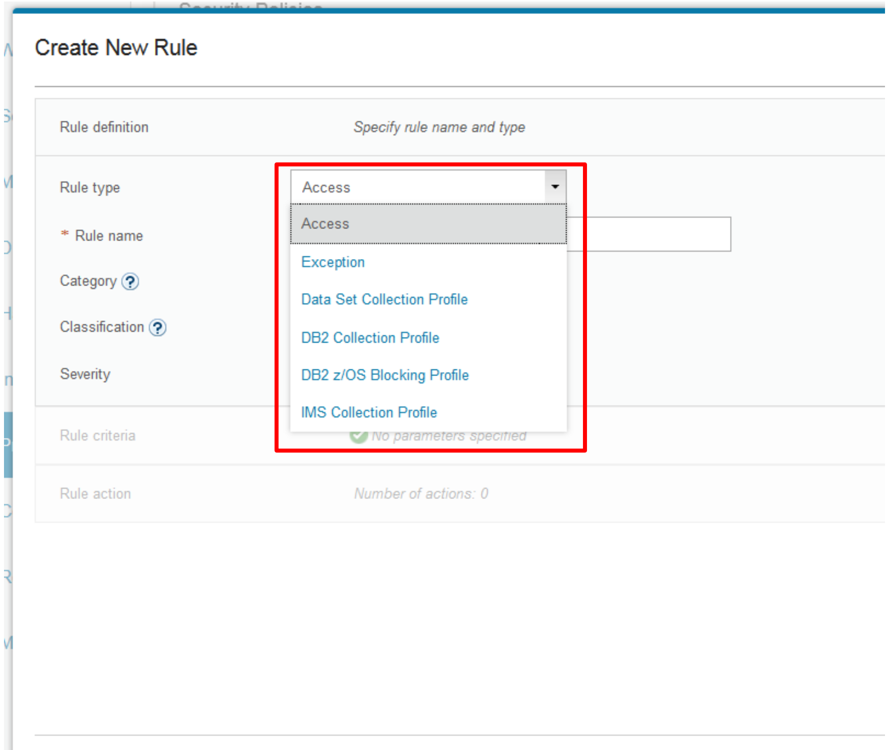
Rule definition
Specify rule name and type

Rule type	Access
* Rule name	*Enter rule name*
Category ?	*Enter rule category*
Classification ?	*Enter rule classification*
Severity	Information

Rule criteria ✓
No parameters specified

Rule action
Number of actions: 0

Rule type – new vs legacy



Create New Rule

Rule definition — *Specify rule name and type*

Rule type: Access

* Rule name

Category

Classification

Severity

Rule criteria — *No parameters specified*

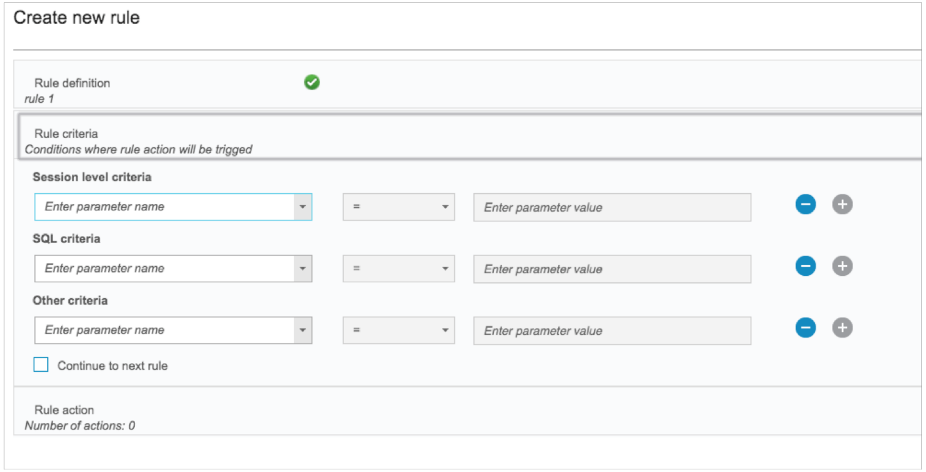
Rule action — *Number of actions: 0*

The new UI rule type includes the collection and blocking profiles.

In the legacy UI, users access the collection profile types by choosing access rule and DB type= <collection profile type>

Extrusion is also a rule type, but it was not enabled on the system this screen shot was taken.

Rule criteria – new vs legacy



Create new rule

Rule definition ✓
rule 1

Rule criteria
Conditions where rule action will be trigged

Session level criteria

Enter parameter name | = | *Enter parameter value* | − | +

SQL criteria

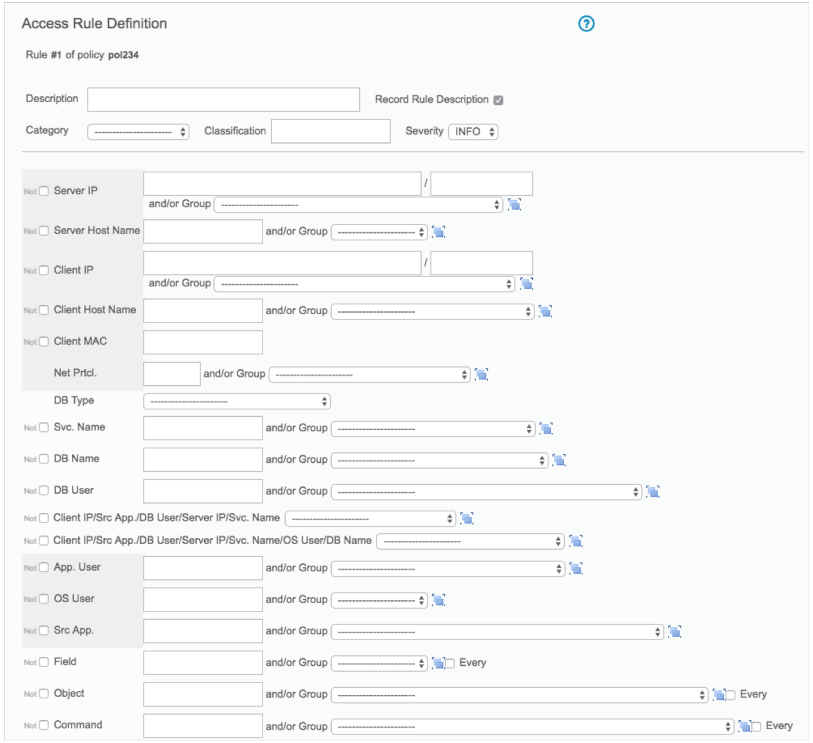
Enter parameter name | = | *Enter parameter value* | − | +

Other criteria

Enter parameter name | = | *Enter parameter value* | − | +

□ Continue to next rule

Rule action
Number of actions: 0



Access Rule Definition

Rule **#1** of policy **pol234**

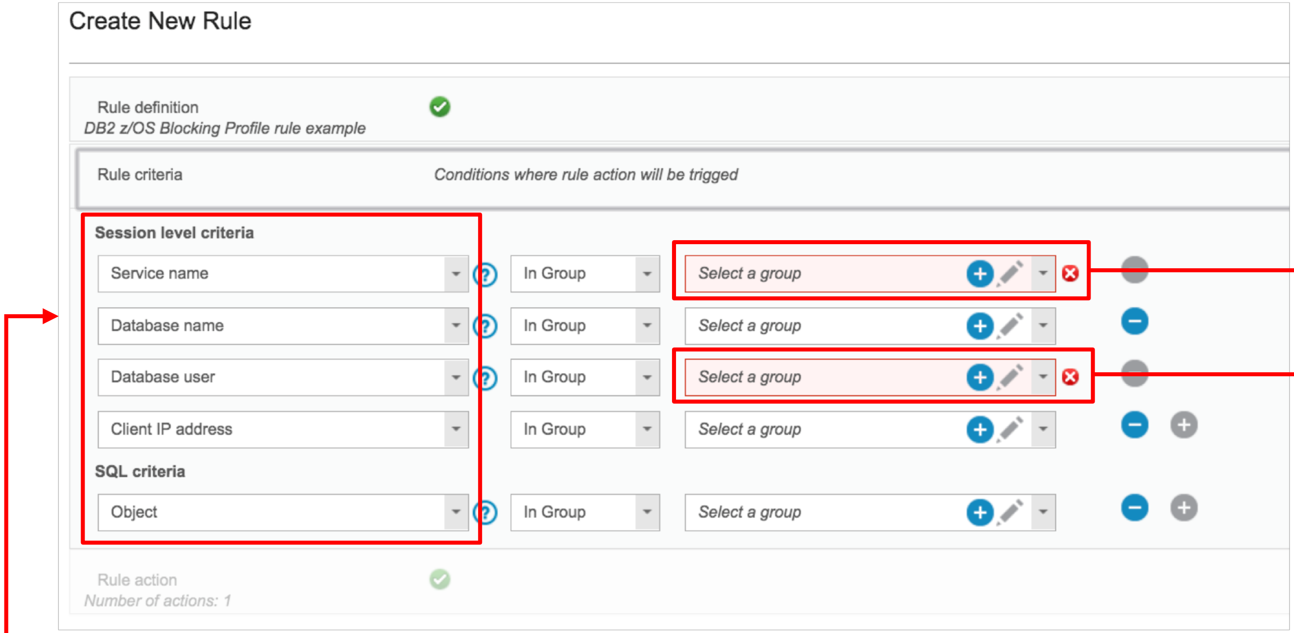
Description ______ Record Rule Description ☑

Category -------------------- Classification ______ Severity INFO

Not □ Server IP ______ / ______ and/or Group --------------------
Not □ Server Host Name ______ and/or Group --------------------
Not □ Client IP ______ / ______ and/or Group --------------------
Not □ Client Host Name ______ and/or Group --------------------
Not □ Client MAC ______
Net Prtcl. ______ and/or Group --------------------
DB Type --------------------
Not □ Svc. Name ______ and/or Group --------------------
Not □ DB Name ______ and/or Group --------------------
Not □ DB User ______ and/or Group --------------------
Not □ Client IP/Src App./DB User/Server IP/Svc. Name --------------------
Not □ Client IP/Src App./DB User/Server IP/Svc. Name/OS User/DB Name --------------------
Not □ App. User ______ and/or Group --------------------
Not □ OS User ______ and/or Group --------------------
Not □ Src App. ______ and/or Group --------------------
Not □ Field ______ and/or Group -------------------- □ Every
Not □ Object ______ and/or Group -------------------- □ Every
Not □ Command ______ and/or Group -------------------- □ Every

- Removed cluttering UI
  - Allow user to add or delete parameter with '-' and '+' button
  - Indicates required parameter by showing red textbox
  - Some rule type has predefined criteria

Example of prepopulated criteria



Create New Rule

Rule definition
DB2 z/OS Blocking Profile rule example

Rule criteria — *Conditions where rule action will be trigged*

Session level criteria

Service name	In Group	*Select a group*
Database name	In Group	*Select a group*
Database user	In Group	*Select a group*
Client IP address	In Group	*Select a group*

SQL criteria

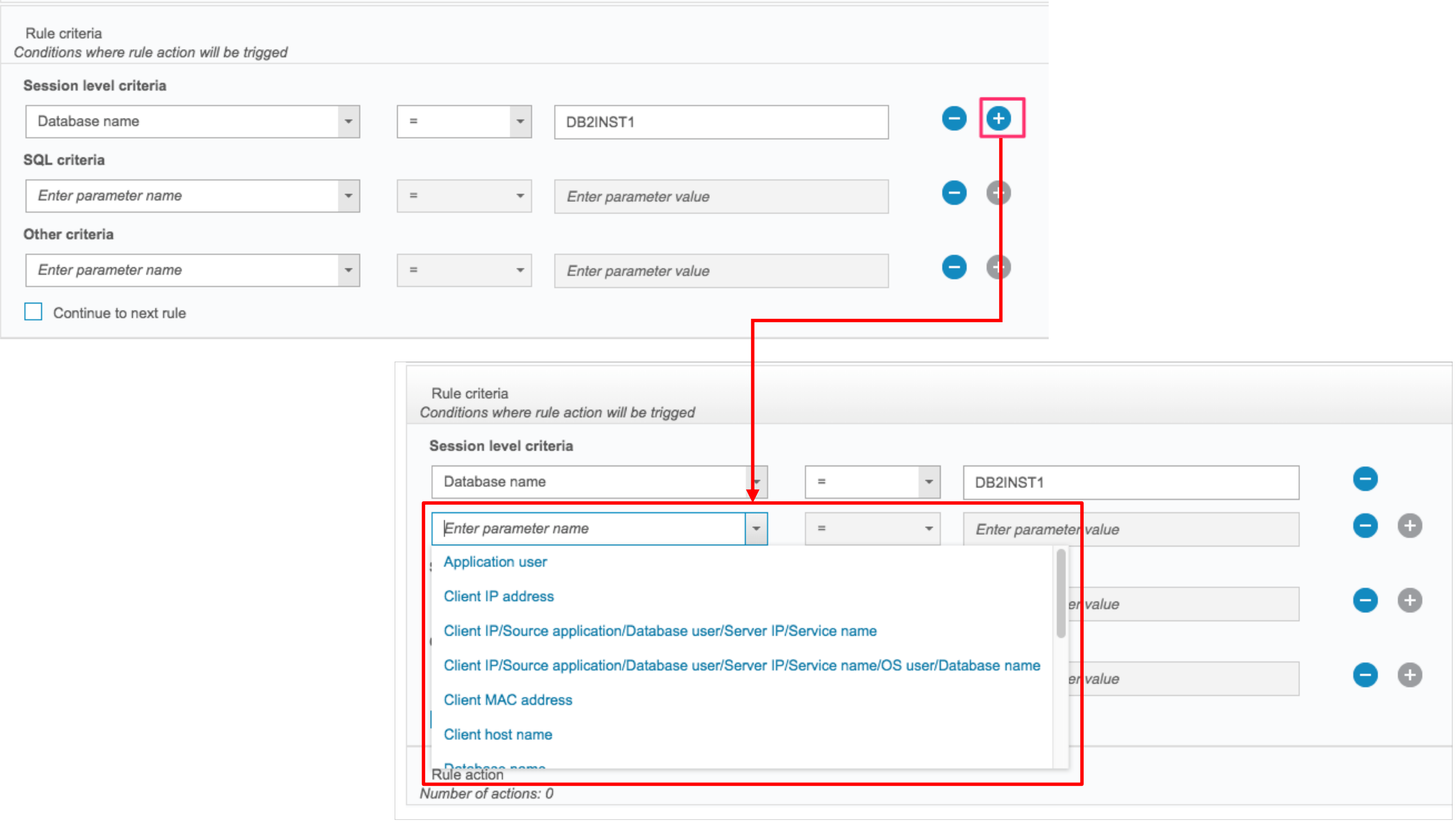
Object	In Group	*Select a group*

Rule action
Number of actions: 1

Prepopulated criteria based on selected rule type

Required parameters will be displayed as red textbox

Adding rule criteria



Rule criteria
Conditions where rule action will be trigged

Session level criteria

Database name | = | DB2INST1

SQL criteria

Enter parameter name | = | *Enter parameter value*

Other criteria

Enter parameter name | = | *Enter parameter value*

□ Continue to next rule

Rule criteria
Conditions where rule action will be trigged

Session level criteria

Database name | = | DB2INST1

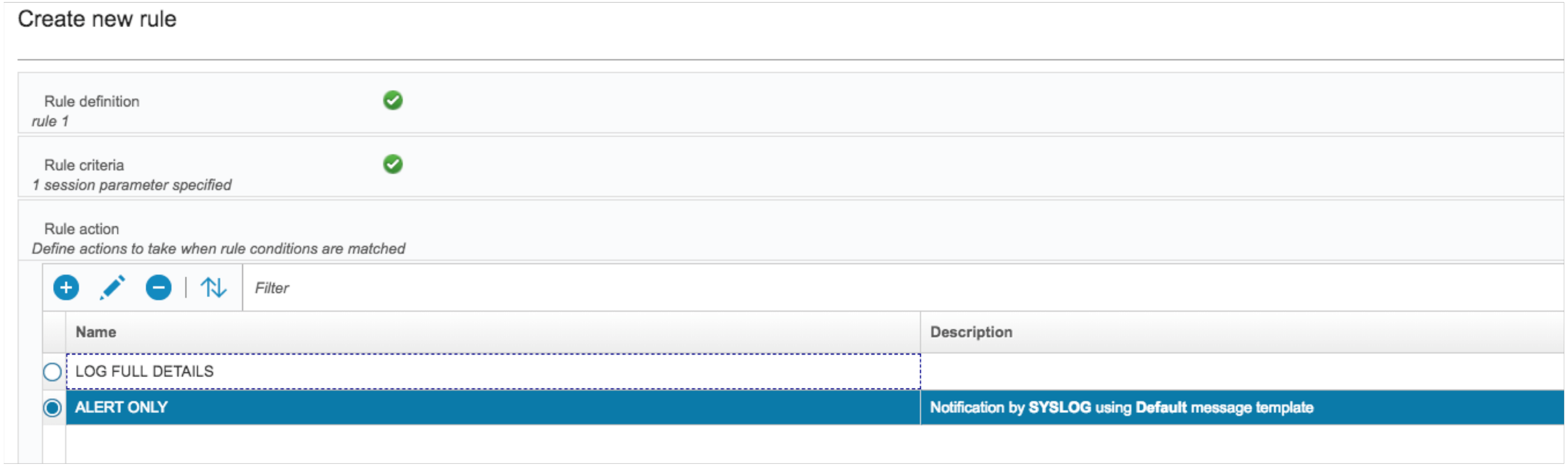
Enter parameter name | = | *Enter parameter value*

- Application user
- Client IP address
- Client IP/Source application/Database user/Server IP/Service name
- Client IP/Source application/Database user/Server IP/Service name/OS user/Database name
- Client MAC address
- Client host name
- Database name

Rule action
Number of actions: 0

Rule action

Rule action



Create new rule

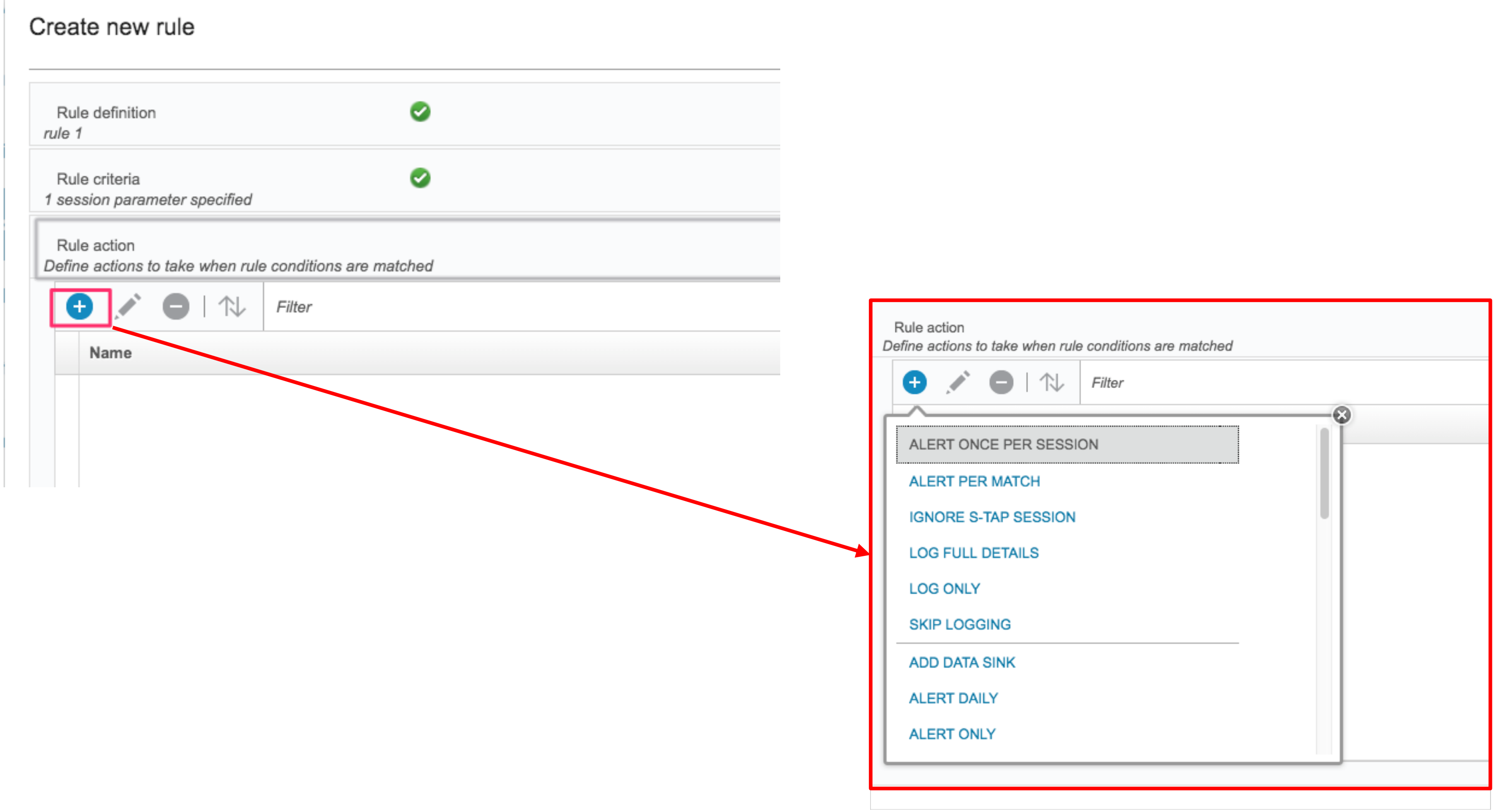
Rule definition ✓
rule 1

Rule criteria ✓
1 session parameter specified

Rule action
Define actions to take when rule conditions are matched

	Name	Description
○	LOG FULL DETAILS	
●	ALERT ONLY	Notification by **SYSLOG** using **Default** message template

Adding rule action



Create new rule

Rule definition ✓
rule 1

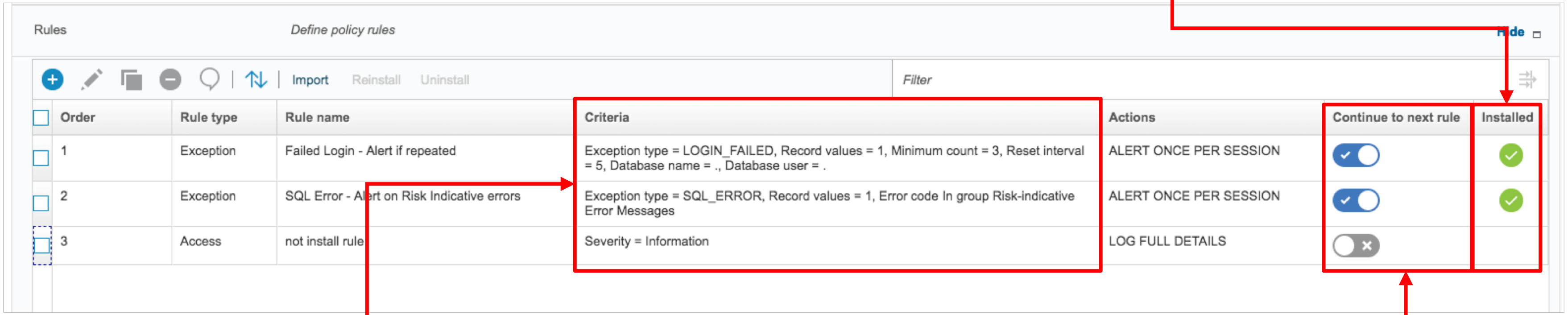
Rule criteria ✓
1 session parameter specified

Rule action
Define actions to take when rule conditions are matched

Rule action
Define actions to take when rule conditions are matched

Defined rules

- Installation indicator
  - Check box means rules are currently installed
  - Rule can be marked install by re-installing the policy



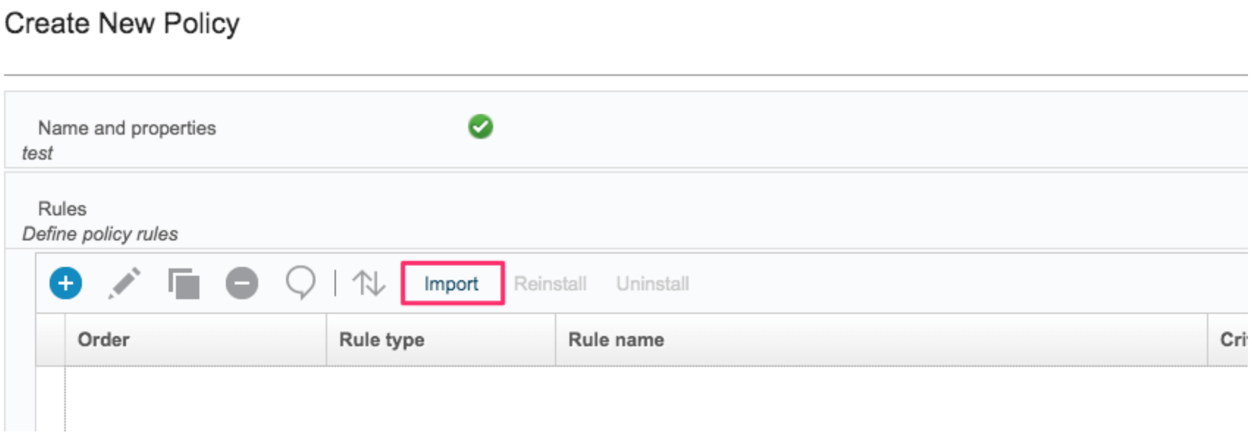
□	Order	Rule type	Rule name	Criteria	Actions	Continue to next rule	Installed
□	1	Exception	Failed Login - Alert if repeated	Exception type = LOGIN_FAILED, Record values = 1, Minimum count = 3, Reset interval = 5, Database name = ., Database user = .	ALERT ONCE PER SESSION	✓	✓
□	2	Exception	SQL Error - Alert on Risk Indicative errors	Exception type = SQL_ERROR, Record values = 1, Error code In group Risk-indicative Error Messages	ALERT ONCE PER SESSION	✓	✓
□	3	Access	not install rule	Severity = Information	LOG FULL DETAILS	✕	

- Defined criteria
  - Criteria are displayed in csv format

- Allow user to control ’Continue to next rule’
  - Blue check box means enabled

Import rules

Import from other policy



Create New Policy

Name and properties ✓

test

Rules

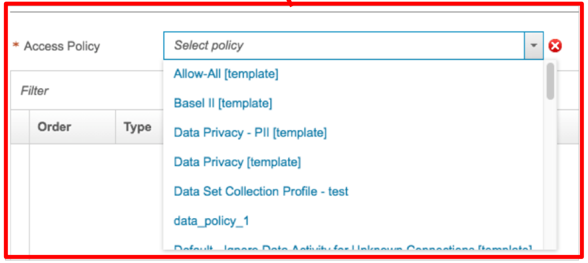
Define policy rules

Order	Rule type	Rule name	Cri

- Rules defined in other policy can be imported
- Policy type must be same
  - Data level policy cannot import rules from session level policy and vice versa

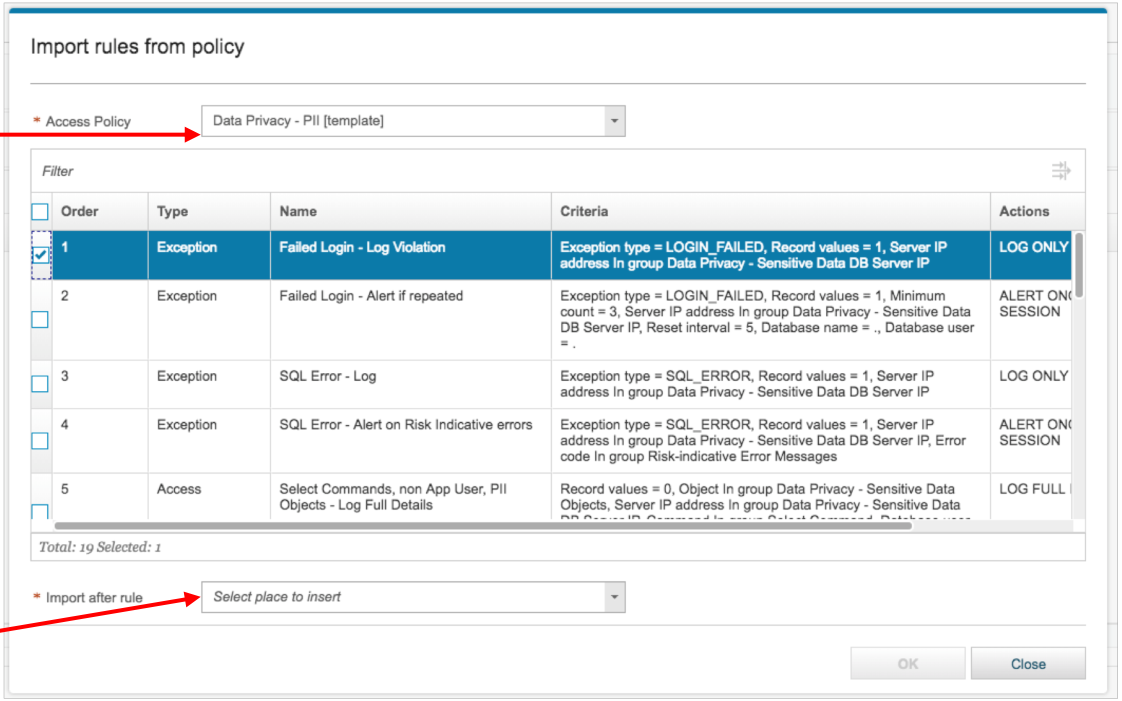
Import rules from policy

Policy to import rules from



* Access Policy: Select policy

- Allow-All [template]
- Basel II [template]
- Data Privacy - PII [template]
- Data Privacy [template]
- Data Set Collection Profile - test
- data_policy_1
- Default - Ignore Data Activity for Unknown Connections [template]



Import rules from policy

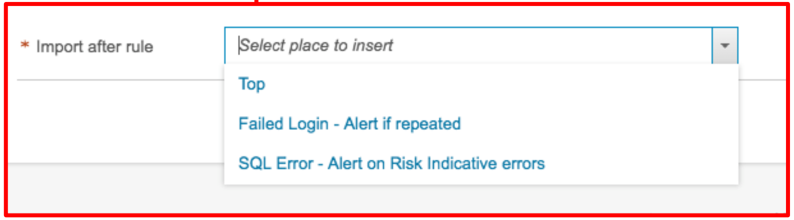
* Access Policy: Data Privacy - PII [template]

	Order	Type	Name	Criteria	Actions
☑	1	Exception	Failed Login - Log Violation	Exception type = LOGIN_FAILED, Record values = 1, Server IP address In group Data Privacy - Sensitive Data DB Server IP	LOG ONLY
□	2	Exception	Failed Login - Alert if repeated	Exception type = LOGIN_FAILED, Record values = 1, Minimum count = 3, Server IP address In group Data Privacy - Sensitive Data DB Server IP, Reset interval = 5, Database name = ., Database user = .	ALERT ON(SESSION
□	3	Exception	SQL Error - Log	Exception type = SQL_ERROR, Record values = 1, Server IP address In group Data Privacy - Sensitive Data DB Server IP	LOG ONLY
□	4	Exception	SQL Error - Alert on Risk Indicative errors	Exception type = SQL_ERROR, Record values = 1, Server IP address In group Data Privacy - Sensitive Data DB Server IP, Error code In group Risk-indicative Error Messages	ALERT ON(SESSION
□	5	Access	Select Commands, non App User, PII Objects - Log Full Details	Record values = 0, Object In group Data Privacy - Sensitive Data Objects, Server IP address In group Data Privacy - Sensitive Data DB Server IP, Command In group Select Command, Database user	LOG FULL

Total: 19 Selected: 1

* Import after rule: *Select place to insert*

Select import order



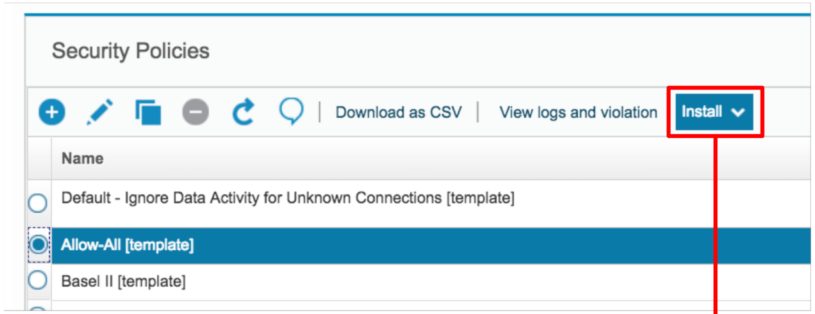
* Import after rule: *Select place to insert*

- Top
- Failed Login - Alert if repeated
- SQL Error - Alert on Risk Indicative errors

Policy installation

Install action

- New policy installation actions
  - Install before
  - Install and replace

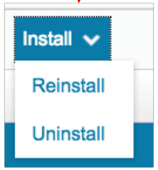


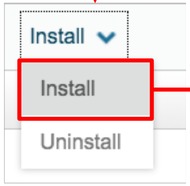
Security Policies

Name
○ Default - Ignore Data Activity for Unknown Connections [template]
● Allow-All [template]
○ Basel II [template]

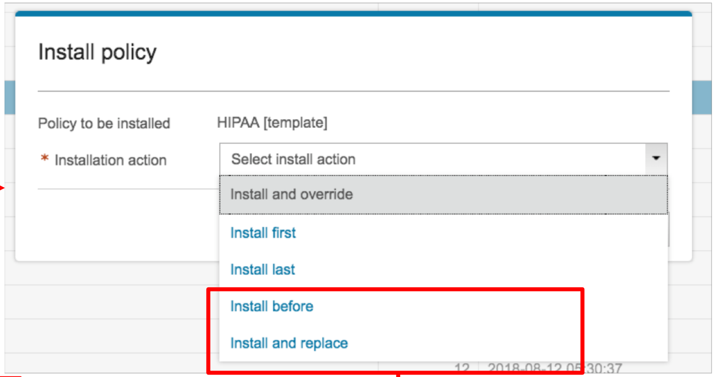
Selected policy is already installed

Selected policy is not installed





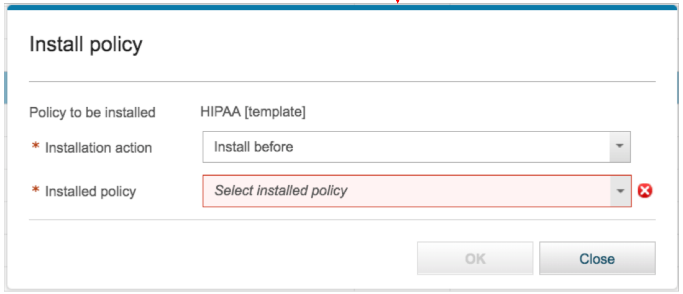
Selected install action



Install policy

Policy to be installed: HIPAA [template]

* Installation action: Select install action



Install policy

Policy to be installed: HIPAA [template]

* Installation action: Install before

* Installed policy: *Select installed policy*

Session Level Policy

What is session level policy

- New rule types introduced in 10.6
- Improved performance because validation occurs at beginning of sniffer processing
- Strictly define policy based on session level criteria
- The policies with session rule type will be installed before regular policies
- Not backward compatible. The policy can only be installed on machine v10.6 or above.

When is it useful?

1. Decrease the load on collector
   - Trusted session scenario: policy rule to ignore sessions from certain IP address
     - If session consists of binary traffic with no SQL statements, a regular rule would never be triggered. Session level policy is solution for this case.
   - Policy with rule to ignore non-privileged user S-TAP session
     - As a “regular policy” session will be ignored after first SQL statement.
     - As a session level policy, session will be ignored on authentication stage before first SQL statement received from S-TAP. So as a result no SQL will be processed by sniffer.

2. Optimizing firewall
   - Restrict database user from using a certain program by terminating session.
   - Restrict database user to access from certain IP addresses by terminating session.

   Without session level rules, reaction based on SQL requests which could do harm.

3. Transformation
   - Session level rule allows transform of user names, db names, source programs in runtime for SIEM
   - Transforming user name based on what is defined in policy.

Supported actions in session level

- Decrease the load on collector.
  - SELECTIVE SESSION AUDIT
  - SR IGNORE SESSION
- Optimizing firewall
  - S-GATE SESSION ATTACH
  - S-GATE SESSION ATTACH OR DETACH
  - S-GATE SESSION DETACH
  - S-GATE SESSION TERMINATE
- Transformation
  - TRANSFORM CLIENT HOST NAME
  - TRANSFORM DB NAME
  - TRANSFORM DB_USER NAME
  - TRANSFORM OS USER
  - TRANSFORM SERVER HOST NAME
  - TRANSFORM SERVICE NAME
  - TRANSFORM SOURCE PROGRAM NAME

Supported database types

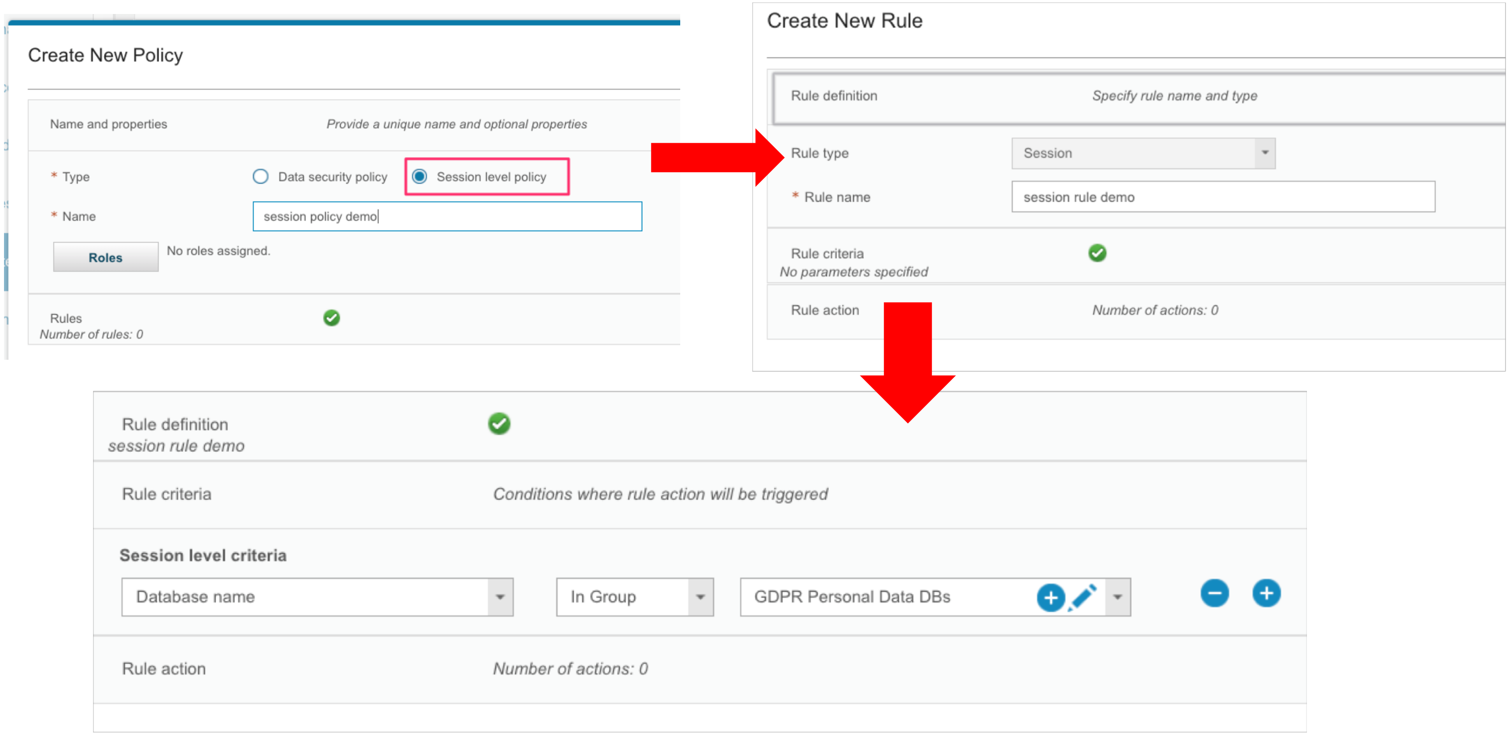
- ASTER
- CASSANDRA
- DB2
- GREENPLUMDB
- HADOOP
- HP-Vertica
- IBM INFORMIX (DRDA)
- IBM ISERIES
- INFORMIX
- MARIADB
- MEMSQL
- MONGODB
- MS SQL SERVER
- MYSQL
- NETEZZA
- ORACLE
- POSTGRESQL
- SAP HANA
- SYBASE
- TERADATA

Unsupported database types

- HTTP
- HIVE
- IMPALA
- WEBHDFS
- FTP
- CIFS
- COUCHDB
- IMS
- DATA SET
- DB2 z/OS

Flow of session level policy

- Once the policy is saved as ‘Session level policy’, it cannot be switched over to ‘Data security policy’
- Unlike access policy, it allows user to only define criteria based on session



Create New Policy

Name and properties — *Provide a unique name and optional properties*

* Type ○ Data security policy ● Session level policy

* Name: session policy demo

Roles — No roles assigned.

Rules ✓
Number of rules: 0

Create New Rule

Rule definition — *Specify rule name and type*

Rule type: Session

* Rule name: session rule demo

Rule criteria ✓
No parameters specified

Rule action — *Number of actions: 0*

Rule definition ✓
session rule demo

Rule criteria — *Conditions where rule action will be triggered*

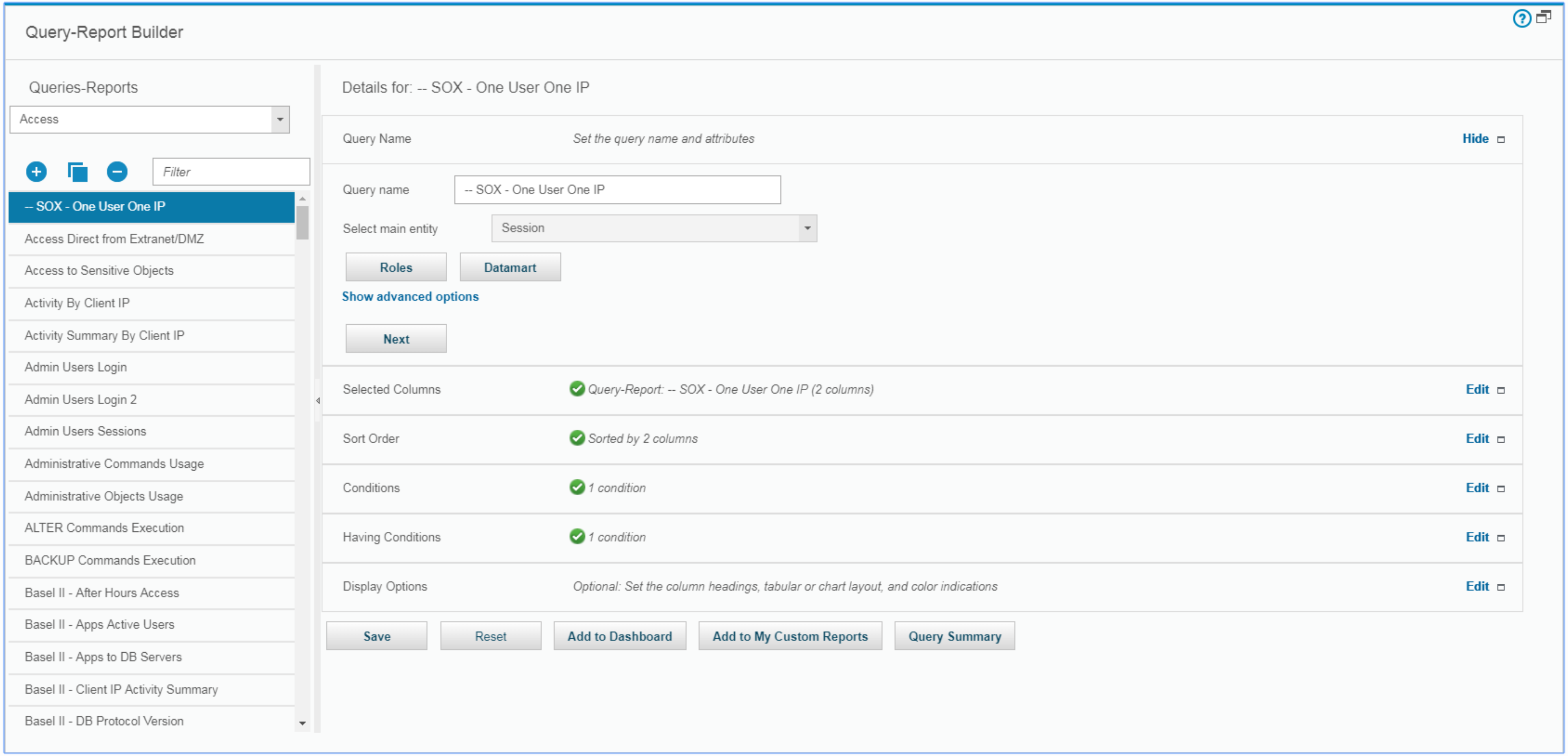
Session level criteria

Database name | In Group | GDPR Personal Data DBs

Rule action — *Number of actions: 0*

New Query Builder

Query-Report Builder Screen Structure



Query-Report Builder

Queries-Reports

Access

Filter

- -- SOX - One User One IP
- Access Direct from Extranet/DMZ
- Access to Sensitive Objects
- Activity By Client IP
- Activity Summary By Client IP
- Admin Users Login
- Admin Users Login 2
- Admin Users Sessions
- Administrative Commands Usage
- Administrative Objects Usage
- ALTER Commands Execution
- BACKUP Commands Execution
- Basel II - After Hours Access
- Basel II - Apps Active Users
- Basel II - Apps to DB Servers
- Basel II - Client IP Activity Summary
- Basel II - DB Protocol Version

Details for: -- SOX - One User One IP

Query Name — *Set the query name and attributes* — Hide

Query name: -- SOX - One User One IP

Select main entity: Session

Selected Columns — ✓ *Query-Report: -- SOX - One User One IP (2 columns)* — Edit

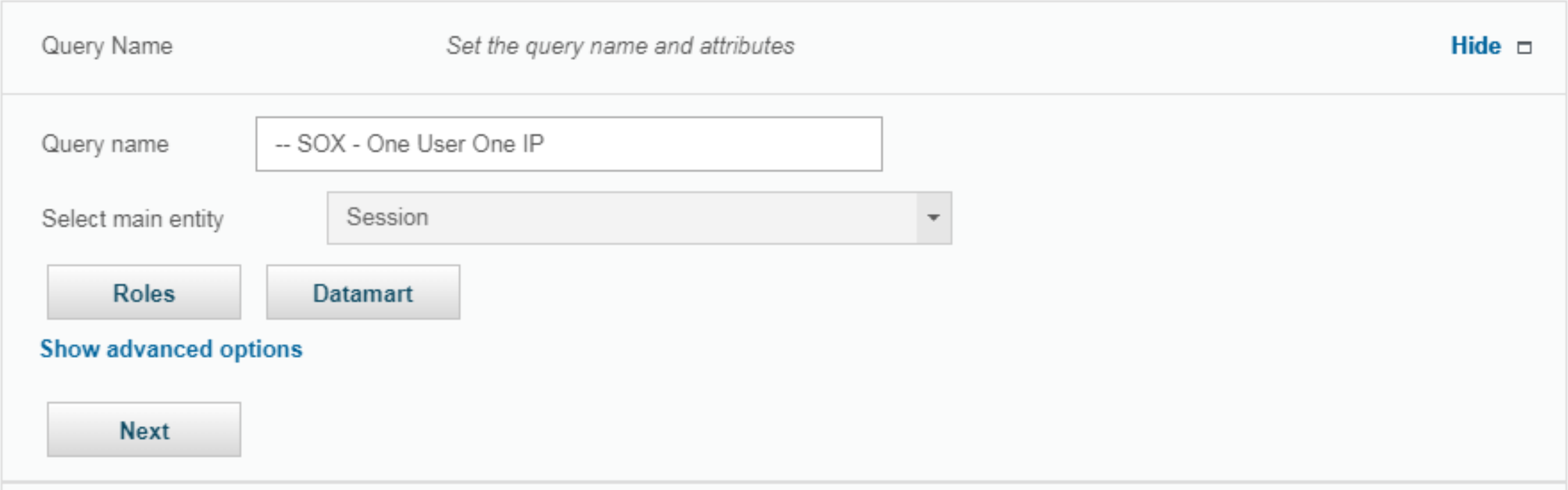
Sort Order — ✓ *Sorted by 2 columns* — Edit

Conditions — ✓ *1 condition* — Edit

Having Conditions — ✓ *1 condition* — Edit

Display Options — *Optional: Set the column headings, tabular or chart layout, and color indications* — Edit

Query Name and Attributes

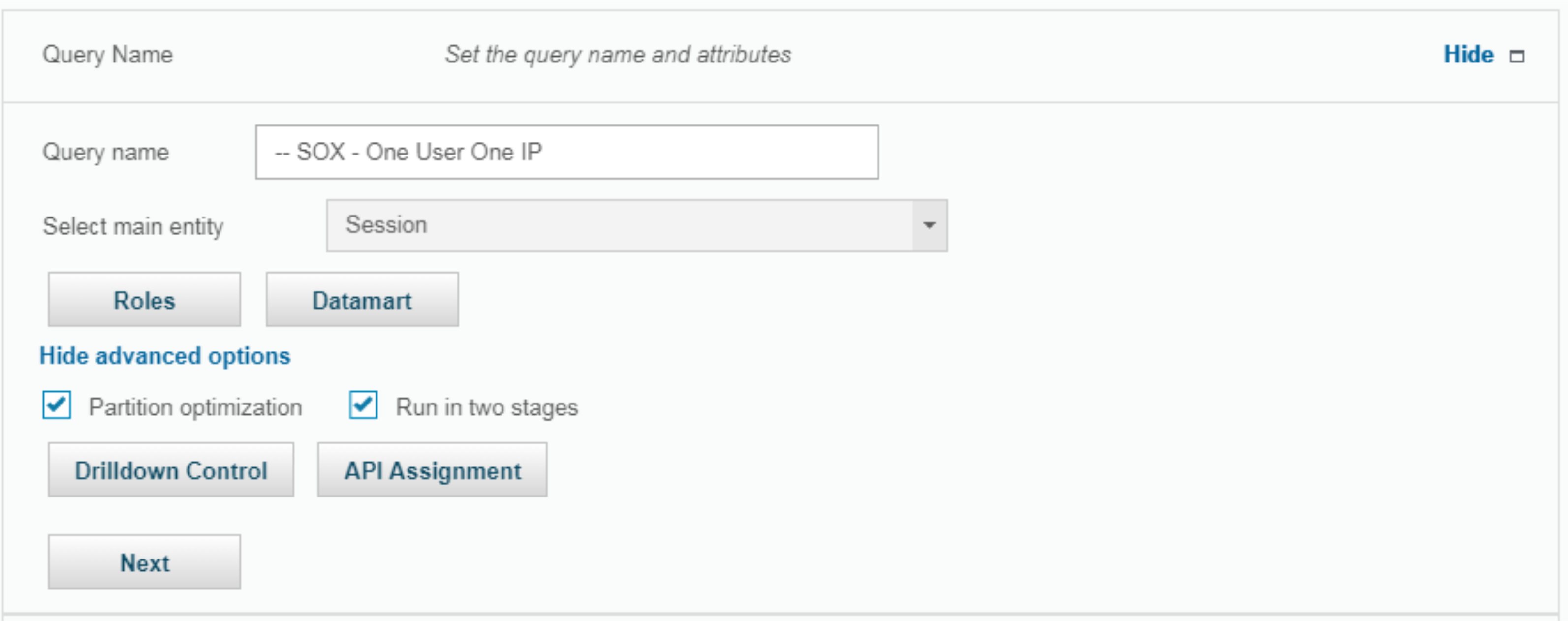


Query Name *Set the query name and attributes*

Query name: -- SOX - One User One IP

Select main entity: Session

Query Name and Attributes – Advanced Options



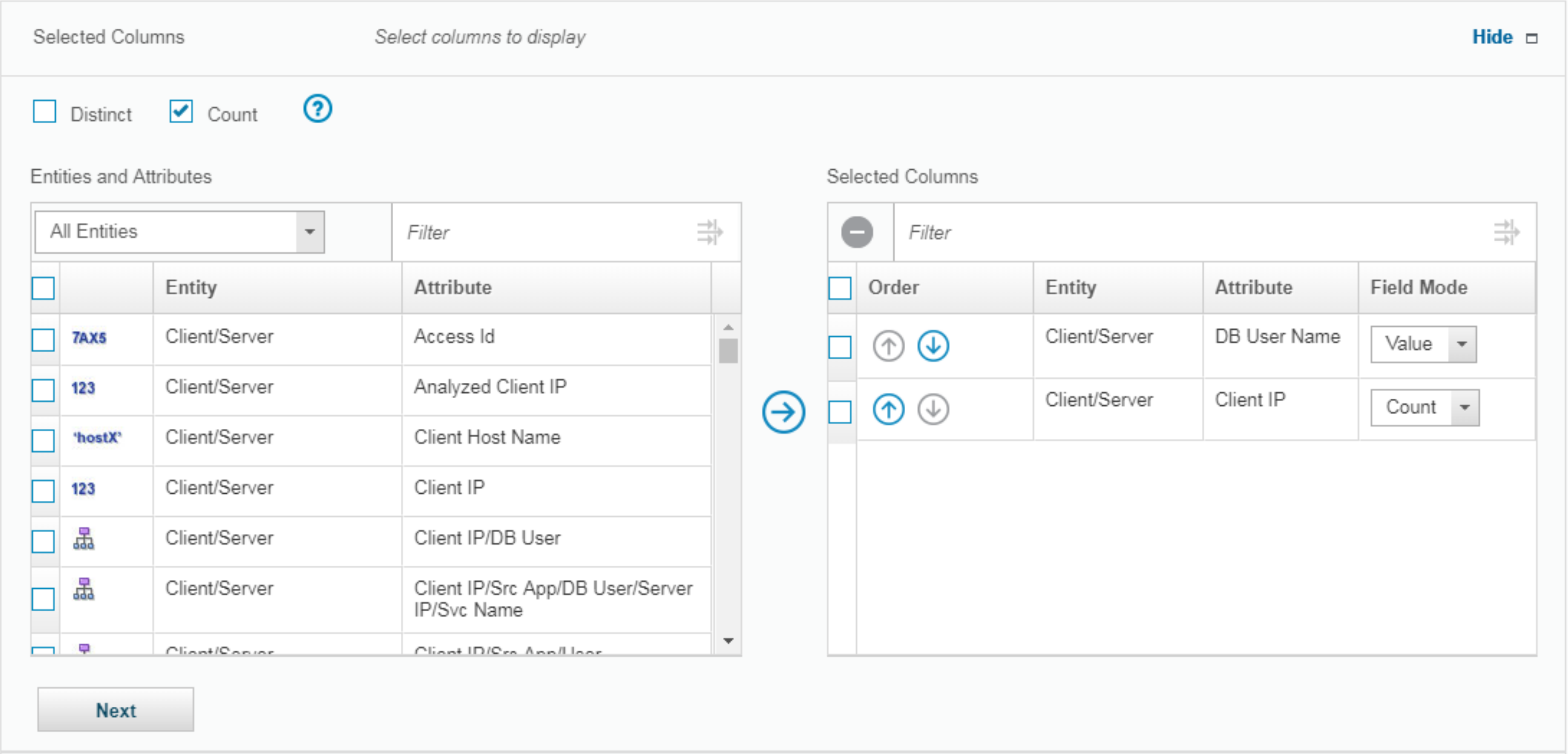
Query Name *Set the query name and attributes*

Query name: -- SOX - One User One IP

Select main entity: Session

☑ Partition optimization ☑ Run in two stages

Columns



Selected Columns *Select columns to display* **Hide**

□ Distinct ☑ Count ?

Entities and Attributes

All Entities ▾ | *Filter*

□		Entity	Attribute
□	7AX5	Client/Server	Access Id
□	123	Client/Server	Analyzed Client IP
□	'hostX'	Client/Server	Client Host Name
□	123	Client/Server	Client IP
□		Client/Server	Client IP/DB User
□		Client/Server	Client IP/Src App/DB User/Server IP/Svc Name
□		Client/Server	Client IP/Src App/User

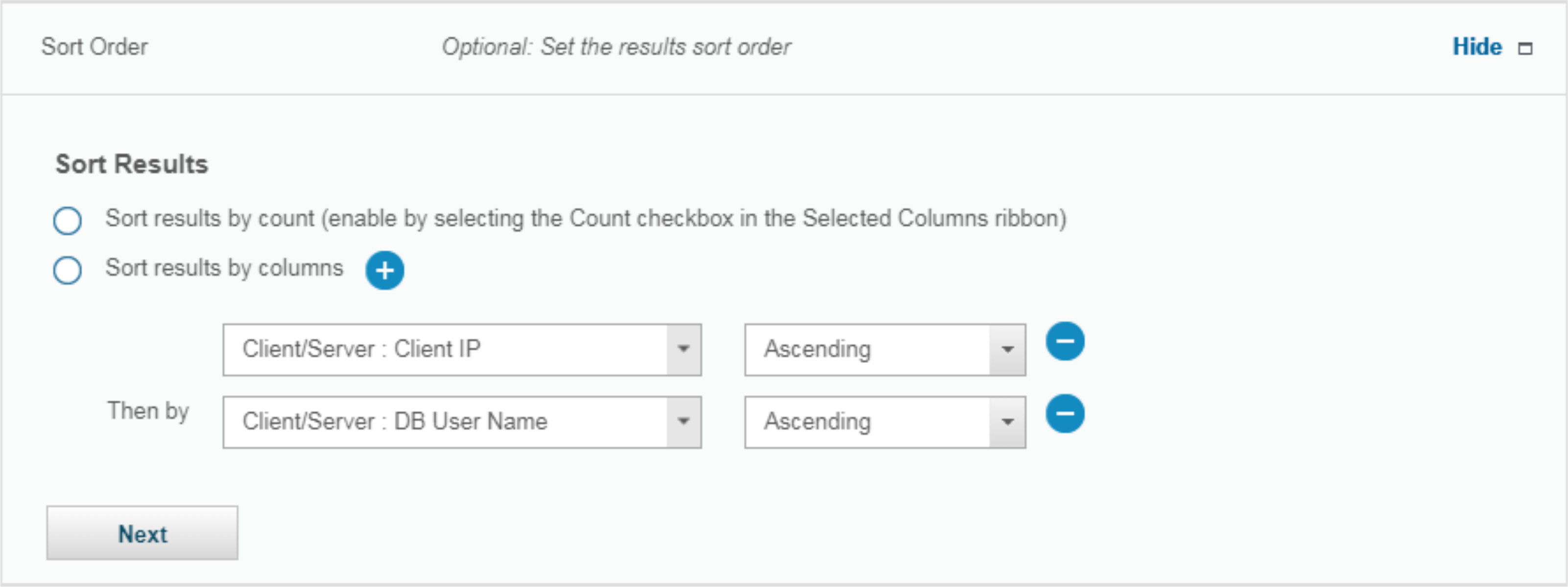
Selected Columns

Filter

□	Order	Entity	Attribute	Field Mode
□	↑ ↓	Client/Server	DB User Name	Value ▾
□	↑ ↓	Client/Server	Client IP	Count ▾

Next

Sort Order



Sort Order *Optional: Set the results sort order* Hide

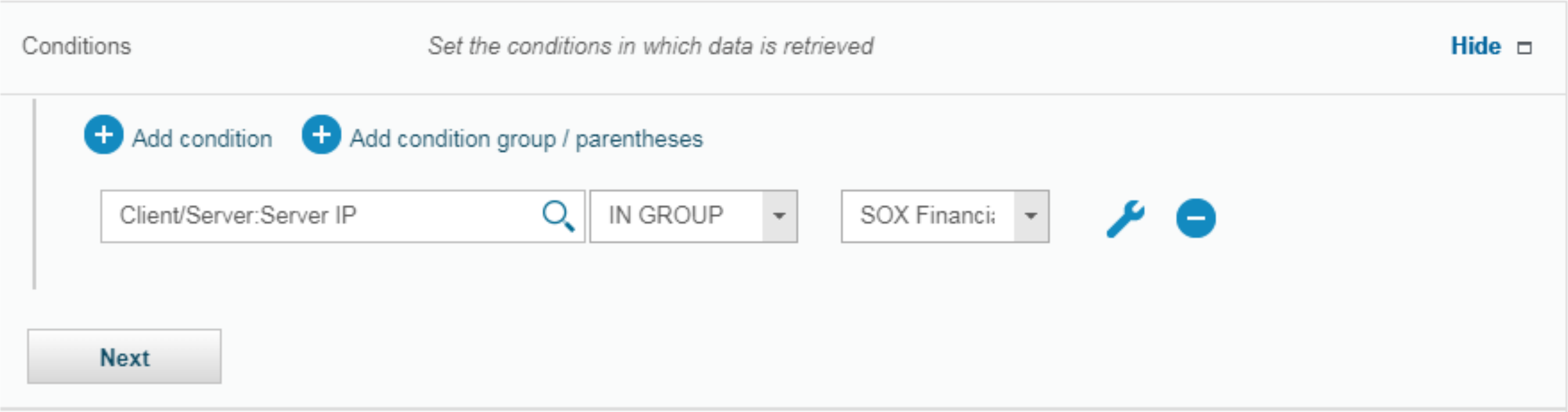
Sort Results

○ Sort results by count (enable by selecting the Count checkbox in the Selected Columns ribbon)

○ Sort results by columns

	Client/Server : Client IP	Ascending
Then by	Client/Server : DB User Name	Ascending

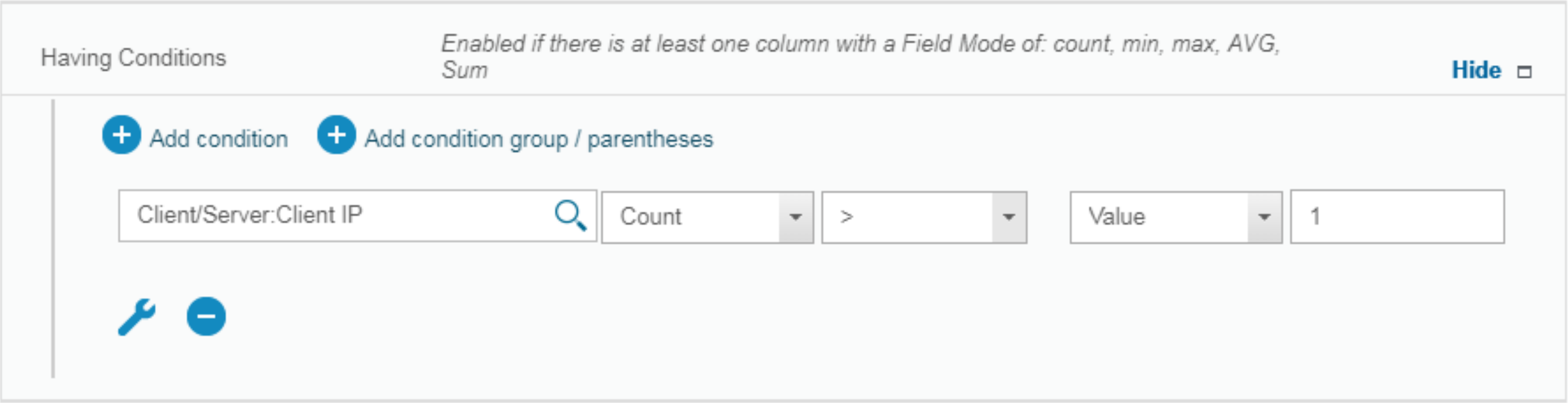
Conditions



Conditions — *Set the conditions in which data is retrieved*

Client/Server:Server IP — IN GROUP — SOX Financi:

Having Conditions

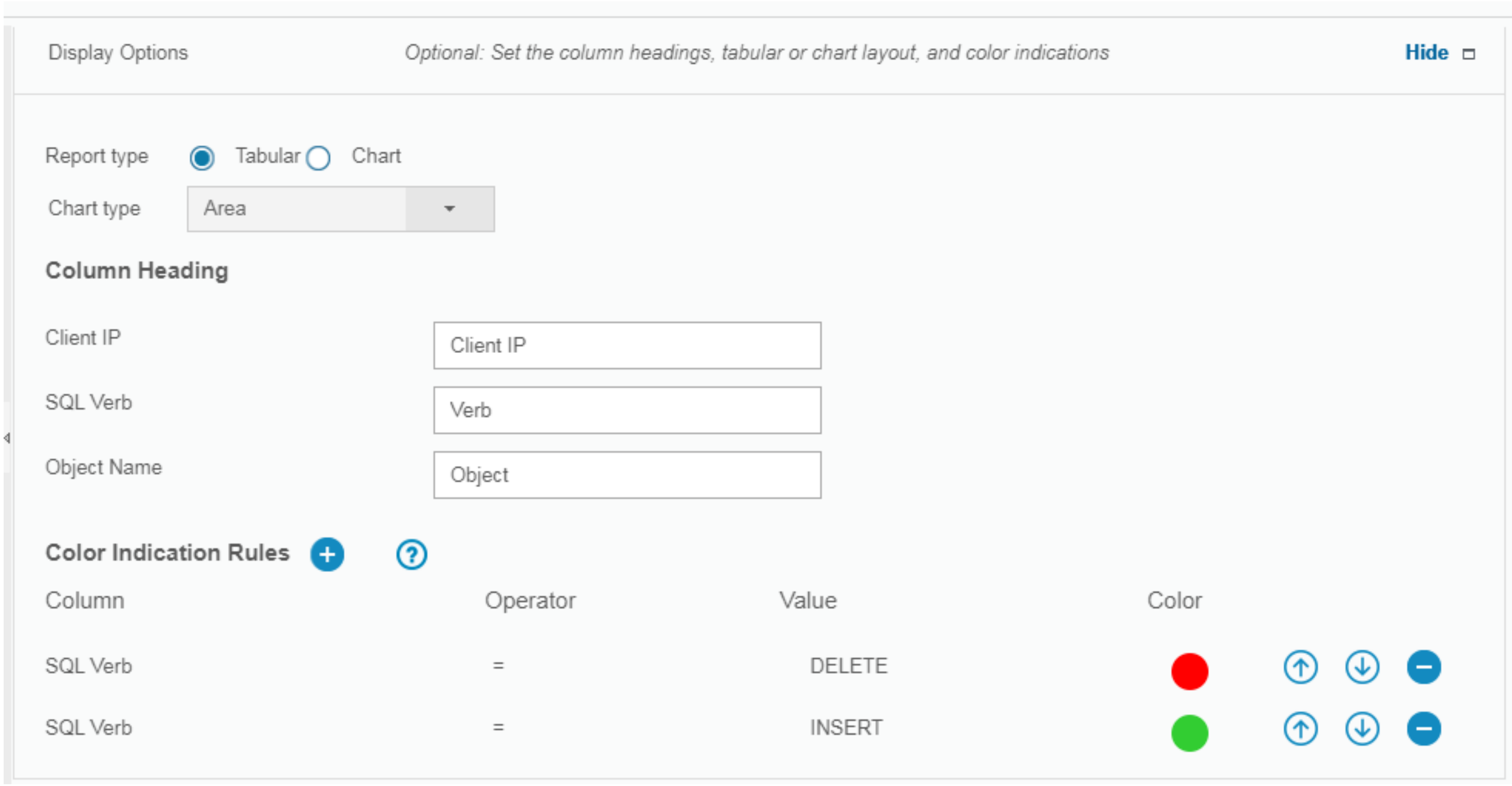


Having Conditions

Enabled if there is at least one column with a Field Mode of: count, min, max, AVG, Sum

Client/Server:Client IP | Count | > | Value | 1

Display Options



Display Options *Optional: Set the column headings, tabular or chart layout, and color indications* **Hide**

Report type ● Tabular ○ Chart

Chart type: Area

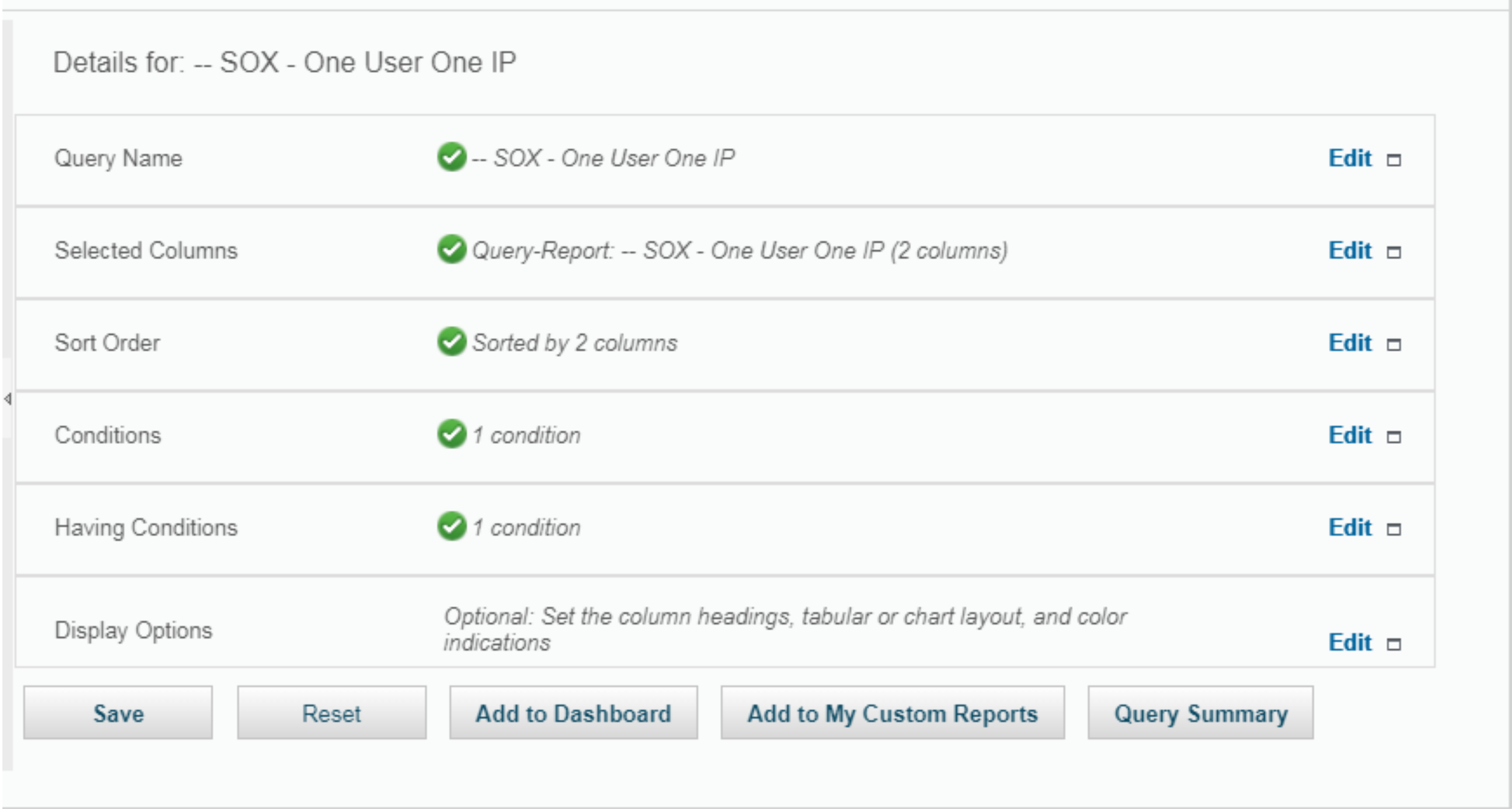
Column Heading

Client IP	Client IP
SQL Verb	Verb
Object Name	Object

Color Indication Rules

Column	Operator	Value	Color
SQL Verb	=	DELETE	🔴
SQL Verb	=	INSERT	🟢

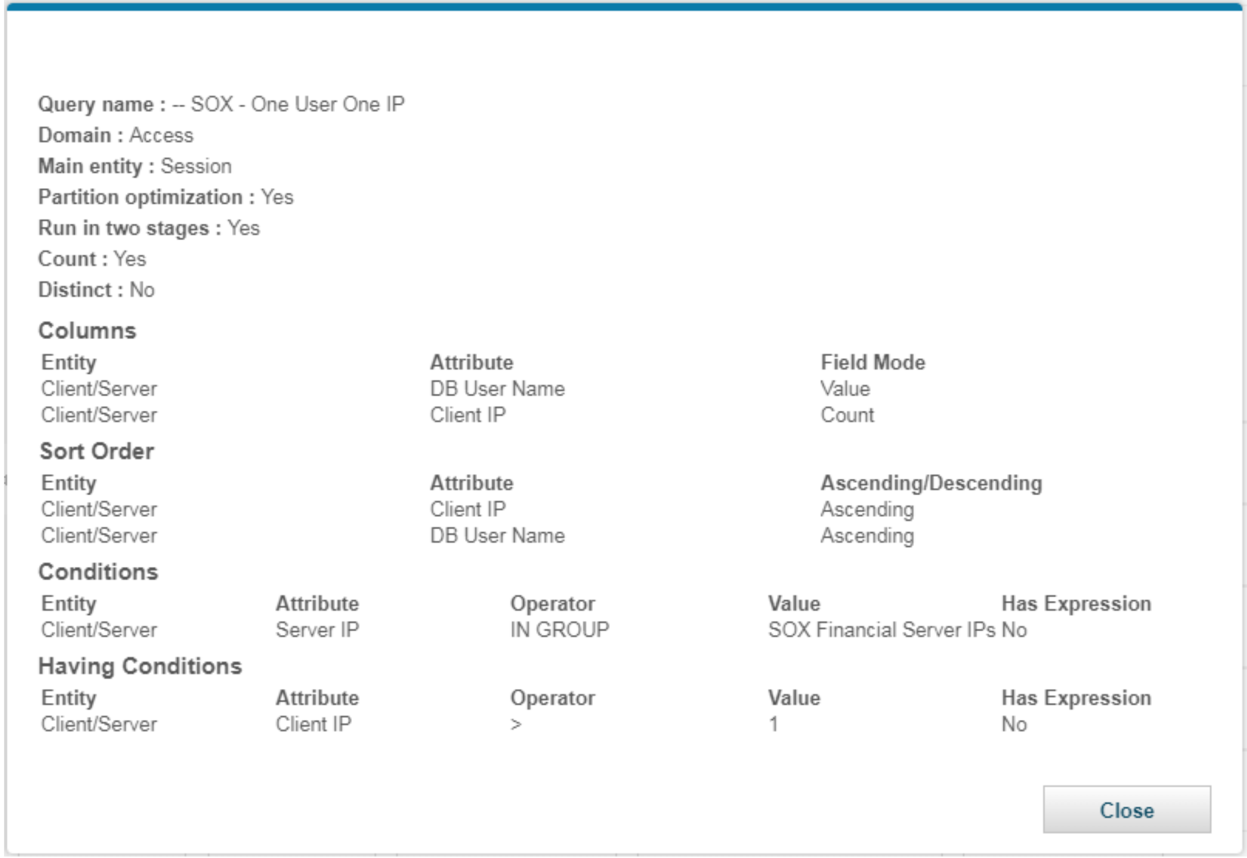
Screen Buttons



Details for: -- SOX - One User One IP

Query Name	✓ *-- SOX - One User One IP*	Edit
Selected Columns	✓ *Query-Report: -- SOX - One User One IP (2 columns)*	Edit
Sort Order	✓ *Sorted by 2 columns*	Edit
Conditions	✓ *1 condition*	Edit
Having Conditions	✓ *1 condition*	Edit
Display Options	*Optional: Set the column headings, tabular or chart layout, and color indications*	Edit

Query Summary



Query name : -- SOX - One User One IP
Domain : Access
Main entity : Session
Partition optimization : Yes
Run in two stages : Yes
Count : Yes
Distinct : No

Columns

Entity	Attribute	Field Mode
Client/Server	DB User Name	Value
Client/Server	Client IP	Count

Sort Order

Entity	Attribute	Ascending/Descending
Client/Server	Client IP	Ascending
Client/Server	DB User Name	Ascending

Conditions

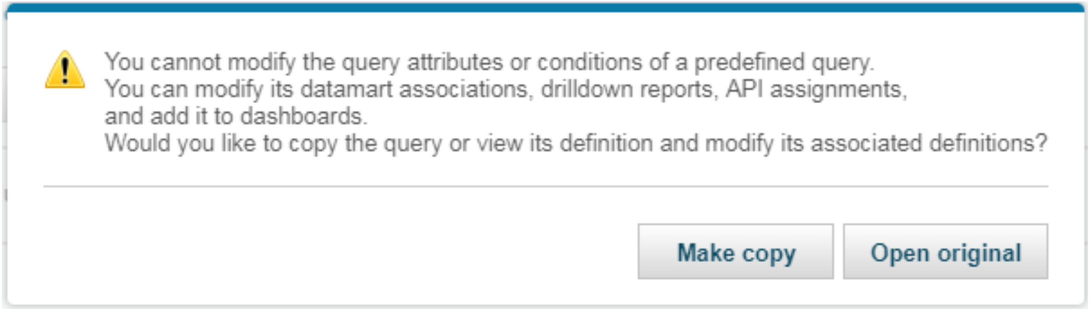
Entity	Attribute	Operator	Value	Has Expression
Client/Server	Server IP	IN GROUP	SOX Financial Server IPs	No

Having Conditions

Entity	Attribute	Operator	Value	Has Expression
Client/Server	Client IP	>	1	No

Predefined Queries

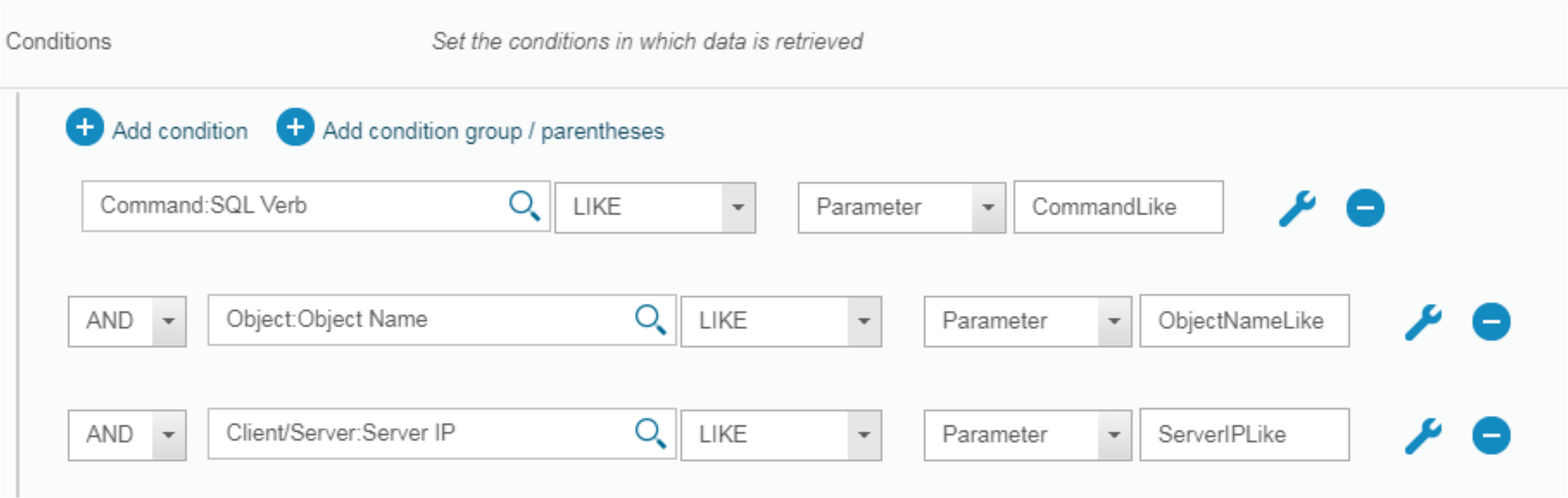
- The query cannot be modified
- Can set roles, datamart, report drilldown, API assignment
- Can add to dashboards and custom reports menu
- When selected, the user is prompted to open the original or make a copy



You cannot modify the query attributes or conditions of a predefined query.
You can modify its datamart associations, drilldown reports, API assignments,
and add it to dashboards.
Would you like to copy the query or view its definition and modify its associated definitions?

Query Conditions

Simple Conditions – One Level

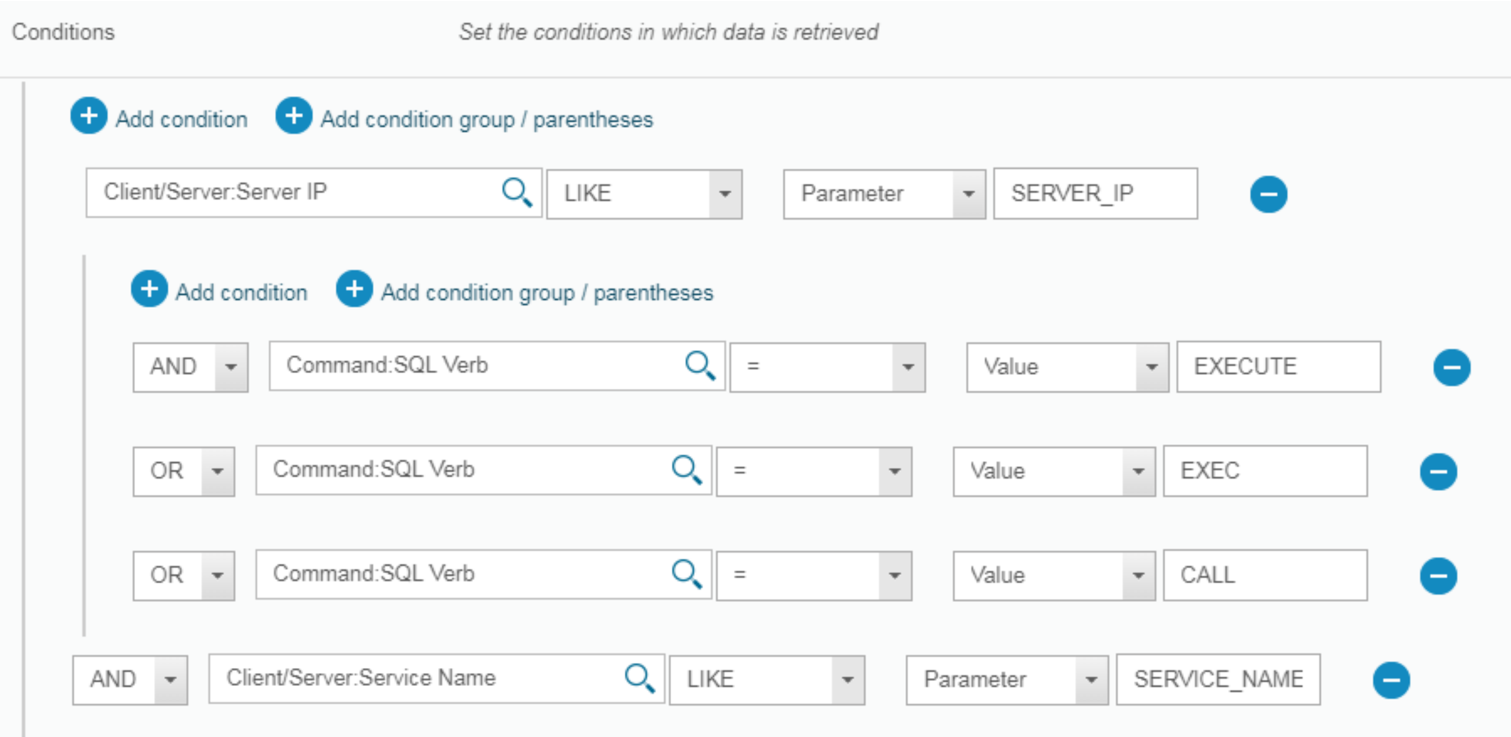


Conditions *Set the conditions in which data is retrieved*

	Command:SQL Verb	LIKE	Parameter	CommandLike
AND	Object:Object Name	LIKE	Parameter	ObjectNameLike
AND	Client/Server:Server IP	LIKE	Parameter	ServerIPLike

SQL Verb like CommandLike AND Object Name like ObjectNameLike AND Server IP like ServerIPLike

Complex Conditions – Condition Group


Add condition
Add condition group / parentheses
Add condition
Add condition group / parentheses

Conditions *Set the conditions in which data is retrieved*

Client/Server:Server IP LIKE Parameter SERVER_IP

AND Command:SQL Verb = Value EXECUTE

OR Command:SQL Verb = Value EXEC

OR Command:SQL Verb = Value CALL

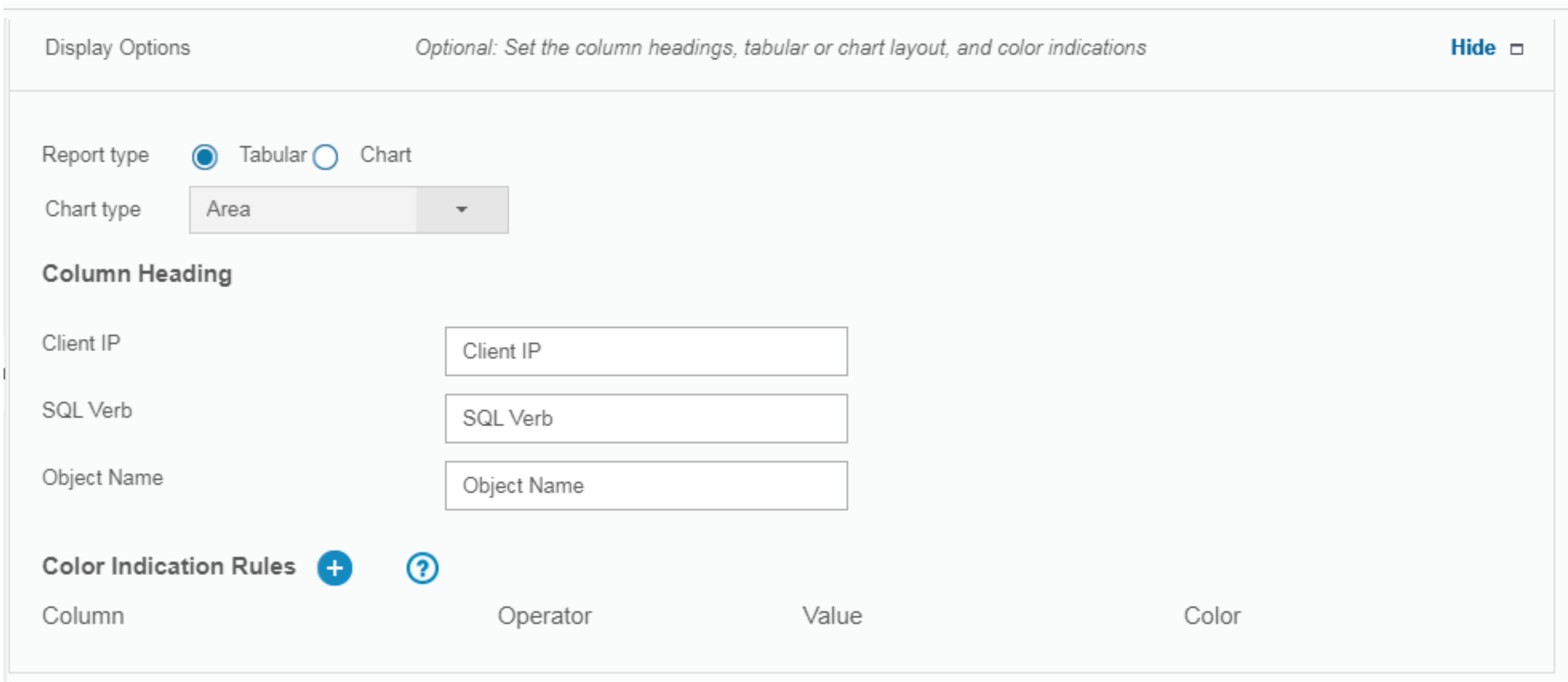
AND Client/Server:Service Name LIKE Parameter SERVICE_NAME

Server IP like SERVER_IP AND (SQL Verb= ‘EXECUTE’ OR SQL Verb = ‘EXEC’ OR SQL Verb = ‘CALL) AND Service Name like SERVICE_NAME

One Query – One Report

- Each query can have only one report
- Queries with multiple reports are duplicated

Display Options – Tabular Report



Display Options *Optional: Set the column headings, tabular or chart layout, and color indications* **Hide** □

Report type ● Tabular ○ Chart

Chart type: Area ▾

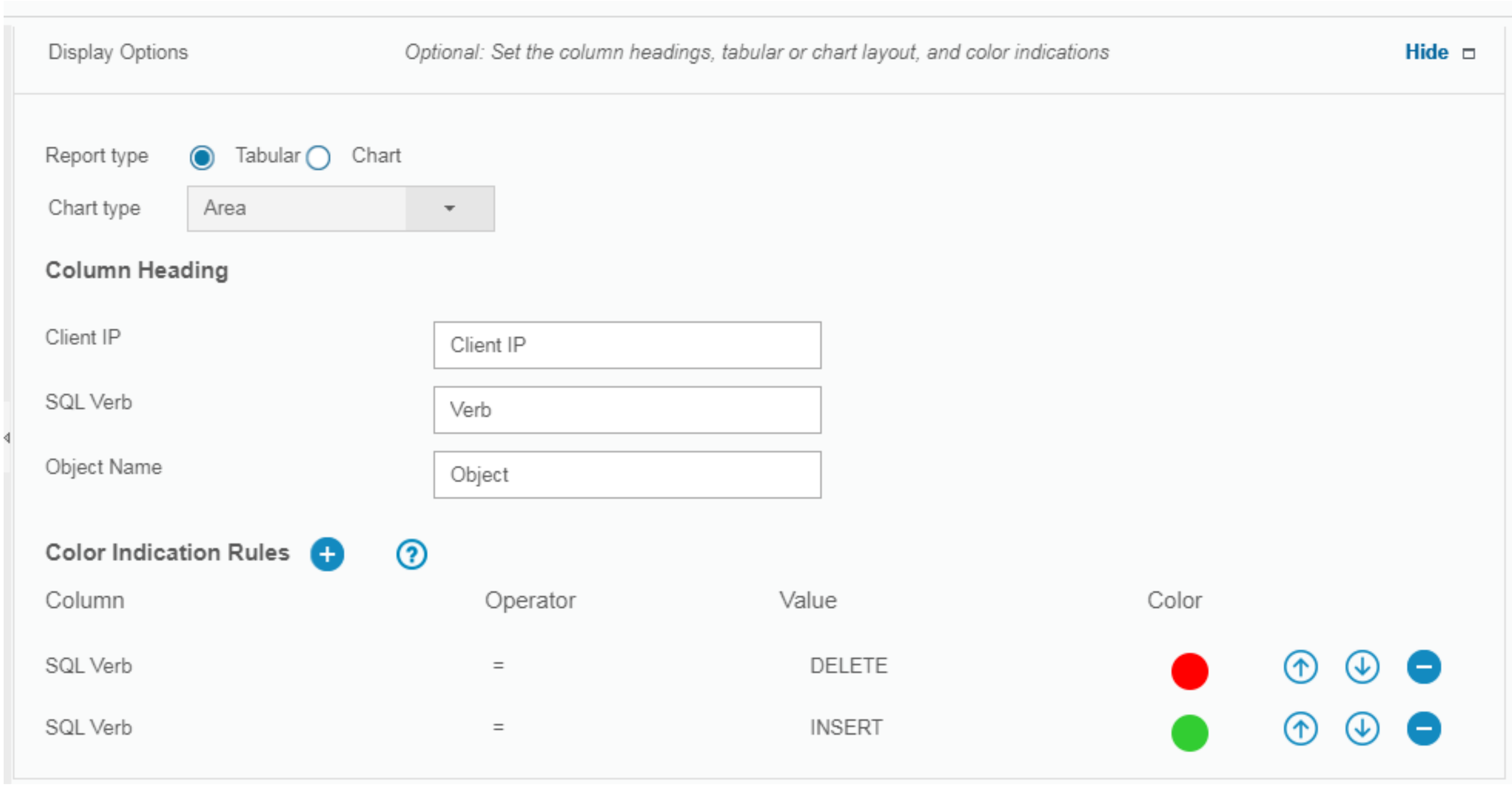
Column Heading

Client IP	Client IP
SQL Verb	SQL Verb
Object Name	Object Name

Color Indication Rules + ?

Column	Operator	Value	Color

Display Options – Tabular Report



Display Options *Optional: Set the column headings, tabular or chart layout, and color indications* **Hide**

Report type ● Tabular ○ Chart

Chart type Area

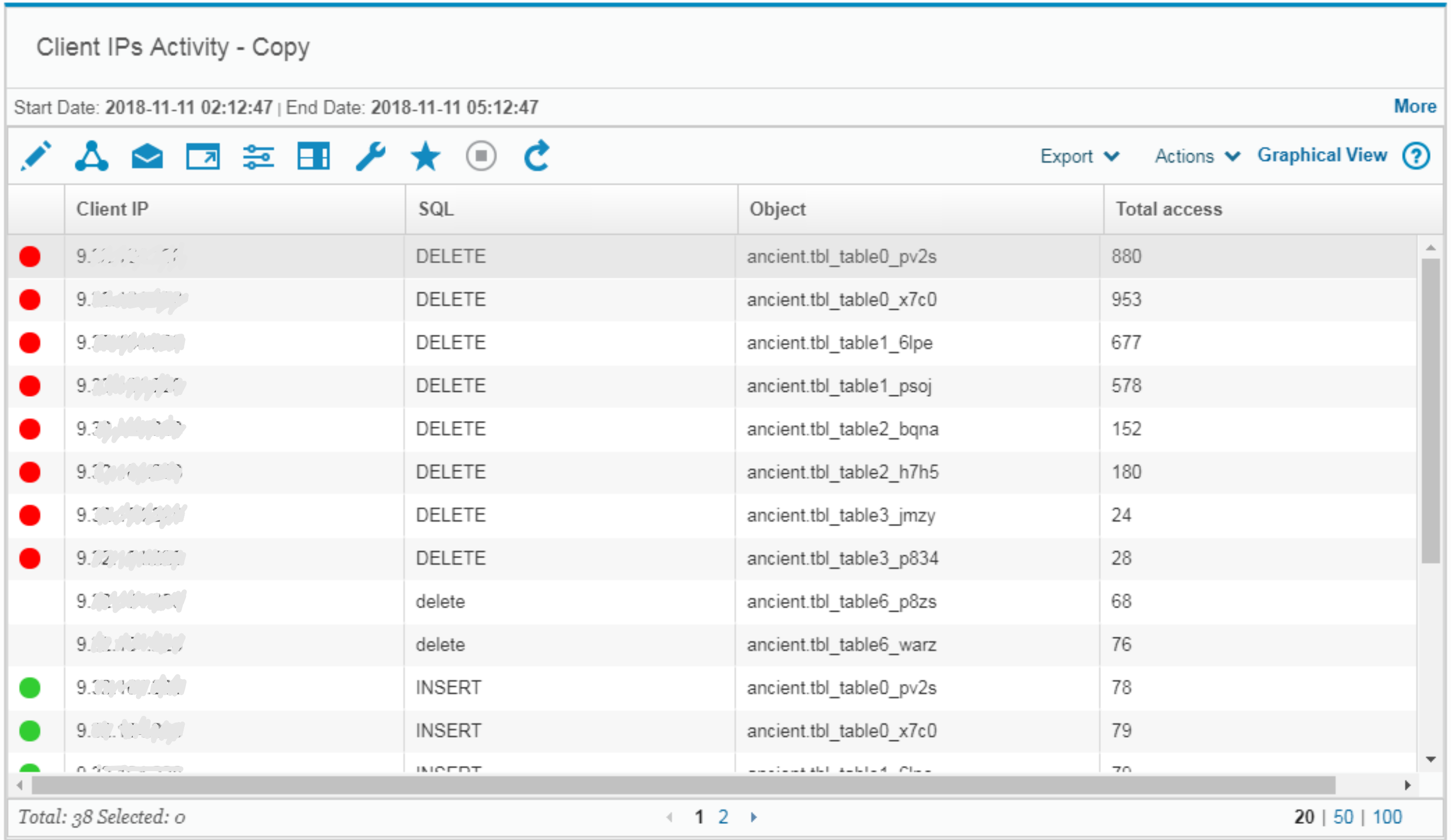
Column Heading

Client IP	Client IP
SQL Verb	Verb
Object Name	Object

Color Indication Rules

Column	Operator	Value	Color
SQL Verb	=	DELETE	🟥
SQL Verb	=	INSERT	🟩

Display Options – Tabular Report



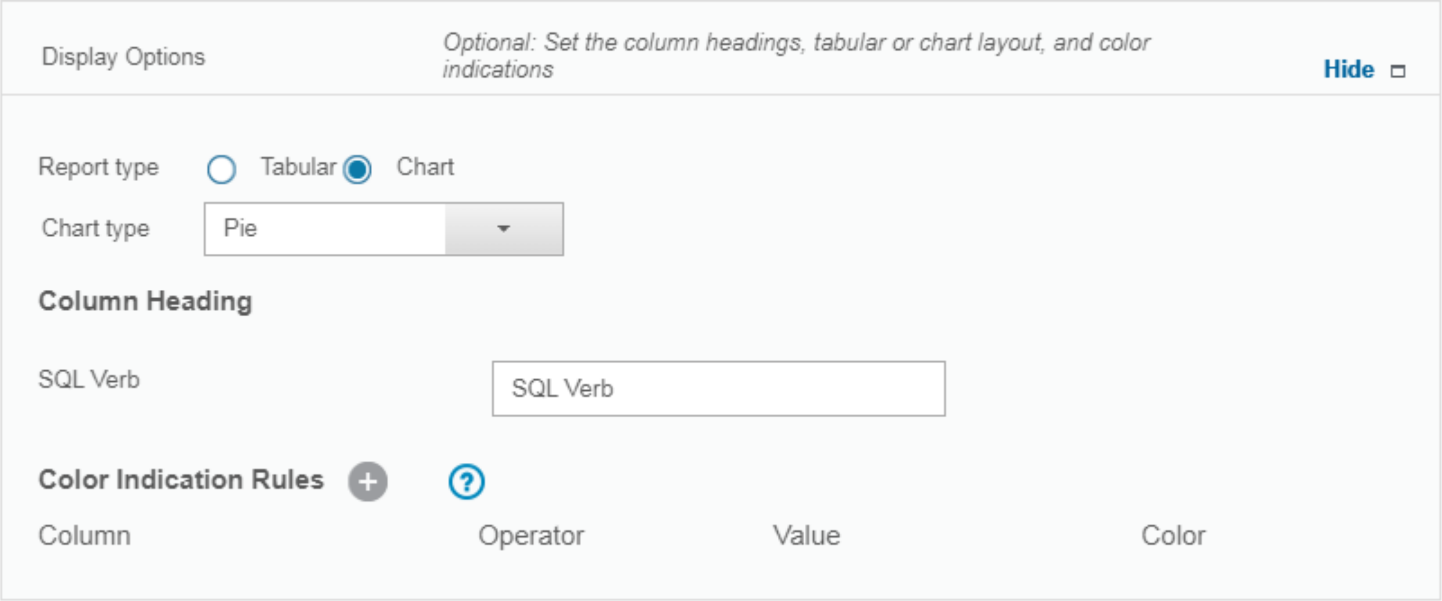
Client IPs Activity - Copy

Start Date: **2018-11-11 02:12:47** | End Date: **2018-11-11 05:12:47**

	Client IP	SQL	Object	Total access
🔴	9.[redacted]	DELETE	ancient.tbl_table0_pv2s	880
🔴	9.[redacted]	DELETE	ancient.tbl_table0_x7c0	953
🔴	9.[redacted]	DELETE	ancient.tbl_table1_6lpe	677
🔴	9.[redacted]	DELETE	ancient.tbl_table1_psoj	578
🔴	9.[redacted]	DELETE	ancient.tbl_table2_bqna	152
🔴	9.[redacted]	DELETE	ancient.tbl_table2_h7h5	180
🔴	9.[redacted]	DELETE	ancient.tbl_table3_jmzy	24
🔴	9.[redacted]	DELETE	ancient.tbl_table3_p834	28
	9.[redacted]	delete	ancient.tbl_table6_p8zs	68
	9.[redacted]	delete	ancient.tbl_table6_warz	76
🟢	9.[redacted]	INSERT	ancient.tbl_table0_pv2s	78
🟢	9.[redacted]	INSERT	ancient.tbl_table0_x7c0	79

Total: 38 Selected: 0

Display Options – Chart



Display Options *Optional: Set the column headings, tabular or chart layout, and color indications*

Report type ○ Tabular ● Chart

Chart type: Pie

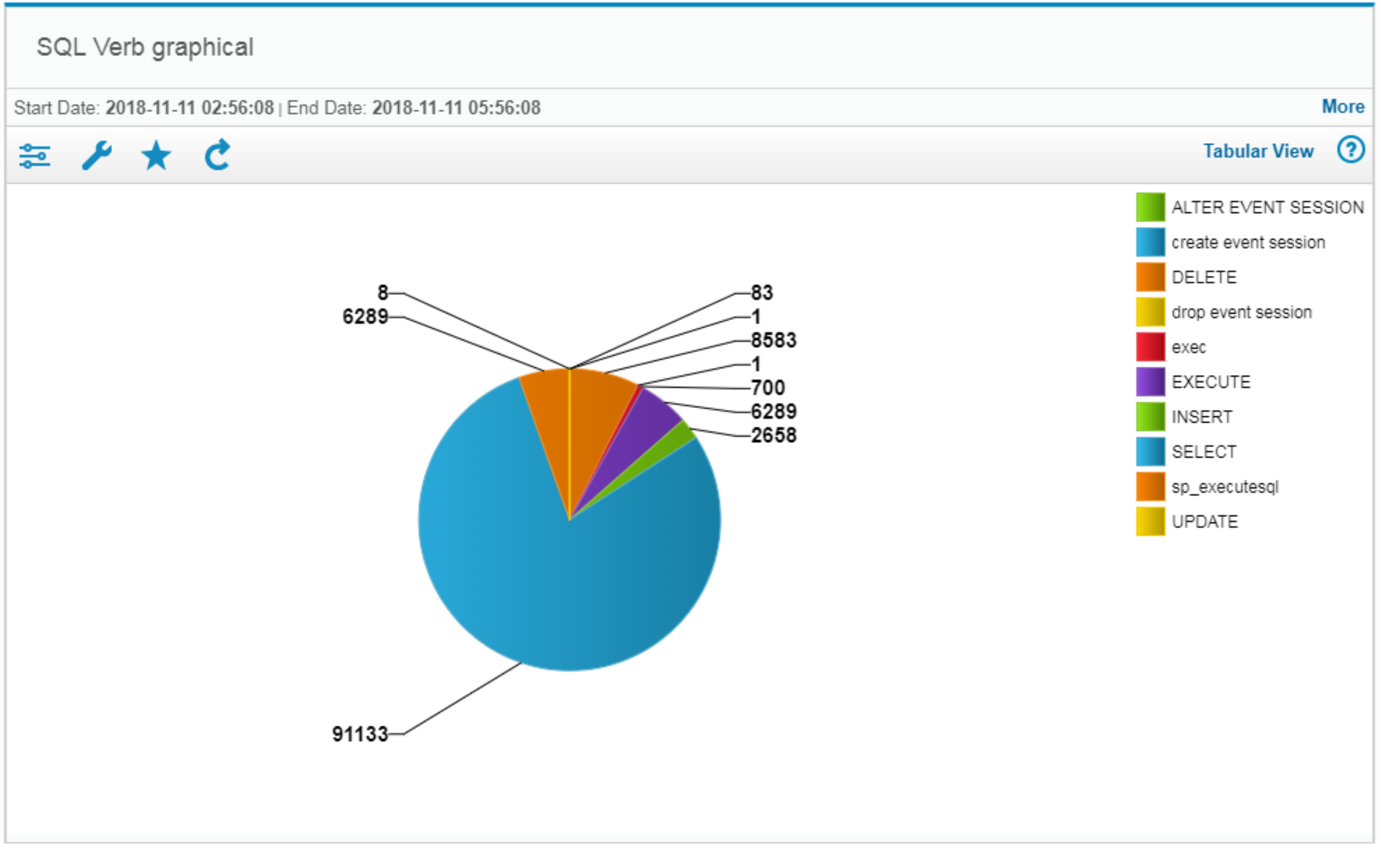
Column Heading

SQL Verb: SQL Verb

Color Indication Rules

Column	Operator	Value	Color

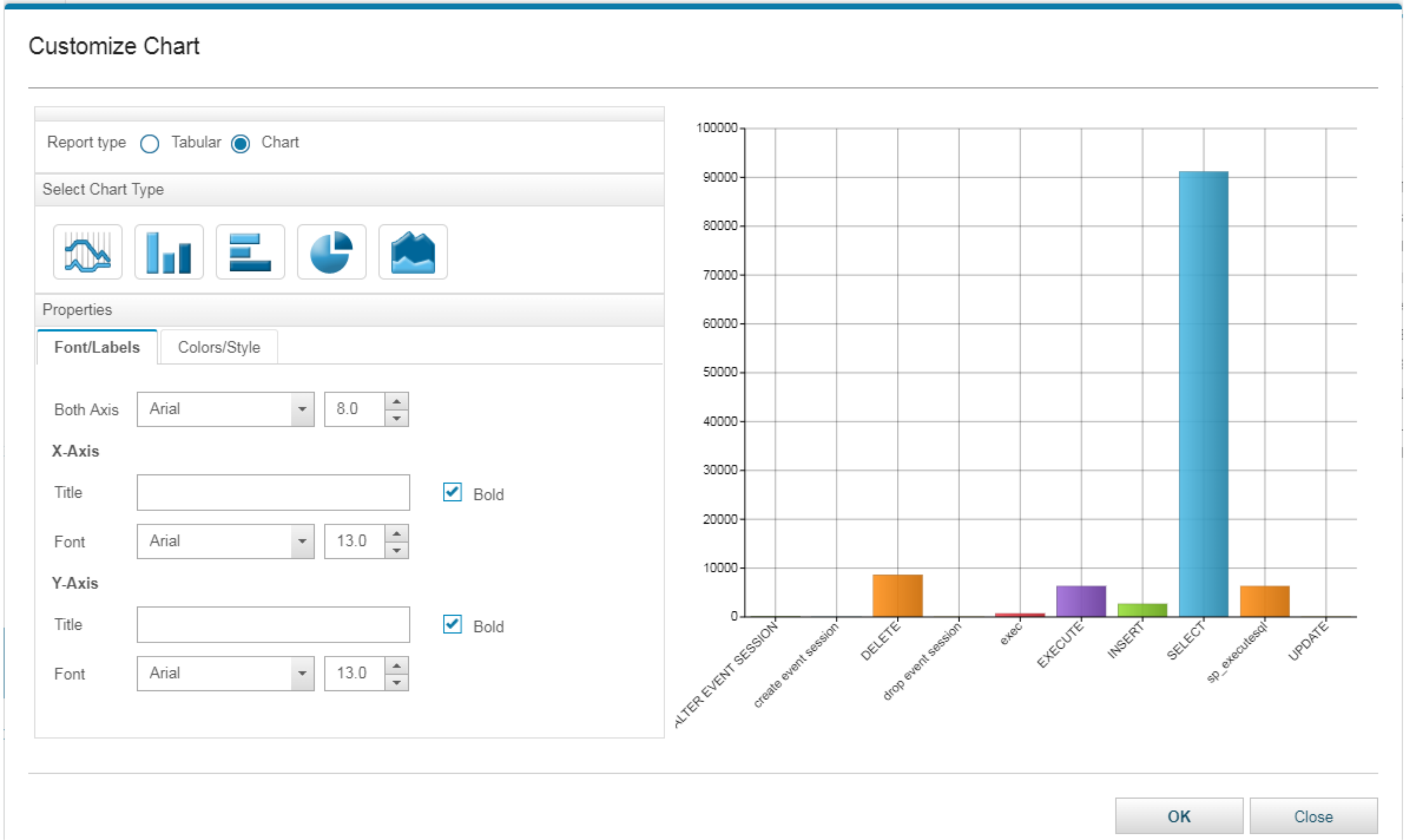
Display Options – Chart



SQL Verb graphical

Start Date: **2018-11-11 02:56:08** | End Date: **2018-11-11 05:56:08**

Display Options – Chart



Customize Chart

Report type ○ Tabular ● Chart

Select Chart Type

Properties

Font/Labels | Colors/Style

Both Axis: Arial 8.0

X-Axis

Title: ☑ Bold

Font: Arial 13.0

Y-Axis

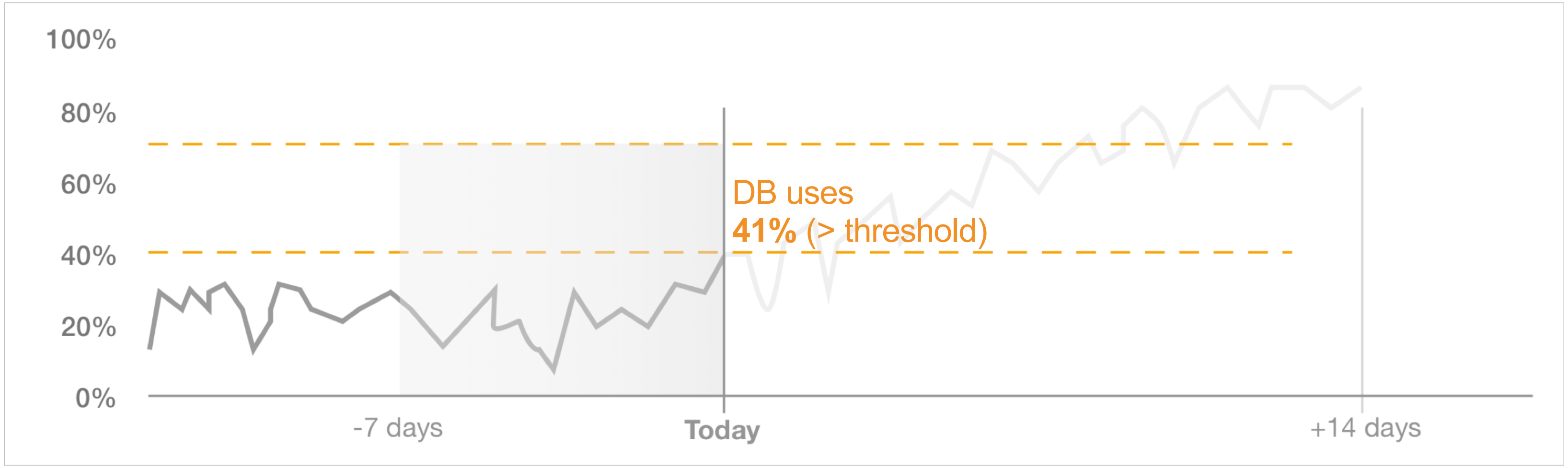
Title: ☑ Bold

Font: Arial 13.0

Disk & DB size alerts

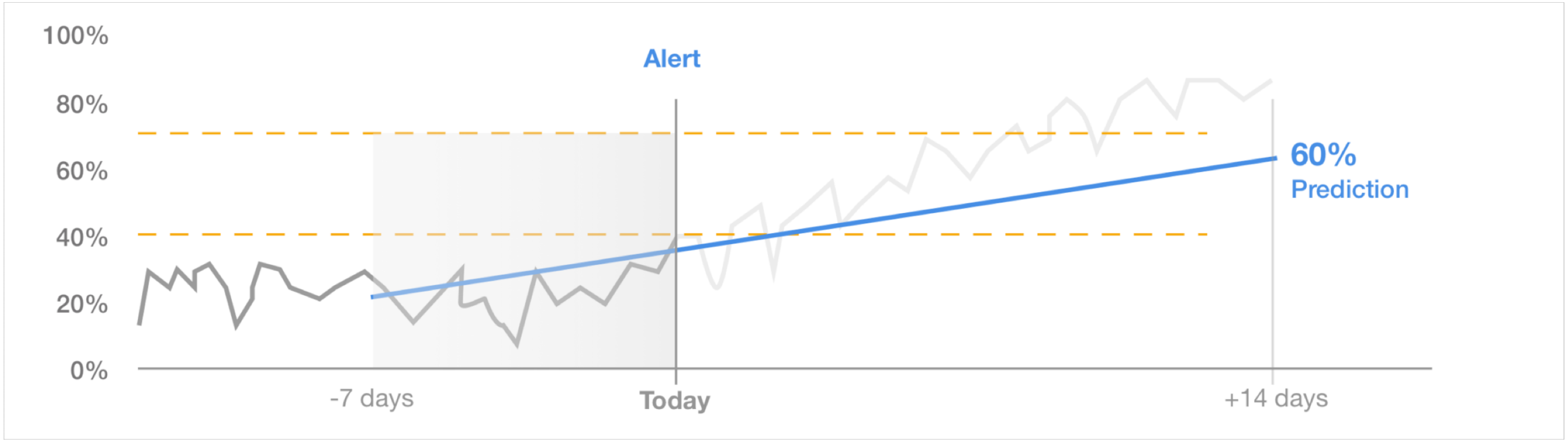
Overview

- Problem: Low disk space can lead to Guardium system failure.
- Solution before Guardium 10.6:
  Alert when disk or database usage > threshold 1 or threshold 2, or create custom correlation alert
  - Severity? Time left to no disk space?



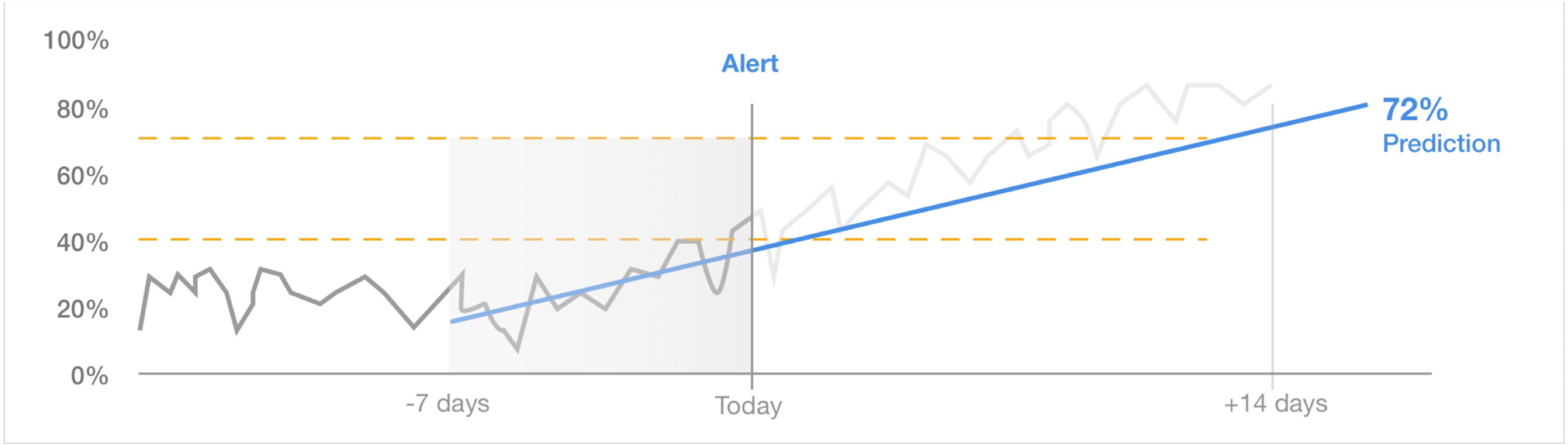
Overview

- New in Guardium 10.6:
  Disk & Database Health Analyzer triggers an alert ahead of time
  if disk usage or database size are expected to reach over 50% within 2 weeks or less.
  - Daily alert; based on statistics from last 7 days.



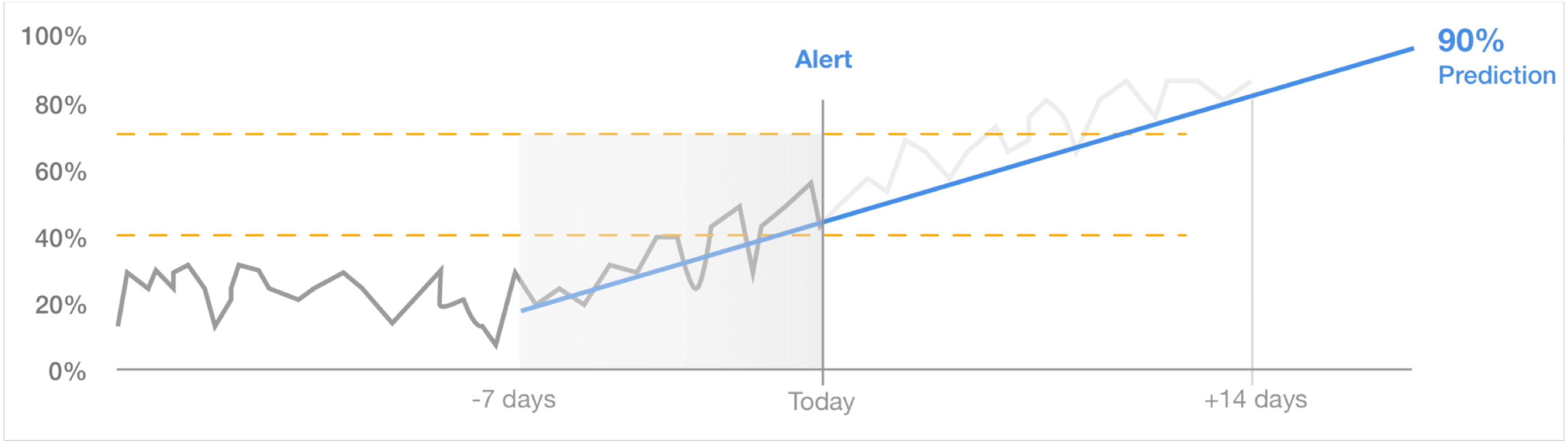
Overview – Description

- If the problem persists, the predicted value will reflect it, the next day:



Overview – Description

- If the problem persists, the predicted value will reflect it, the next day
- Alert details top files or table sizes



Demo: Database size alert (email)

From: DB Size alert

Subject: **Disk is getting full!**

DB size is estimated to exceed 50% of its recommended size in 14 days (reaching 63%), which may lead to space and stability problems.

Top tables:
GDM_EXCEPTION: +11 MB in last 24 hours; current size: 355 MB;
GDM_SESSION: +12 MB in last 24 hours; current size: 200 MB;
GDM_POLICY_VIOLATIONS_LOG: +2 MB in last 24 hours; current size: 5 MB;
…

For causes and actions you can take, see the Technote http://www-01.ibm.com/support/docview.wss?uid=swg21696497.

Demo: Disk space usage alert (email)

From: DB Size alert

Subject: **Disk is getting full!**

Disk space used in /var is estimated to exceed 50% in 14 days (reaching 74%), which may lead to space and stability problems.

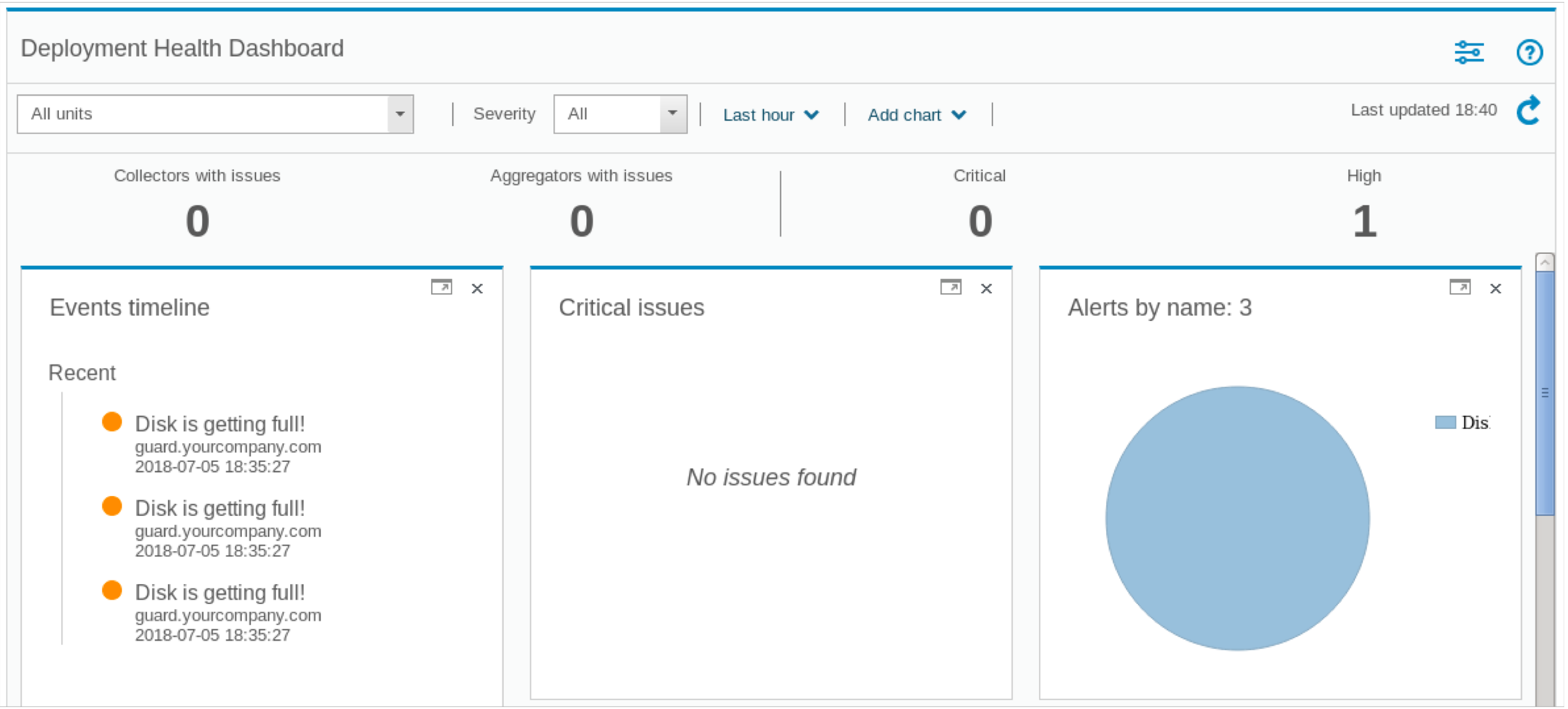
Top files:

2304837875 Wed 25 Jul 2018 … /var/com/IBM/Guardium/…
190474334 Tue 24 Jul 2018 … /var/….log
190474334 Tue 24 Jul 2018 … /var/….log2
…

To find more and delete large files, see the Technote http://www-01.ibm.com/support/docview.wss?uid=swg21995197

Demo: Alerts in Health dashboard

- Health dashboard available on Central manager only.



Deployment Health Dashboard

All units | Severity All | Last hour | Add chart | Last updated 18:40

Collectors with issues	Aggregators with issues	Critical	High
0	0	0	1

Events timeline

Recent

- Disk is getting full! guard.yourcompany.com 2018-07-05 18:35:27
- Disk is getting full! guard.yourcompany.com 2018-07-05 18:35:27
- Disk is getting full! guard.yourcompany.com 2018-07-05 18:35:27

Critical issues

No issues found

Alerts by name: 3

Implementation Considerations – Configuration

- **disable**
  `grdapi disable_health_analyzer`

- **enable** (default)
  `grdapi enable_health_analyzer`

- Get modifiable **params**
  `grdapi get_all_modifiable_guard_params paramlike=health_analyze`
  - HEALTH_ANALYZER_DB_LOOKAHEAD_DAYS (default: 14 [next days])
  - HEALTH_ANALYZER_DB_SAMPLE_DAYS (default: last 7 days)
  - HEALTH_ANALYZER_DB_USAGE_THRESHOLD (default: 50% used)
  - HEALTH_ANALYZER_VAR_LOOKAHEAD_DAYS (default: 14 [next days])
  - HEALTH_ANALYZER_VAR_SAMPLE_DAYS (default: last 7 days)
  - HEALTH_ANALYZER_VAR_USAGE_THRESHOLD (default: 50% used)

- **Get** current value
  `grdapi get_guard_param paramName="HEALTH_ANALYZER_VAR_SAMPLE_DAYS”`

- **Set** value:
  `grdapi modify_guard_param paramName=parameter paramValue=value`

- **It is recommended that you experiment with the values carefully**

IBM Security

What’s new in 10.6 GIM? Feature Overview

IBM

Quick Summary

- Improved interaction for creating new client groups, including import from CSV
- Ability to view installed modules before selecting clients
  - A dialog which displays information cross client which is filterable and refreshable
- Notifying if GIM process is not running on some client
- Bundle action shown in configure clients
  - Provides Overall summary in one section rather than 2 sections for easier skimming and verification
- Displaying status for the module sent for installation/uninstallation
- Ability to generate Guard API across clients vs. only 1 client as in legacy UI

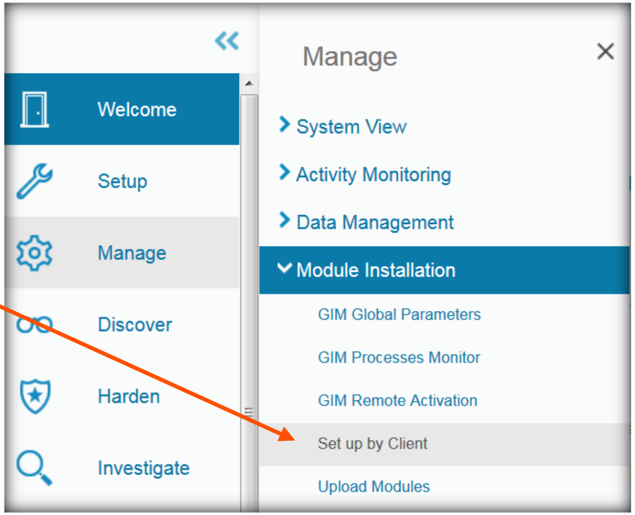
Note: All the enhancements are customer requests/pain points which have been gathered through various customer feedback sessions

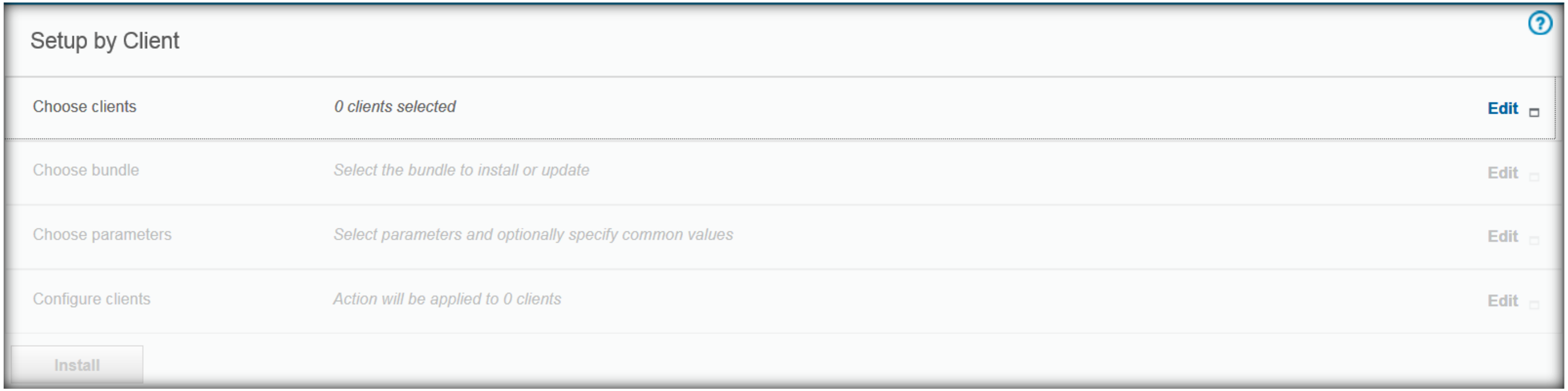
Quick reminder: Where is “Set up by Client”?

- GIM Sections

1. Choose clients
2. Choose bundle
3. Choose parameters
4. Configure clients

Where to find new “Setup by Client” feature?
Manage -> Module Installation -> Set up by Client




Setup by Client

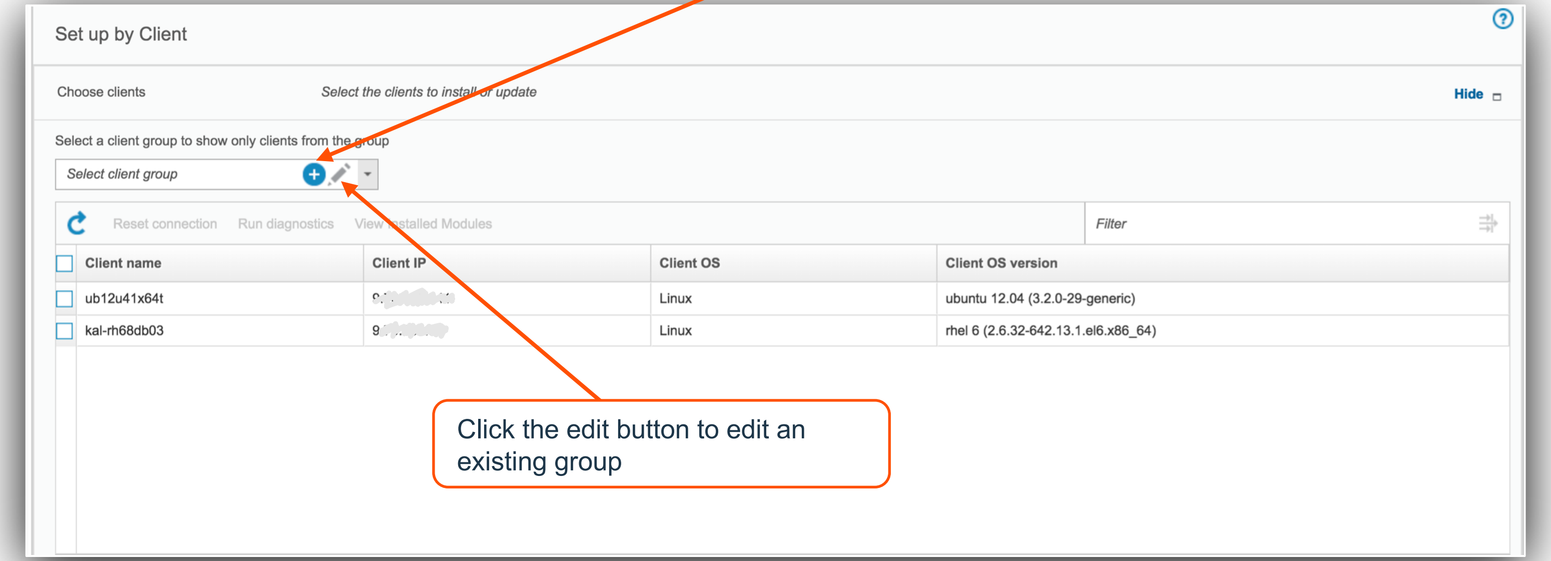
Choose clients	*0 clients selected*	Edit
Choose bundle	*Select the bundle to install or update*	Edit
Choose parameters	*Select parameters and optionally specify common values*	Edit
Configure clients	*Action will be applied to 0 clients*	Edit

GIM Group Builder

GIM Group Builder

- Quick Reminder: How to access GIM Group Builder from setup by client

Click the ‘+’ button to create a new group



Set up by Client

Choose clients — *Select the clients to install or update*

Select a client group to show only clients from the group

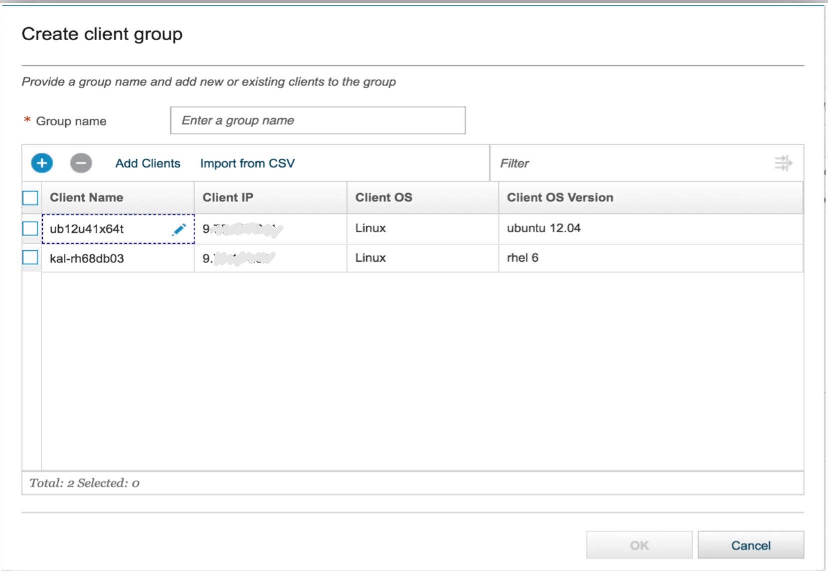
□	Client name	Client IP	Client OS	Client OS version
□	ub12u41x64t	[redacted]	Linux	ubuntu 12.04 (3.2.0-29-generic)
□	kal-rh68db03	[redacted]	Linux	rhel 6 (2.6.32-642.13.1.el6.x86_64)

Click the edit button to edit an existing group

GIM Group Builder

- Shows only the members of the group as compared to 10.5 behavior where it showed all the clients
- It has two new features, Add Clients and Import from CSV
- Through Add Clients, the user gets a list of non member client to select to add to the group
- The Import From CSV enables the user to import members from a CSV file

New UI



Create client group

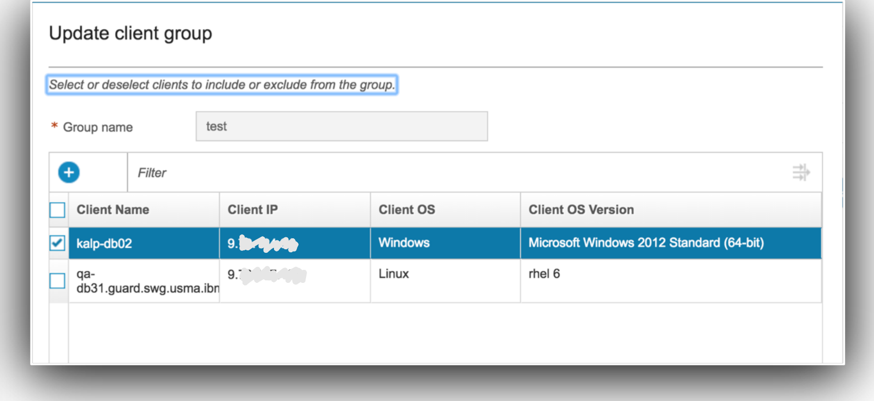
Provide a group name and add new or existing clients to the group

* Group name: *Enter a group name*

□	Client Name	Client IP	Client OS	Client OS Version
□	ub12u41x64t	9.[redacted]	Linux	ubuntu 12.04
□	kal-rh68db03	9.[redacted]	Linux	rhel 6

Total: 2 Selected: 0

10.5 UI



Update client group

Select or deselect clients to include or exclude from the group.

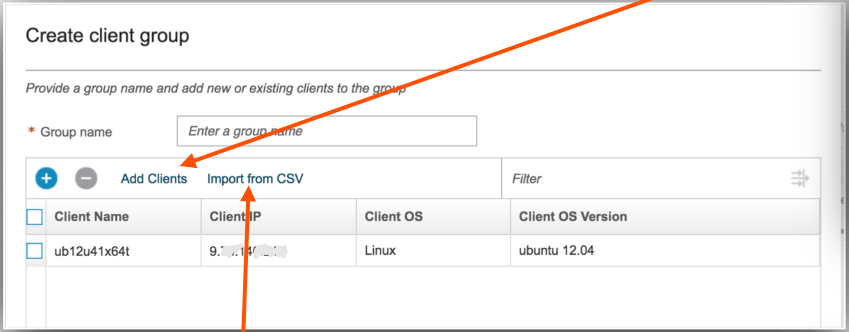
* Group name: test

□	Client Name	Client IP	Client OS	Client OS Version
☑	kalp-db02	9.[redacted]	Windows	Microsoft Windows 2012 Standard (64-bit)
□	qa-db31.guard.swg.usma.ibn	9.[redacted]	Linux	rhel 6

GIM Group Builder

New UI

Shows only the members of the group



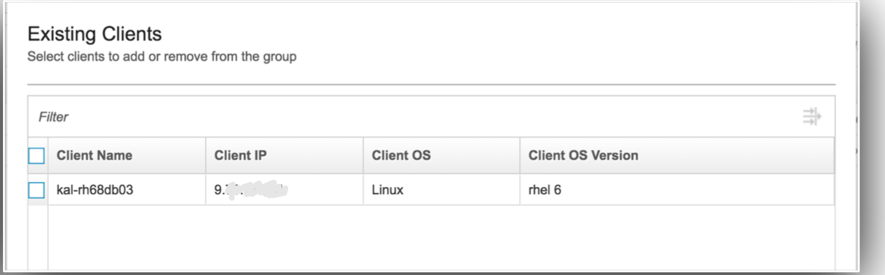
Create client group

Provide a group name and add new or existing clients to the group

* Group name: *Enter a group name*

□	Client Name	Client IP	Client OS	Client OS Version
□	ub12u41x64t	9.[redacted]	Linux	ubuntu 12.04

The “Add Clients” Button displays all the clients which are not part of the group and allows you to add them as a part of the group.



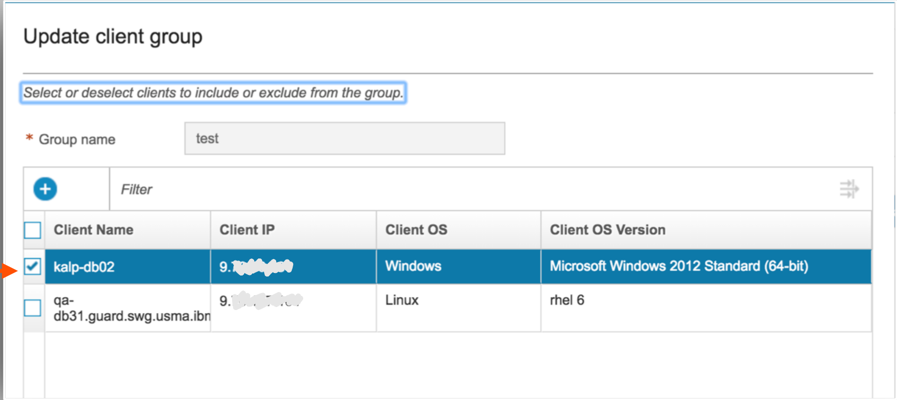
Existing Clients

Select clients to add or remove from the group

□	Client Name	Client IP	Client OS	Client OS Version
□	kal-rh68db03	9.[redacted]	Linux	rhel 6

“Import from CSV” allows you to import group members from a CSV file

10.5 UI



Update client group

Select or deselect clients to include or exclude from the group.

* Group name: test

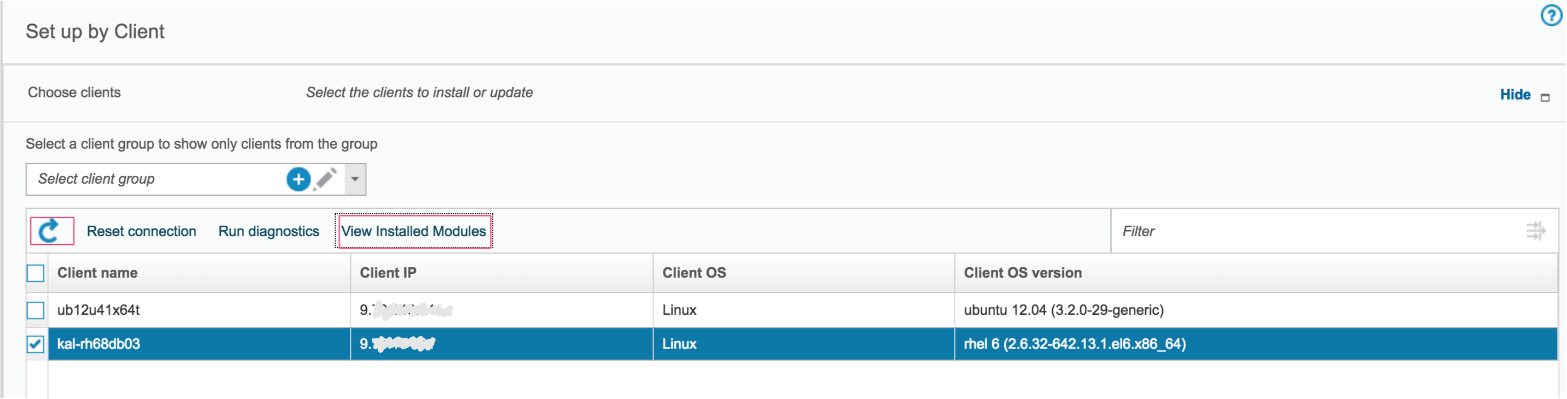
□	Client Name	Client IP	Client OS	Client OS Version
☑	kalp-db02	9.[redacted]	Windows	Microsoft Windows 2012 Standard (64-bit)
□	qa-db31.guard.swg.usma.ibn	9.[redacted]	Linux	rhel 6

10.5 UI showed all the clients and the members were auto selected to distinguish them as members

Choose clients

Choose clients

- ➢ The choose clients section has three new enhancements- the Refresh button, the View installed Modules dialog, and enhanced error checking (displays whether the GIM process is running (or not) on a selected client)
- ➢ The refresh button refreshes the list of clients to get the updated list and thus eliminates the need of refreshing the whole UI
- ➢ The View Installed Modules shows all the installed modules (including stap), their versions and also if some module is in pending state for all the selected clients
- ➢ The View Installed Modules is equivalent to the “i” button in the legacy UI



Set up by Client

Choose clients *Select the clients to install or update* **Hide**

Select a client group to show only clients from the group

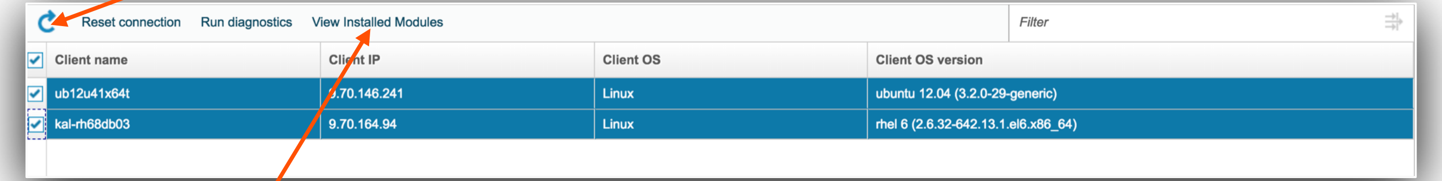
Select client group

☐	Client name	Client IP	Client OS	Client OS version
☐	ub12u41x64t	9.[redacted]	Linux	ubuntu 12.04 (3.2.0-29-generic)
☑	kal-rh68db03	9.[redacted]	Linux	rhel 6 (2.6.32-642.13.1.el6.x86_64)

Choose clients

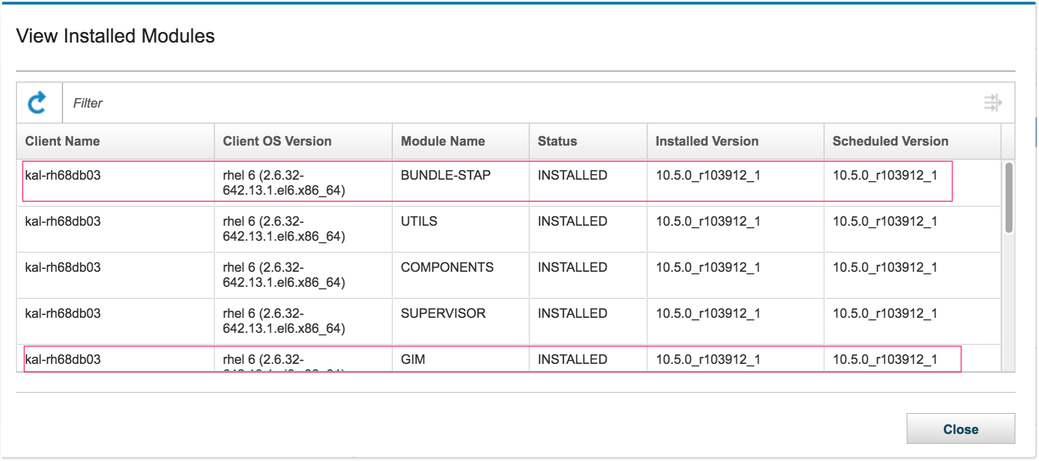
The new refresh button refreshes the list of the clients to show the most recent client list without refreshing the page

New UI



☑	Client name	Client IP	Client OS	Client OS version
☑	ub12u41x64t	9.70.146.241	Linux	ubuntu 12.04 (3.2.0-29-generic)
☑	kal-rh68db03	9.70.164.94	Linux	rhel 6 (2.6.32-642.13.1.el6.x86_64)

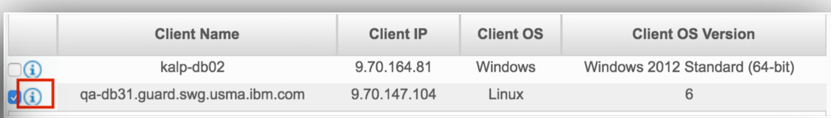
The View Installed Modules displays the information of the installed modules like name, status, version on the selected clients



View Installed Modules

Client Name	Client OS Version	Module Name	Status	Installed Version	Scheduled Version
kal-rh68db03	rhel 6 (2.6.32-642.13.1.el6.x86_64)	BUNDLE-STAP	INSTALLED	10.5.0_r103912_1	10.5.0_r103912_1
kal-rh68db03	rhel 6 (2.6.32-642.13.1.el6.x86_64)	UTILS	INSTALLED	10.5.0_r103912_1	10.5.0_r103912_1
kal-rh68db03	rhel 6 (2.6.32-642.13.1.el6.x86_64)	COMPONENTS	INSTALLED	10.5.0_r103912_1	10.5.0_r103912_1
kal-rh68db03	rhel 6 (2.6.32-642.13.1.el6.x86_64)	SUPERVISOR	INSTALLED	10.5.0_r103912_1	10.5.0_r103912_1
kal-rh68db03	rhel 6 (2.6.32-	GIM	INSTALLED	10.5.0_r103912_1	10.5.0_r103912_1

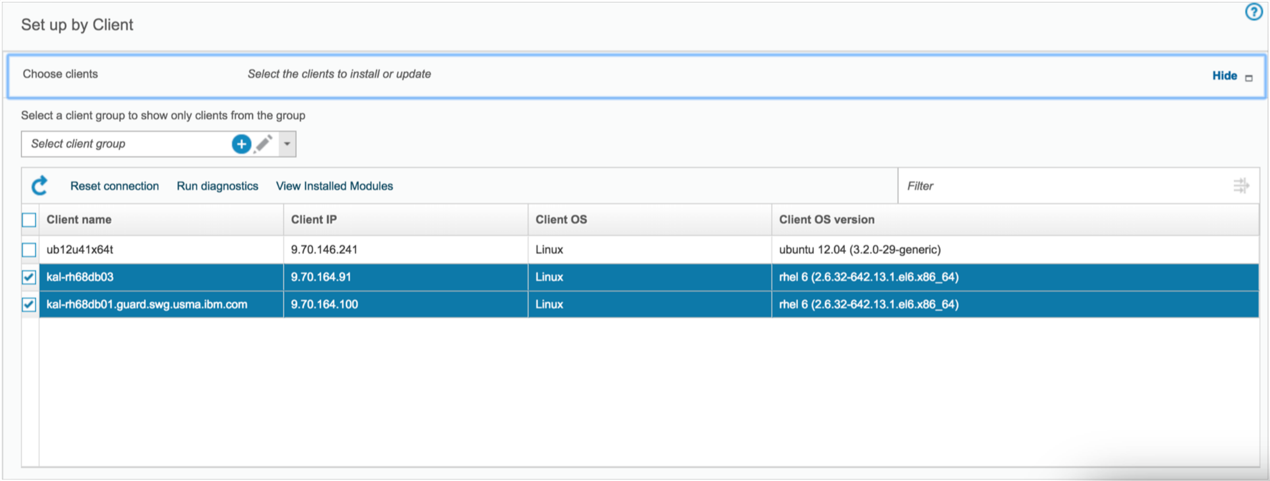
Legacy UI



	Client Name	Client IP	Client OS	Client OS Version
☐ ⓘ	kalp-db02	9.70.164.81	Windows	Windows 2012 Standard (64-bit)
☑ ⓘ	qa-db31.guard.swg.usma.ibm.com	9.70.147.104	Linux	6

Choose Clients

➢ The choose clients screen also notifies the user if GIM process is not running on some selected client



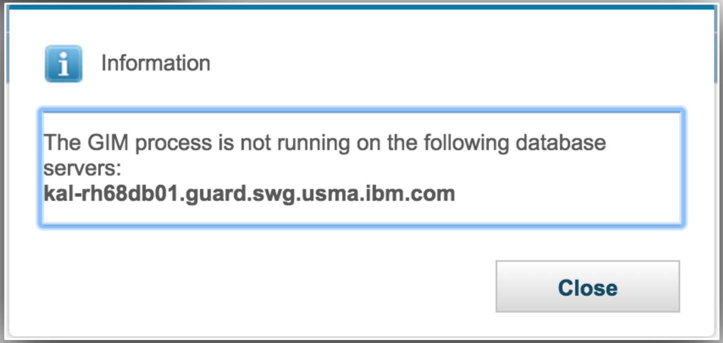
Set up by Client

Choose clients — *Select the clients to install or update*

Select a client group to show only clients from the group

Select client group

	Client name	Client IP	Client OS	Client OS version
□	ub12u41x64t	9.70.146.241	Linux	ubuntu 12.04 (3.2.0-29-generic)
☑	kal-rh68db03	9.70.164.91	Linux	rhel 6 (2.6.32-642.13.1.el6.x86_64)
☑	kal-rh68db01.guard.swg.usma.ibm.com	9.70.164.100	Linux	rhel 6 (2.6.32-642.13.1.el6.x86_64)



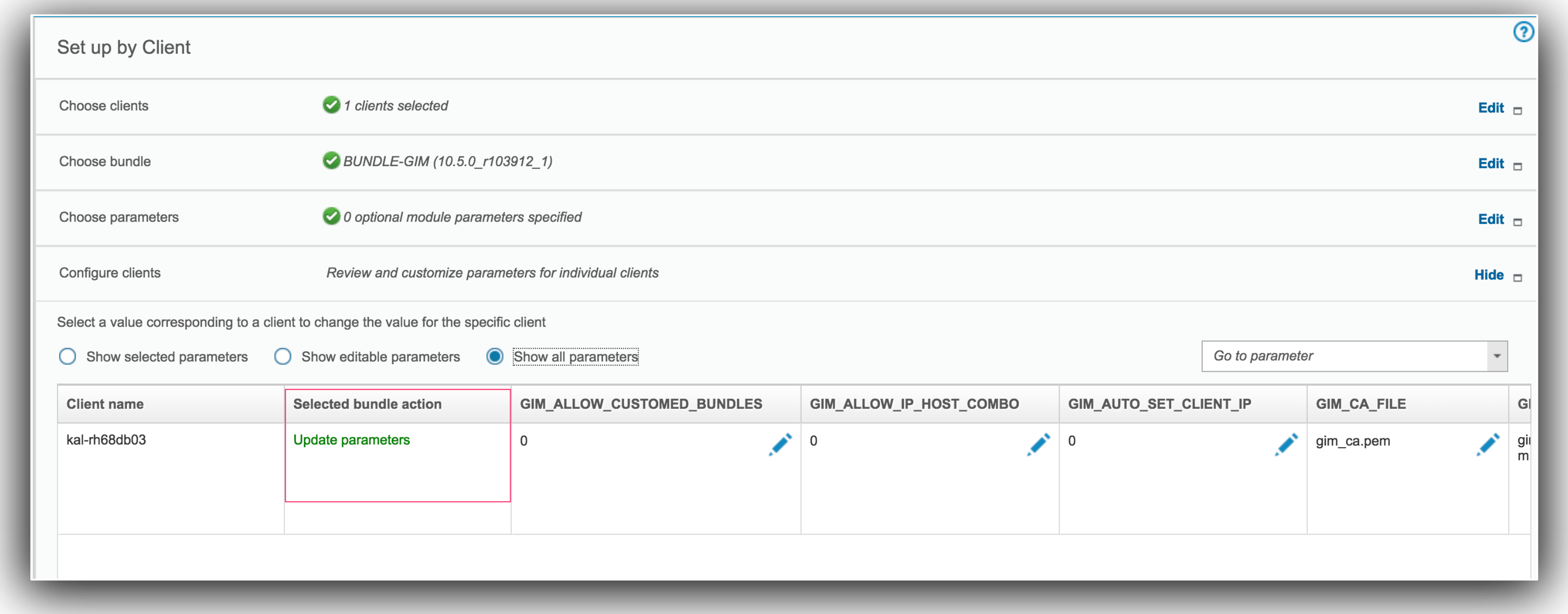
Information

The GIM process is not running on the following database servers:
kal-rh68db01.guard.swg.usma.ibm.com

Configure clients

Configure clients

- The configure clients section now has a new column which displays the bundle action
- This enables the user to see all the important information in one section before performing the install/uninstall action



Set up by Client

Choose clients ✓ *1 clients selected* Edit

Choose bundle ✓ *BUNDLE-GIM (10.5.0_r103912_1)* Edit

Choose parameters ✓ *0 optional module parameters specified* Edit

Configure clients *Review and customize parameters for individual clients* Hide

Select a value corresponding to a client to change the value for the specific client

○ Show selected parameters ○ Show editable parameters ● Show all parameters

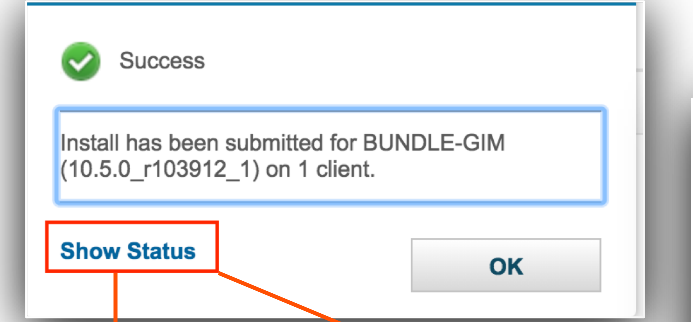
Go to parameter

Client name	Selected bundle action	GIM_ALLOW_CUSTOMED_BUNDLES	GIM_ALLOW_IP_HOST_COMBO	GIM_AUTO_SET_CLIENT_IP	GIM_CA_FILE	GI
kal-rh68db03	Update parameters	0	0	0	gim_ca.pem	gi m

Status Info

Status Info

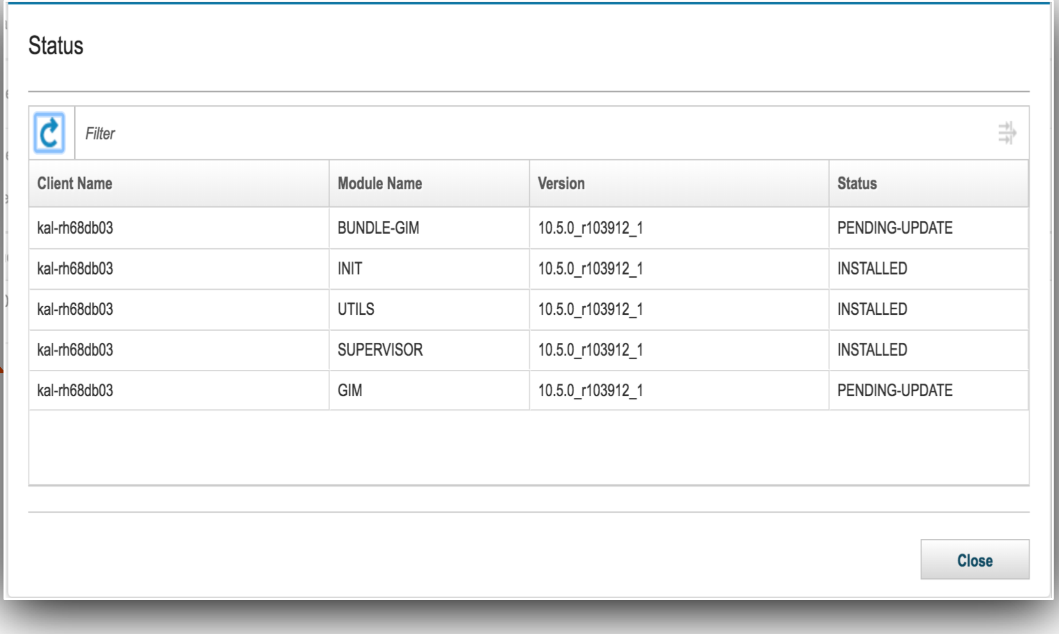
- After submitting the modules for desired action, in the confirmation dialog, we have a link “Show Status” which shows a Status dialog displaying the current state of the submitted module for all the clients



Success

Install has been submitted for BUNDLE-GIM (10.5.0_r103912_1) on 1 client.

After submitting the action, we can see the status of the submitted bundle/module by clicking on this link



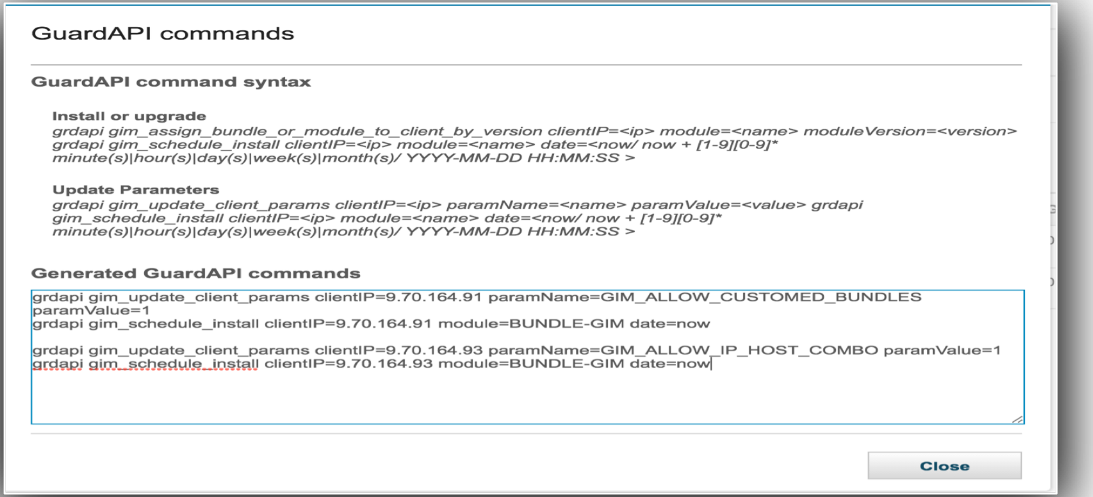
Status

Client Name	Module Name	Version	Status
kal-rh68db03	BUNDLE-GIM	10.5.0_r103912_1	PENDING-UPDATE
kal-rh68db03	INIT	10.5.0_r103912_1	INSTALLED
kal-rh68db03	UTILS	10.5.0_r103912_1	INSTALLED
kal-rh68db03	SUPERVISOR	10.5.0_r103912_1	INSTALLED
kal-rh68db03	GIM	10.5.0_r103912_1	PENDING-UPDATE

Generate GuardAPI

Generate GuardAPI

- The generate GuardAPI button was present in legacy UI but missing from 10.5
- The new and improved GuardAPI button is located next to the install uninstall buttons and is always enabled
- If enough information is not available to generate guard API for clients then it will display templates by default
- If enough information is available it will generate GuardAPI for multiple clients in one single go as compared to legacy UI where it used to generate GuardAPI for one client in one instance



GuardAPI commands

GuardAPI command syntax

Install or upgrade

```
grdapi gim_assign_bundle_or_module_to_client_by_version clientIP=<ip> module=<name> moduleVersion=<version>
grdapi gim_schedule_install clientIP=<ip> module=<name> date=<now/ now + [1-9][0-9]*
minute(s)|hour(s)|day(s)|week(s)|month(s)/ YYYY-MM-DD HH:MM:SS >
```

Update Parameters

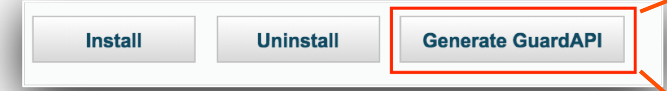
```
grdapi gim_update_client_params clientIP=<ip> paramName=<name> paramValue=<value> grdapi
gim_schedule_install clientIP=<ip> module=<name> date=<now/ now + [1-9][0-9]*
minute(s)|hour(s)|day(s)|week(s)|month(s)/ YYYY-MM-DD HH:MM:SS >
```

Generated GuardAPI commands

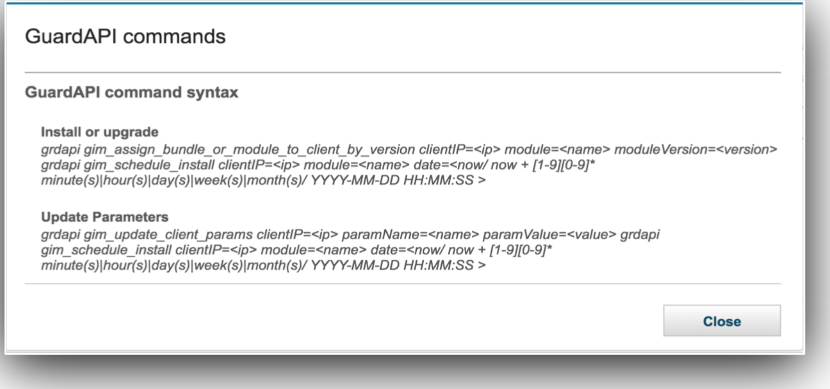
```
grdapi gim_update_client_params clientIP=9.70.164.91 paramName=GIM_ALLOW_CUSTOMED_BUNDLES
paramValue=1
grdapi gim_schedule_install clientIP=9.70.164.91 module=BUNDLE-GIM date=now

grdapi gim_update_client_params clientIP=9.70.164.93 paramName=GIM_ALLOW_IP_HOST_COMBO paramValue=1
grdapi gim_schedule_install clientIP=9.70.164.93 module=BUNDLE-GIM date=now
```

Generate GuardAPI

New UI



If enough information is not available then it will display only template



GuardAPI commands

GuardAPI command syntax

Install or upgrade

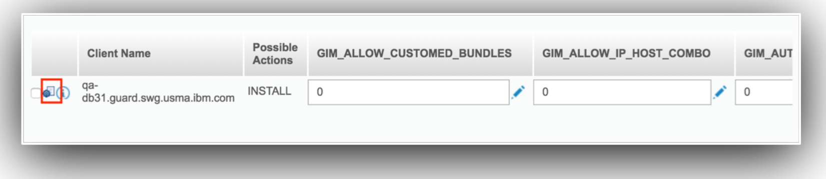
grdapi gim_assign_bundle_or_module_to_client_by_version clientIP=<ip> module=<name> moduleVersion=<version>
*grdapi gim_schedule_install clientIP=<ip> module=<name> date=<now/ now + [1-9][0-9]**
minute(s)|hour(s)|day(s)|week(s)|month(s)/ YYYY-MM-DD HH:MM:SS >

Update Parameters

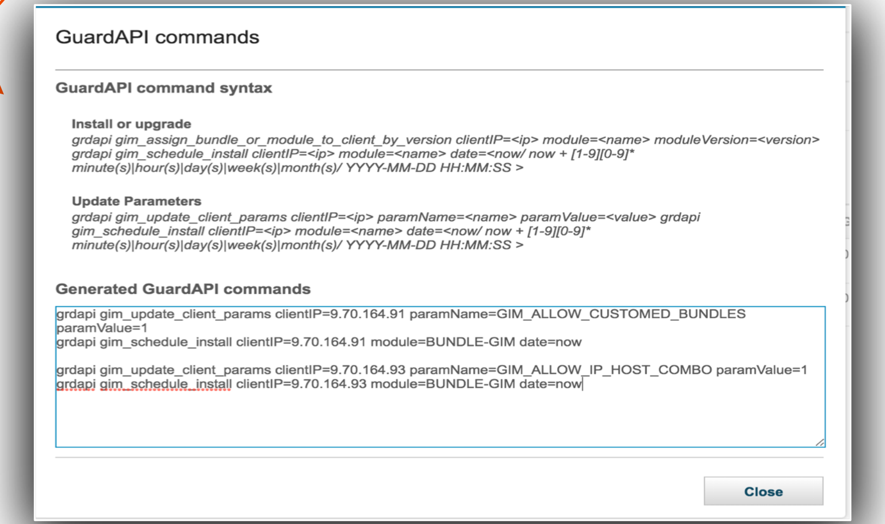
grdapi gim_update_client_params clientIP=<ip> paramName=<name> paramValue=<value> grdapi
*gim_schedule_install clientIP=<ip> module=<name> date=<now/ now + [1-9][0-9]**
minute(s)|hour(s)|day(s)|week(s)|month(s)/ YYYY-MM-DD HH:MM:SS >

If enough information is available then it will display the GuardAPI

Legacy UI



	Client Name	Possible Actions	GIM_ALLOW_CUSTOMED_BUNDLES	GIM_ALLOW_IP_HOST_COMBO	GIM_AUT
	qa-db31.guard.swg.usma.ibm.com	INSTALL	0	0	0



GuardAPI commands

GuardAPI command syntax

Install or upgrade

grdapi gim_assign_bundle_or_module_to_client_by_version clientIP=<ip> module=<name> moduleVersion=<version>
*grdapi gim_schedule_install clientIP=<ip> module=<name> date=<now/ now + [1-9][0-9]**
minute(s)|hour(s)|day(s)|week(s)|month(s)/ YYYY-MM-DD HH:MM:SS >

Update Parameters

grdapi gim_update_client_params clientIP=<ip> paramName=<name> paramValue=<value> grdapi
*gim_schedule_install clientIP=<ip> module=<name> date=<now/ now + [1-9][0-9]**
minute(s)|hour(s)|day(s)|week(s)|month(s)/ YYYY-MM-DD HH:MM:SS >

Generated GuardAPI commands

```
grdapi gim_update_client_params clientIP=9.70.164.91 paramName=GIM_ALLOW_CUSTOMED_BUNDLES
paramValue=1
grdapi gim_schedule_install clientIP=9.70.164.91 module=BUNDLE-GIM date=now

grdapi gim_update_client_params clientIP=9.70.164.93 paramName=GIM_ALLOW_IP_HOST_COMBO paramValue=1
grdapi gim_schedule_install clientIP=9.70.164.93 module=BUNDLE-GIM date=now
```

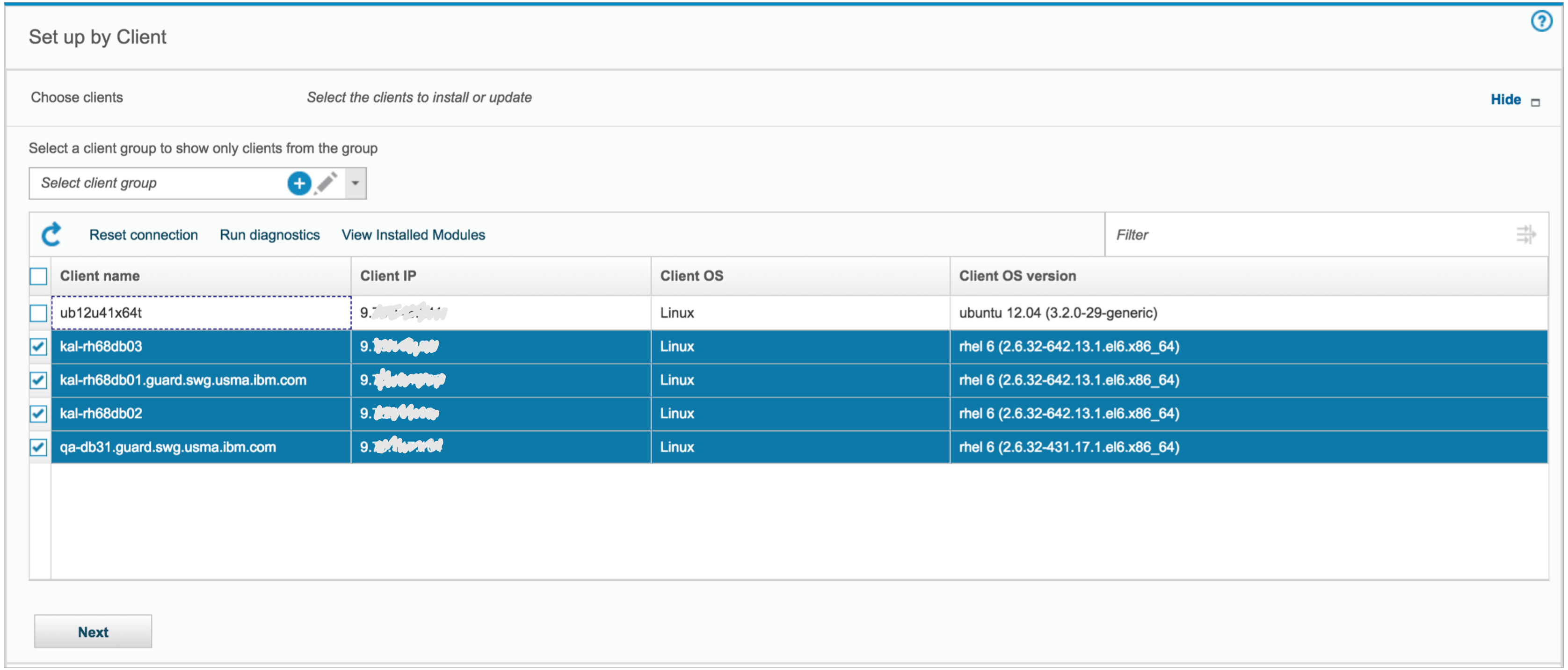
Filtering based impact

Filtering based impact

- This functionality exists in choose bundle section of setup by client
- A common use case is to group clients based on if the impact is an upgrade, changing some parameters, etc. This is supported via our filtering functionality
- Here user can filter clients based on names, modules, bundle action, client OS and other various parameters
- The difference here as compared to filters in other sections is this filter is persistent in the choose bundle section
- For example, if I have total 4 clients, out of which 2 clients have bundle action of install and 2 have upgrade and if we search for upgrade, then the 2 clients clients get filtered out
- So the actions will only be applied to 2 remaining clients
- This is not a new functionality and it existed in 10.5 but from the feedback sessions it was observed that this user-flow/functionality has been unnoticed and it solves one of the customer pain points

Filtering based impact example

Choose Clients Section:



Set up by Client

Choose clients *Select the clients to install or update* **Hide**

Select a client group to show only clients from the group

Select client group

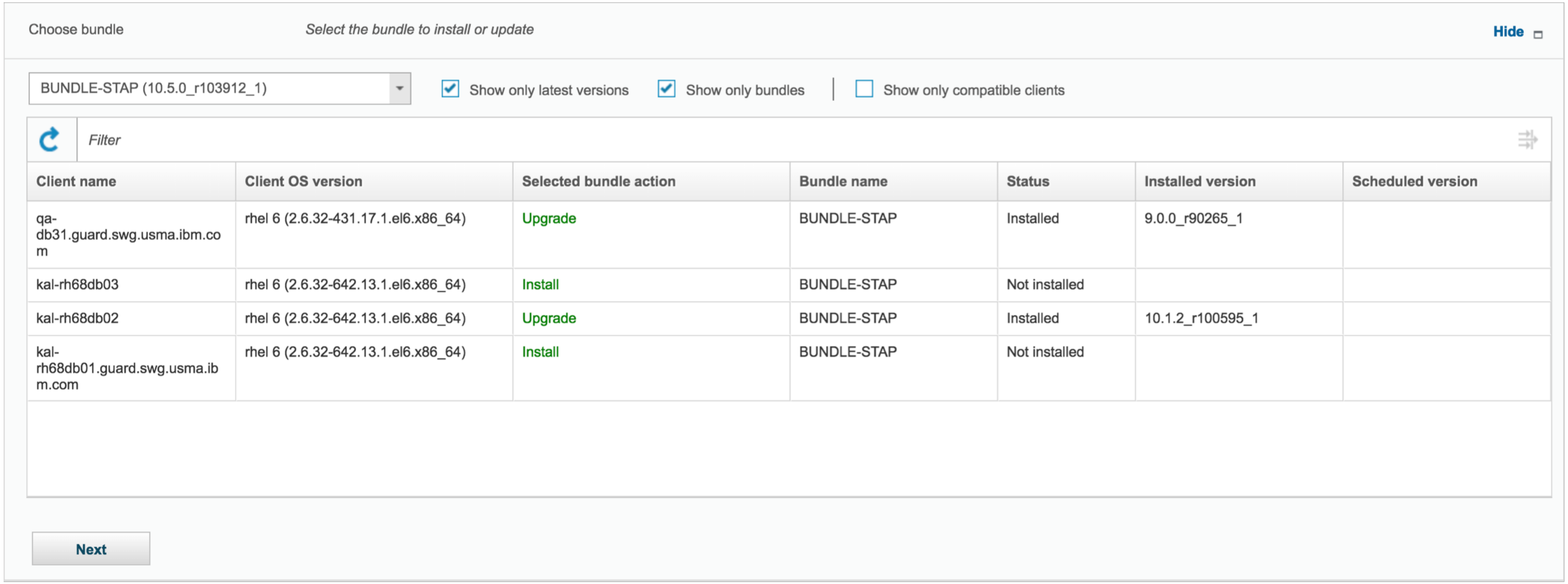
Reset connection Run diagnostics View Installed Modules *Filter*

□	Client name	Client IP	Client OS	Client OS version
□	ub12u41x64t	9.[redacted]	Linux	ubuntu 12.04 (3.2.0-29-generic)
☑	kal-rh68db03	9.[redacted]	Linux	rhel 6 (2.6.32-642.13.1.el6.x86_64)
☑	kal-rh68db01.guard.swg.usma.ibm.com	9.[redacted]	Linux	rhel 6 (2.6.32-642.13.1.el6.x86_64)
☑	kal-rh68db02	9.[redacted]	Linux	rhel 6 (2.6.32-642.13.1.el6.x86_64)
☑	qa-db31.guard.swg.usma.ibm.com	9.[redacted]	Linux	rhel 6 (2.6.32-431.17.1.el6.x86_64)

Next

Filtering based Impact example (continued)

Choose bundle section



Choose bundle *Select the bundle to install or update* Hide

BUNDLE-STAP (10.5.0_r103912_1)

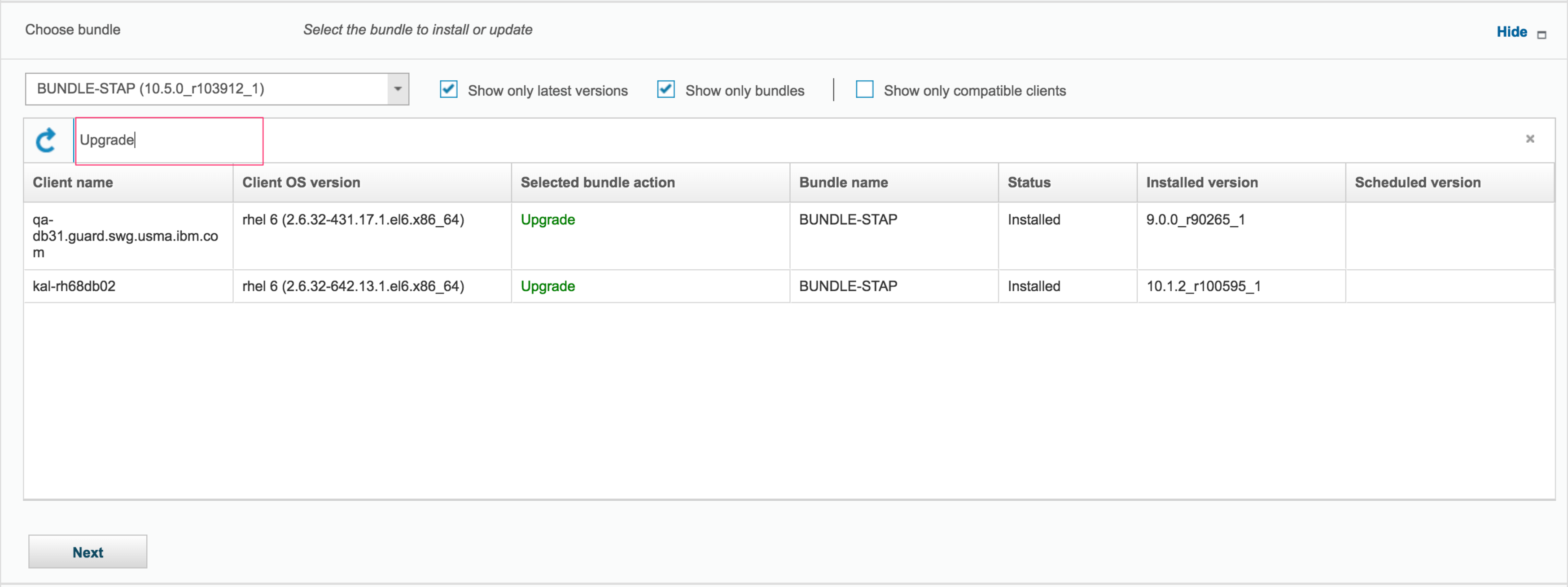
☑ Show only latest versions ☑ Show only bundles | □ Show only compatible clients

Filter

Client name	Client OS version	Selected bundle action	Bundle name	Status	Installed version	Scheduled version
qa-db31.guard.swg.usma.ibm.com	rhel 6 (2.6.32-431.17.1.el6.x86_64)	Upgrade	BUNDLE-STAP	Installed	9.0.0_r90265_1	
kal-rh68db03	rhel 6 (2.6.32-642.13.1.el6.x86_64)	Install	BUNDLE-STAP	Not installed		
kal-rh68db02	rhel 6 (2.6.32-642.13.1.el6.x86_64)	Upgrade	BUNDLE-STAP	Installed	10.1.2_r100595_1	
kal-rh68db01.guard.swg.usma.ibm.com	rhel 6 (2.6.32-642.13.1.el6.x86_64)	Install	BUNDLE-STAP	Not installed		

Filtering based Impact example (continued)

Choose bundle section after applying filter



Choose bundle   *Select the bundle to install or update*   Hide

BUNDLE-STAP (10.5.0_r103912_1)   ☑ Show only latest versions   ☑ Show only bundles   □ Show only compatible clients

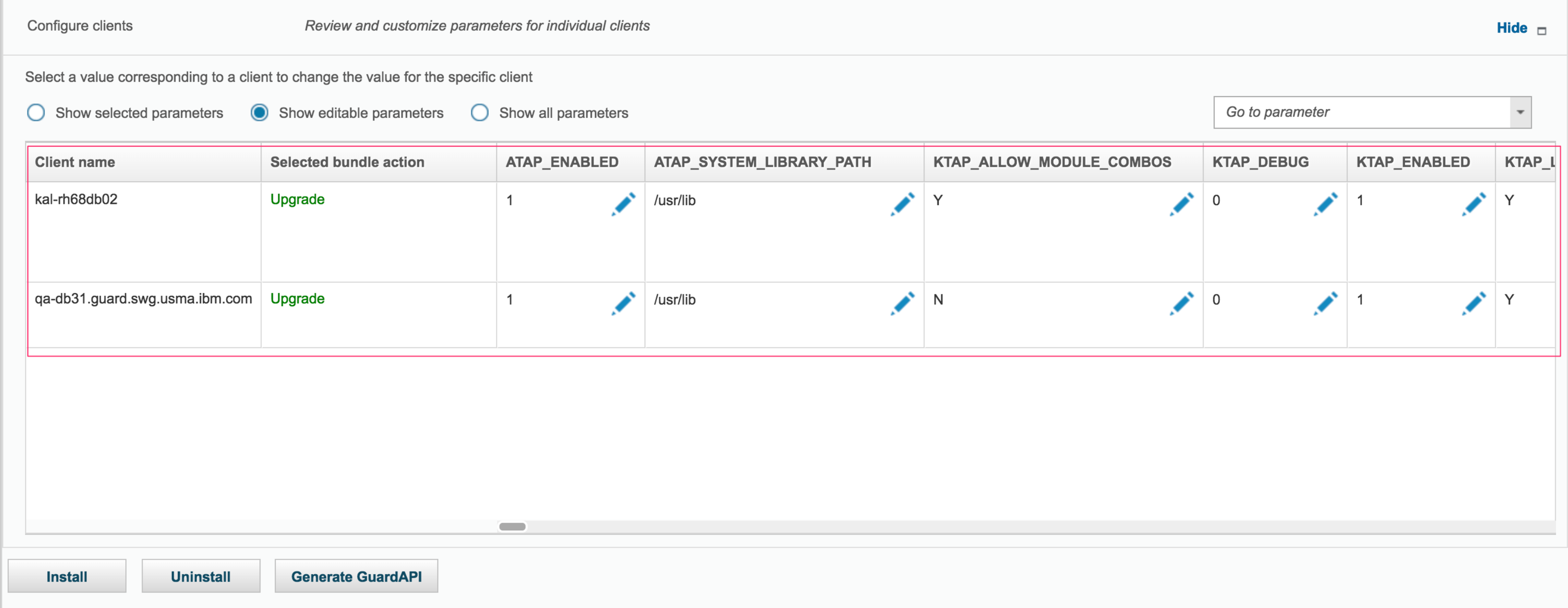
Upgrade

Client name	Client OS version	Selected bundle action	Bundle name	Status	Installed version	Scheduled version
qa-db31.guard.swg.usma.ibm.com	rhel 6 (2.6.32-431.17.1.el6.x86_64)	Upgrade	BUNDLE-STAP	Installed	9.0.0_r90265_1	
kal-rh68db02	rhel 6 (2.6.32-642.13.1.el6.x86_64)	Upgrade	BUNDLE-STAP	Installed	10.1.2_r100595_1	

Filtering based Impact example (continued)

Configure clients screen:

- Only clients with “Upgrade” bundle action persists, the selected action and parameter values will only be applied to these 2 clients even though we selected 4 clients in the choose clients section


Configure clients *Review and customize parameters for individual clients* Hide

Select a value corresponding to a client to change the value for the specific client

○ Show selected parameters ● Show editable parameters ○ Show all parameters

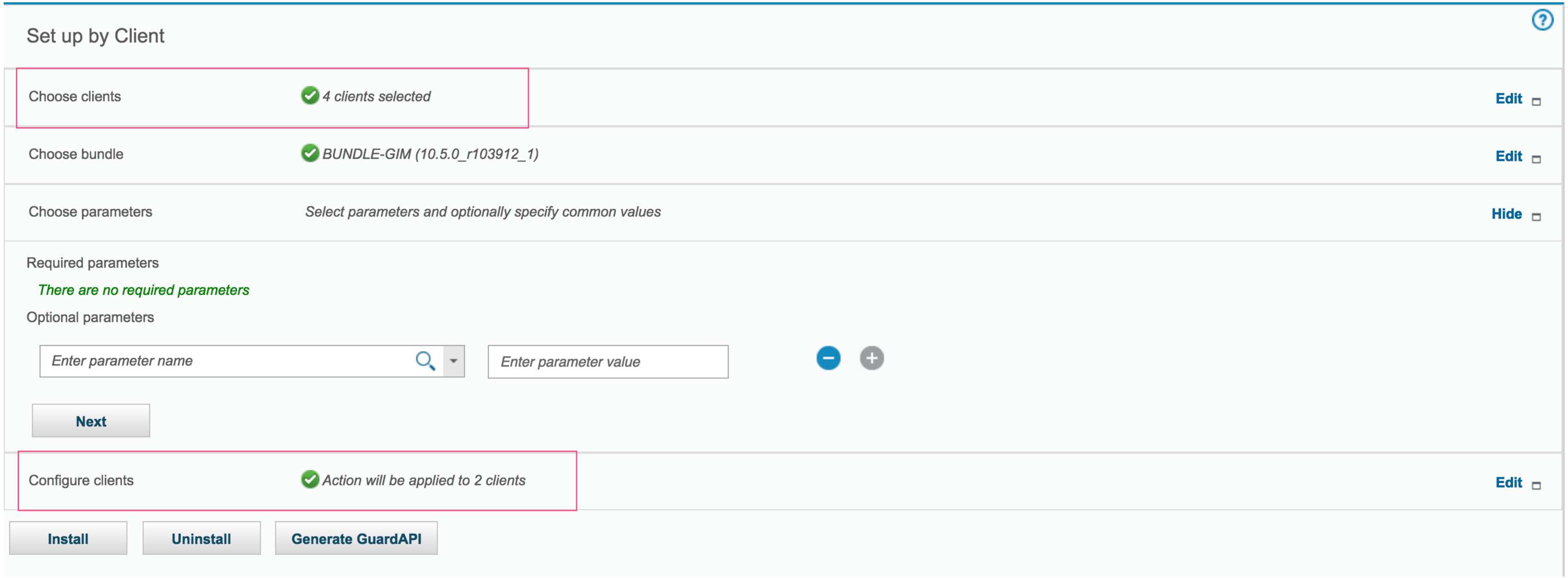
Go to parameter

Client name	Selected bundle action	ATAP_ENABLED	ATAP_SYSTEM_LIBRARY_PATH	KTAP_ALLOW_MODULE_COMBOS	KTAP_DEBUG	KTAP_ENABLED	KTAP_L
kal-rh68db02	Upgrade	1	/usr/lib	Y	0	1	Y
qa-db31.guard.swg.usma.ibm.com	Upgrade	1	/usr/lib	N	0	1	Y

Filtering based Impact example (continued)

Overall summary section:

- We updated the count in the summary section header. So, users can see what the results of the install will be
- When the user has a large amount of clients, the summary can be a great way to do a "sanity" check



Set up by Client

Choose clients ✓ *4 clients selected* **Edit**

Choose bundle ✓ *BUNDLE-GIM (10.5.0_r103912_1)* **Edit**

Choose parameters *Select parameters and optionally specify common values* **Hide**

Required parameters

There are no required parameters

Optional parameters

Enter parameter name | *Enter parameter value*

Next

Configure clients ✓ *Action will be applied to 2 clients* **Edit**

Install **Uninstall** **Generate GuardAPI**

Unix STAP changes for live update

Overview

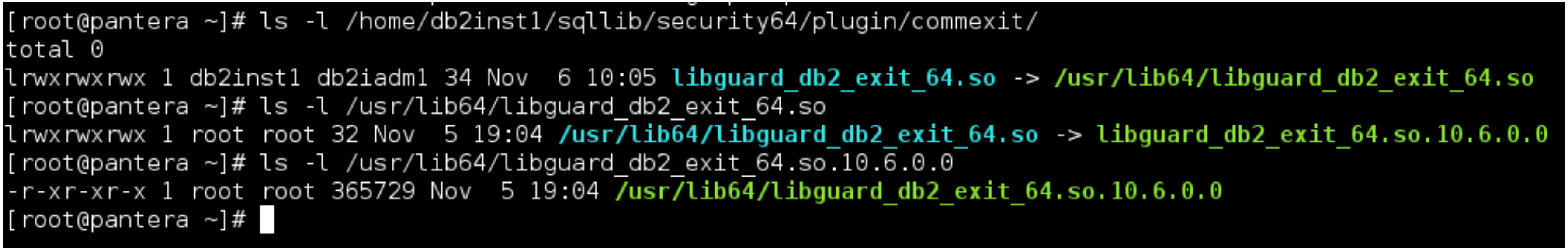
- Customers have employees with separated responsibilities: database administrators, operating system people, Guardium administrators
- Customers have strict database “maintenance windows”
- This feature allows the upgrade of Guardium S-TAP while leaving databases running
- No loss of functionality or of data during S-TAP upgrade
- S-TAP upgrades can be done at any time – so no reason to NOT run latest S-TAP

Changes in Operation – S-TAP version numbering

- S-TAP version numbers now have 4 numbers
- e.g. 10.6.0.0-r123456
- vs. old 10.5.0-r123456
- Collector/snif/etc. versions not affected

Changes in Operation - Installation

- NO CHANGE to installation (.sh, or gim, or rpm)
- New: Guardium shared memory library installed in system library location (e.g. /usr/lib)
- Exit libraries also installed in system library location
- **IMPORTANT:** when configuring an exit, you must **link** to the system library location!
  - Do not copy the file
  - Do not link to the copy in the Guardium install directory
  - Link to the “.so” file (which is itself a link), not to anything else



```
[root@pantera ~]# ls -l /home/db2inst1/sqllib/security64/plugin/commexit/
total 0
lrwxrwxrwx 1 db2inst1 db2iadm1 34 Nov  6 10:05 libguard_db2_exit_64.so -> /usr/lib64/libguard_db2_exit_64.so
[root@pantera ~]# ls -l /usr/lib64/libguard_db2_exit_64.so
lrwxrwxrwx 1 root root 32 Nov  5 19:04 /usr/lib64/libguard_db2_exit_64.so -> libguard_db2_exit_64.so.10.6.0.0
[root@pantera ~]# ls -l /usr/lib64/libguard_db2_exit_64.so.10.6.0.0
-r-xr-xr-x 1 root root 365729 Nov  5 19:04 /usr/lib64/libguard_db2_exit_64.so.10.6.0.0
[root@pantera ~]# 
```

Changes in Operation - Upgrade

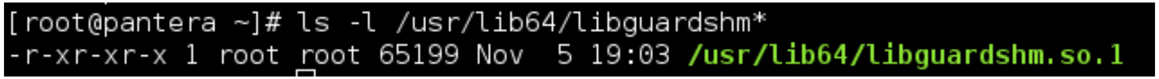
- No change to upgrade (for all methods, .sh / gim / .rpm)
- Databases using exit do NOT need to be stopped, they can continue running
  - Traffic will be captured during upgrade and sent to snif when upgrade complete
  - If there is extremely heavy traffic, some transactions may be dropped
  - After upgrade, monitoring continues using the “old” plugin
  - The next time that database instance restarts it will use the “new” plugin
  - All new instances will use the “new” plugin
  - No time limit to restart – can be months later
- No change at all for other capture methods (K-TAP, A-TAP, pcap)

Limitations

- Only works for EXIT
  - Another reason the EXIT mechanism is preferred over A-TAP
- During the period between S-TAP upgrade and all old database instances being restarted, there can be two sets of shared memory in use (so more memory consumed)
  - Only if shared memory layout changes
  - Returns to normal automatically when all old instances are shut down
- **Only shows benefit AFTER the 10.6.0.0 release!**
  - **Updating from anything before 10.6 is done the old way**

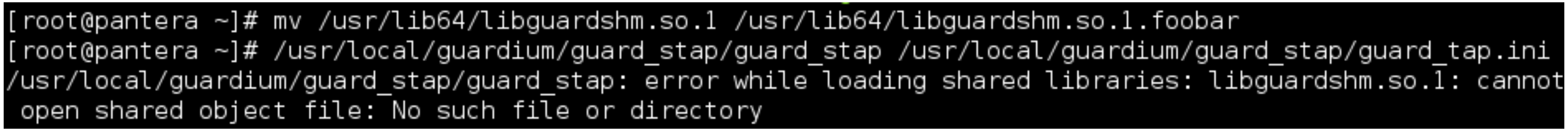
Troubleshooting

- New shared memory library in system library location



```
[root@pantera ~]# ls -l /usr/lib64/libguardshm*
-r-xr-xr-x 1 root root 65199 Nov  5 19:03 /usr/lib64/libguardshm.so.1
```

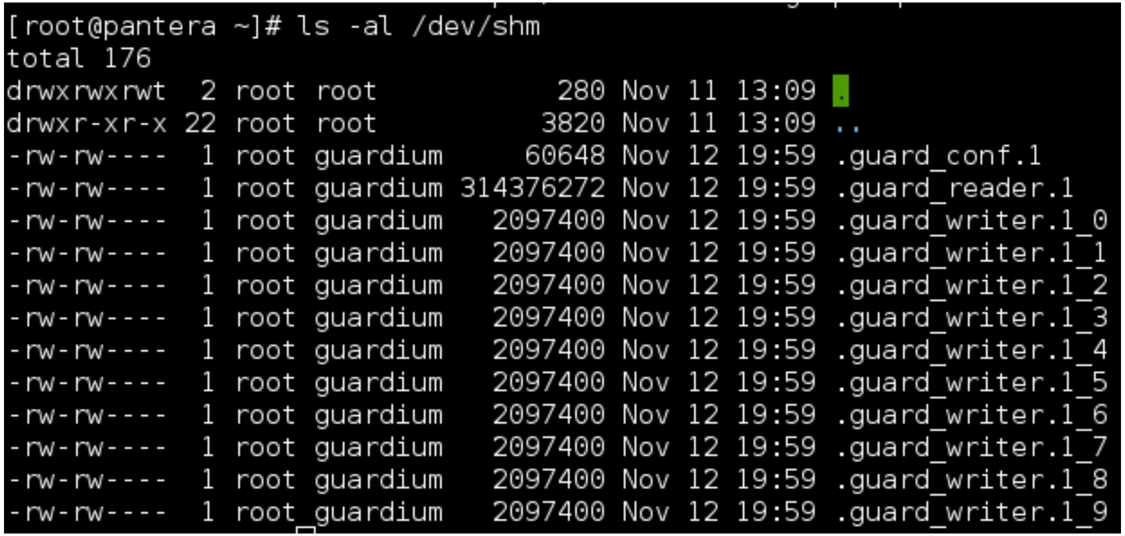
- If removed, missing, etc. S-TAP will not run!



```
[root@pantera ~]# mv /usr/lib64/libguardshm.so.1 /usr/lib64/libguardshm.so.1.foobar
[root@pantera ~]# /usr/local/guardium/guard_stap/guard_stap /usr/local/guardium/guard_stap/guard_tap.ini
/usr/local/guardium/guard_stap/guard_stap: error while loading shared libraries: libguardshm.so.1: cannot
 open shared object file: No such file or directory
```

Troubleshooting 2

- On many platforms you can list shared memory “files”



```
[root@pantera ~]# ls -al /dev/shm
total 176
drwxrwxrwt  2 root  root           280 Nov 11 13:09 .
drwxr-xr-x 22 root  root          3820 Nov 11 13:09 ..
-rw-rw----  1 root  guardium     60648 Nov 12 19:59 .guard_conf.1
-rw-rw----  1 root  guardium 314376272 Nov 12 19:59 .guard_reader.1
-rw-rw----  1 root  guardium   2097400 Nov 12 19:59 .guard_writer.1_0
-rw-rw----  1 root  guardium   2097400 Nov 12 19:59 .guard_writer.1_1
-rw-rw----  1 root  guardium   2097400 Nov 12 19:59 .guard_writer.1_2
-rw-rw----  1 root  guardium   2097400 Nov 12 19:59 .guard_writer.1_3
-rw-rw----  1 root  guardium   2097400 Nov 12 19:59 .guard_writer.1_4
-rw-rw----  1 root  guardium   2097400 Nov 12 19:59 .guard_writer.1_5
-rw-rw----  1 root  guardium   2097400 Nov 12 19:59 .guard_writer.1_6
-rw-rw----  1 root  guardium   2097400 Nov 12 19:59 .guard_writer.1_7
-rw-rw----  1 root  guardium   2097400 Nov 12 19:59 .guard_writer.1_8
-rw-rw----  1 root  guardium   2097400 Nov 12 19:59 .guard_writer.1_9
```

Unix STAP general changes

STAP/ ATAP Pain Points

- ATAP issues would require a lot of manual commands to be issued in order to determine if ATAP was successfully installed or not
  - New script implemented atap_must_gather.sh to collect this information automatically
  - Script is called as part of regular guard_diag diagnostics script
- DB2 exit can be incorrectly set up by the customer
  - New script implemented db2_exit_health_check.sh
  - Script is called as part of regular guard_diag diagnostics script
    - Checks to see if DB2 exit is configured from IE
    - Verifies db_install_dir is set correctly
    - Verifies DB2 user group membership
    - Verifies libraries are installed correctly
    - Checks if DB2 is configured correctly to use the library

Pain Points

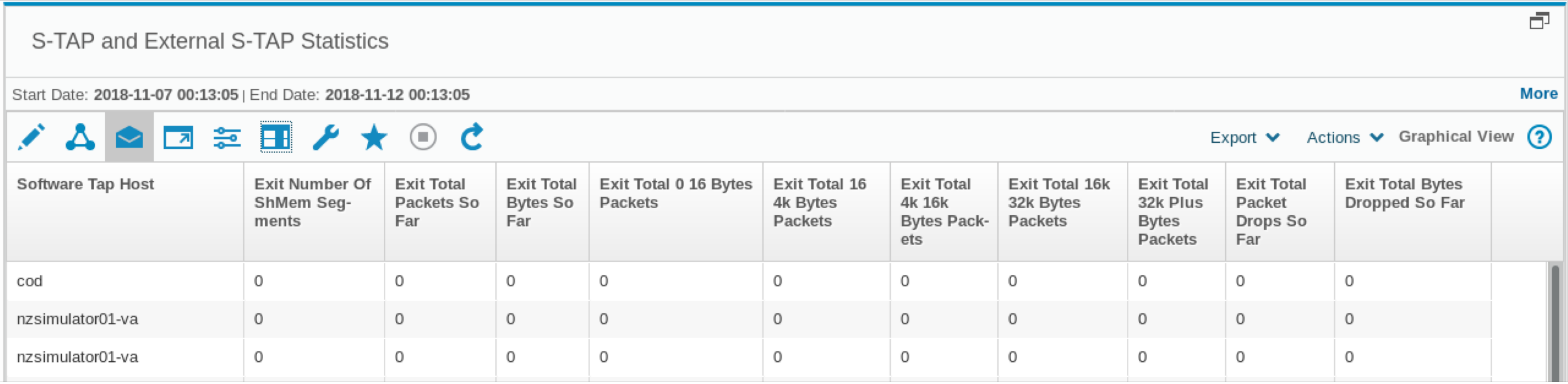
- Improvements made to ATAP to not require root user to activate instances did not work with GIM
    - Problem was that directory and file permissions were too restrictive in a GIM environment to permit a non-root user to check the STAP configuration and create an ATAP instance
    - Permissions have been modified to permit read and execute access to the necessary directories so that users configured in the inspection engine section of the STAP config file can write to a user specific directory to enable ATAP, allowing them to store configurations and activate ATAP
    - Uses the same authorization mechanism introduced in 10.5 to permit those instance to access the KTAP device
- Error messages from STAP with multiple collectors configured and participate_in_load_balancing=0 when processing kerberos tokens
    - Each kerberos token was being processed multiple times due to broken logic in the STAP. Did not cause a problem with processing the tokens, but did cause multiple error messages to be printed after the token was first processed.
    - Each token is now processed only once, eliminating the invalid error messages

Linux module signing

- New versions of Exadata require kernel modules to be signed by an approved key
  - Oracle will not sign the KTAP modules or our signing key
  - Modules are now shipped signed by a Guardium module signing key
  - Key is included in the KTAP files (guardium_module_signing.der) and the bundles on FixCentral, but must be manually enrolled
  - Procedure is documented at http://www-01.ibm.com/support/docview.wss?uid=swg22016425
    - Procedure is not specific to Exadata and the screens provided by the OS while in the EFI shim layer when enrolling the new key may vary

Exit statistics

- EXIT interface statistics have not been sent to the collector or surfaced in the UI
  - This is now provided as part of the regular STAP statistics. Items are similar to the KTAP statistics and count the number of packets and bytes captured, as well as the number of packets within certain size ranges, and the number of packets and bytes dropped by the interface



S-TAP and External S-TAP Statistics

Start Date: **2018-11-07 00:13:05** | End Date: **2018-11-12 00:13:05**

Software Tap Host	Exit Number Of ShMem Segments	Exit Total Packets So Far	Exit Total Bytes So Far	Exit Total 0 16 Bytes Packets	Exit Total 16 4k Bytes Packets	Exit Total 4k 16k Bytes Packets	Exit Total 16k 32k Bytes Packets	Exit Total 32k Plus Bytes Packets	Exit Total Packet Drops So Far	Exit Total Bytes Dropped So Far
cod	0	0	0	0	0	0	0	0	0	0
nzsimulator01-va	0	0	0	0	0	0	0	0	0	0
nzsimulator01-va	0	0	0	0	0	0	0	0	0	0

New databases

- Datastax
  - New parameters in STAP config
    - cassandra_audit_enable (0=off, 1=on), cassandra_audit_delimiter
    - Implemented as a pipe reader for log4j audit logs, file is .cassandra_audit in the STAP directory
    - https://www.ibm.com/support/knowledgecenter/en/SSMPHH_10.6.0/com.ibm.guardium.doc.stap/stap/unix_cassandra_audit_log_to_file_appender.html (when 10.6 documentation is live)
- Vertica 9
  - ATAP is supported, db_type=vertica
- Cloudera 5.12
  - Use the Kafka integration
- Oracle 18
- PostgreSQL 9.6
- Sybase 17.5

New operating systems

- Ubuntu 18.04 LTS support added
- RHEL 4 removed

Masking sensitive data

Overview - Description

Describe what is new

- What’s new

On logging of exceptions and errors, we will mask/replace values when configured either by global cli command or rule pattern

- Benefits/Value

Like access rule, values in sqls are replaced for exception policy rule or parser error when configured. Fulfill GDPR requirements for exceptions and errors.

Overview - Use cases and demonstration

Use cases

- When Masking Pattern/Replacement Character configured in policy rule, sqls for exception rule and syntax errors are masked accordingly.
- When cli parameter snif_mask_sql_value on, generic sql (sql masked with ?) is used for exception rule and syntax error.

Demonstrate the new feature

Exception rule with Excpt. Type: SQL_ERROR, Masking Pattern: (\d{4,10}), Replacement Character: *, Rule Action: alert per match, log full details per session

*Issue select * from phonenumber where phonenumber = '12345' through sqlplus*

Overview - Use cases and demonstration(2)

GDM_EXCEPTION record with:

EXCEPTION_TYPE_ID: SQL_ERROR

DESCRIPTION: ORA-00942

*SQL_STRING: select * from phonenumber where phonenumber = '*****'*

GDM_POLICY_VIOLATIONS_LOG record with same sql string as above.

%%SQLString variable in message template replaced by same sql string as above

Access rule with Masking Pattern: (\d{4,10}), Replacement Character: *, Rule Action: alert per match, log full detail

*Issue delete * from phonenumber where phonenumber = '12345'*

GDM_ERROR record with:

ERROR_TYPE: PARSER_ERROR

*SQL_STRING: delete * from phonenumber where phonenumber = '*****'*

cli command: store_snif_mask_sql_value on

Overview - Use cases and demonstration(3)

Same masked sql in GDM_POLICY_VIOLATIONS_LOG, GDM_CONSTRUCT_TEXT Record, %%SQLString variable in message template(MESSAGE_TEXT record).

cli command: store snif_mask_sql_value on, Access rule with Rule Action: alert per match, log full detail with masked details

*Issue delete * from phonenumber where phonenumber = '12345'*
GDM_ERROR record with:

ERROR_TYPE: PARSER_ERROR

*SQL_STRING: delete * from phonenumber where phonenumber = ?*

Exception rule with Excpt. Type: SQL_ERROR, Rule Action: alert per match

*Issue delete * from phonenumber where phonenumber = '12345' through sqlplus*

Overview - Use cases and demonstration(4)

GDM_EXCEPTION record with:

EXCEPTION_TYPE_ID: SQL_ERROR

DESCRIPTION: ORA-00942

*SQL_STRING: select * from phonenumber where phonenumber = ?*

GDM_POLICY_VIOLATIONS_LOG record with same SQL_STRING as above

%%SQLNoValue variable in message template replaced by same sql string as above

Discover sensitive data (AKA Classification)

Overview - Description

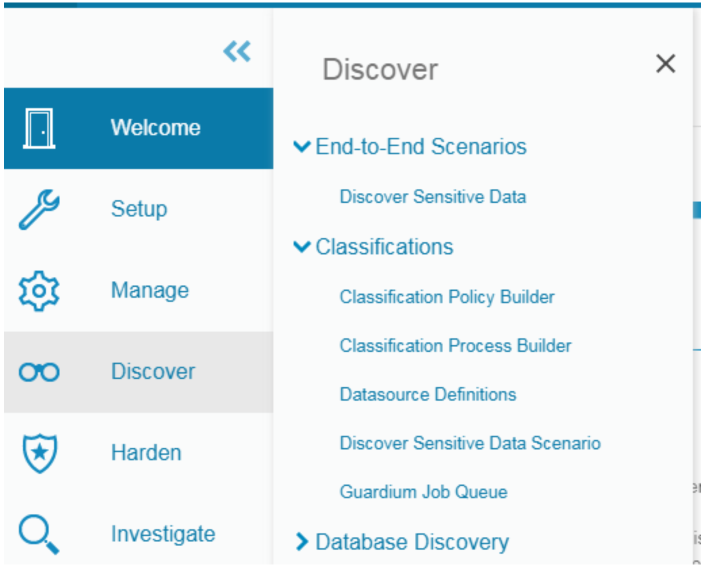
Enhancements have been made to Discover Sensitive Data (DSD) UI in 10.6 release to bring over all the functionality previously available in Classification Policy and Process builders.

With these enhancements DSD became a complete replacement for classification policy and process builders. As a result, these builders were removed in 10.6 simplifying the work load for struts2 migration.

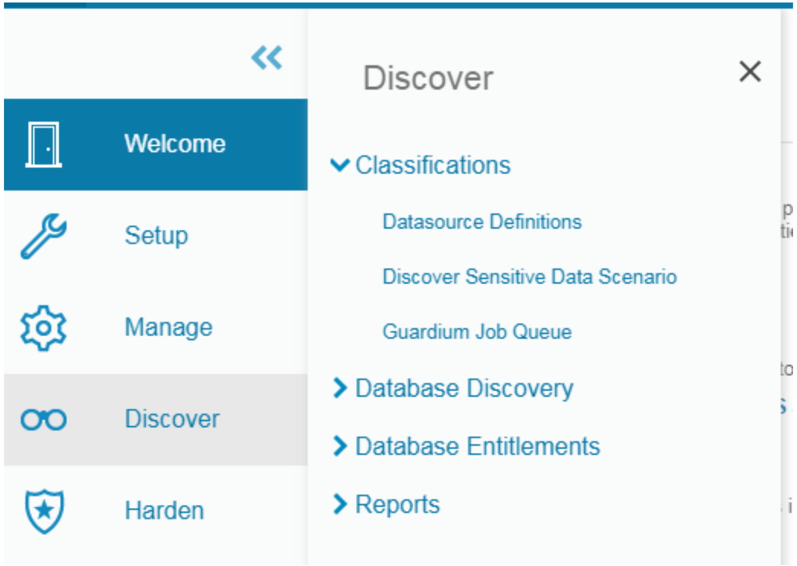
Overview - Description

Navigation structure was simplified and legacy screens removed in 10.6

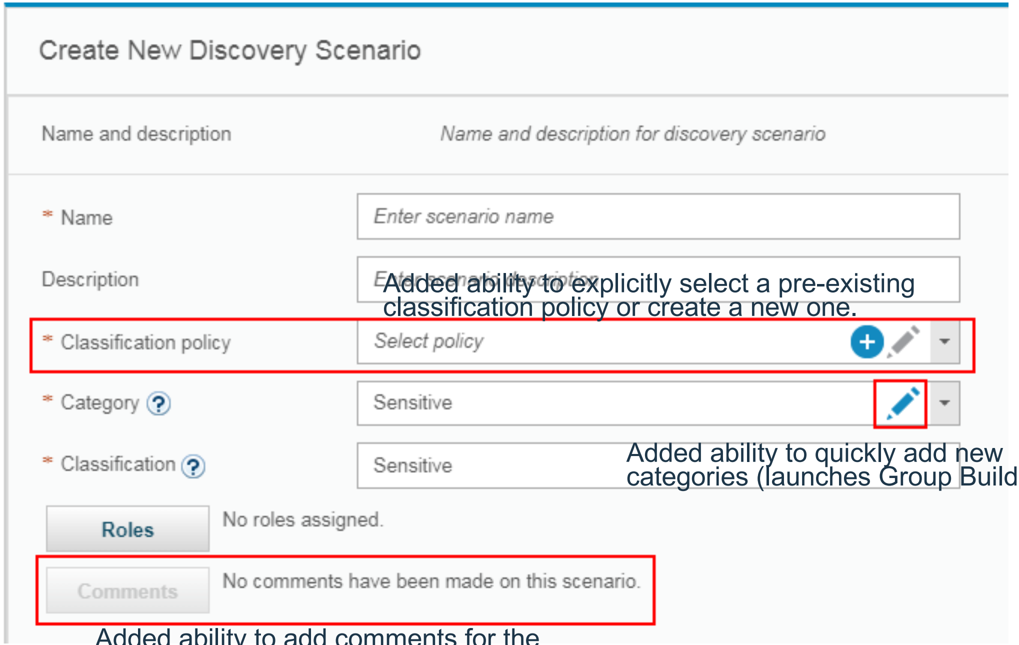
10.5 Navigation Layout



10.6 Navigation Layout



Overview - Description



Create New Discovery Scenario

Name and description — *Name and description for discovery scenario*

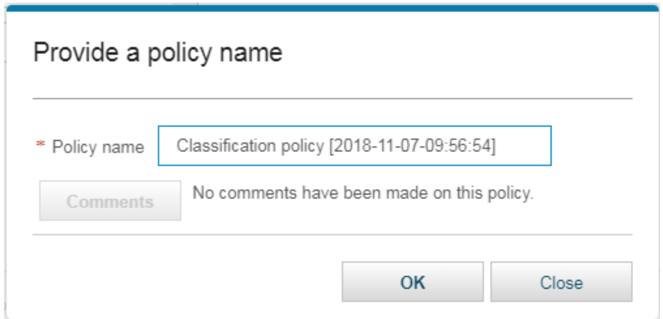
* Name	*Enter scenario name*
Description	*Enter scenario description*
* Classification policy	*Select policy*
* Category ?	Sensitive
* Classification ?	Sensitive
Roles	No roles assigned.
Comments	No comments have been made on this scenario.

Added ability to explicitly select a pre-existing classification policy or create a new one.

Added ability to quickly add new categories (launches Group Builder)

Added ability to add comments for the DSD (classification process level)

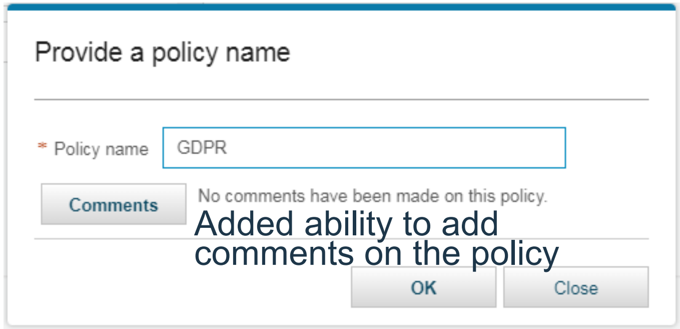
Click ⊕ to create new policy



Provide a policy name

* Policy name	Classification policy [2018-11-07-09:56:54]
Comments	No comments have been made on this policy.

Click ✎ to edit existing policy's name



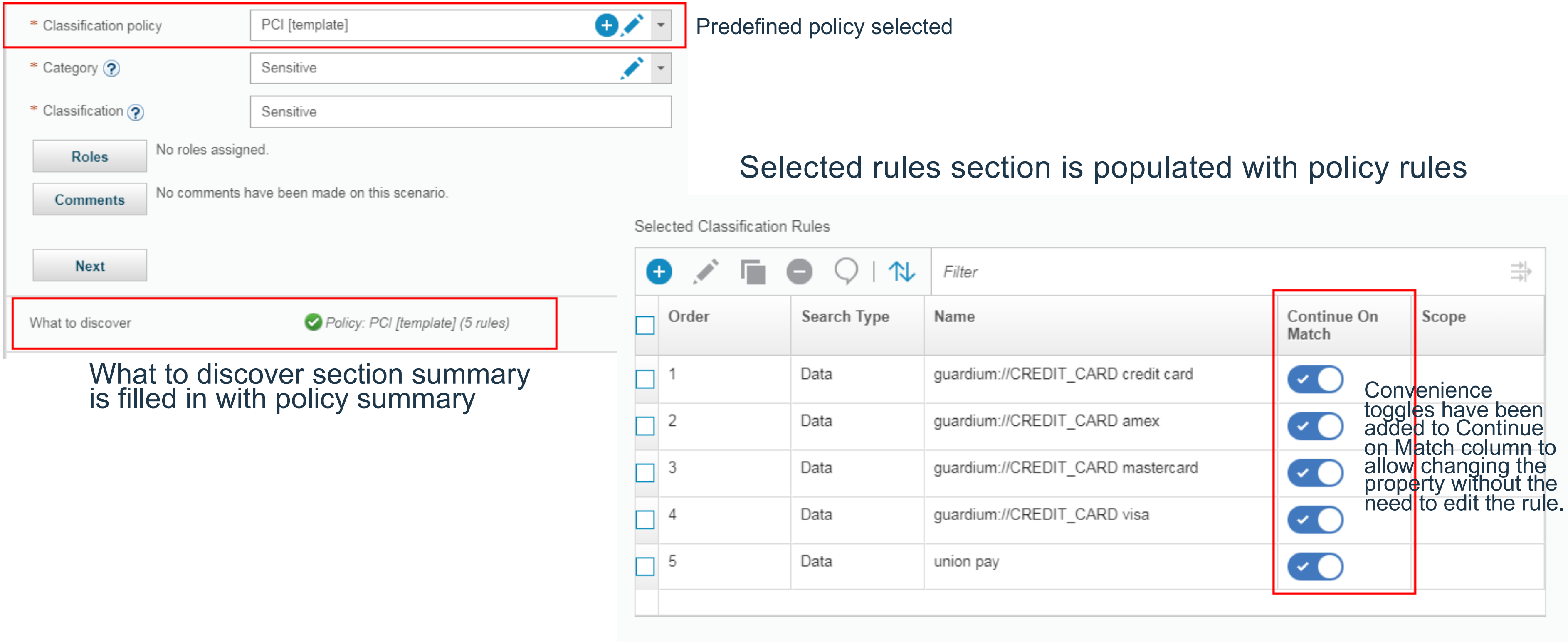
Provide a policy name

* Policy name	GDPR
Comments	No comments have been made on this policy.

Added ability to add comments on the policy

Overview - Description

Selecting an existing policy will populate the rule section with the policy rules.



* Classification policy: PCI [template]

Predefined policy selected

* Category: Sensitive

* Classification: Sensitive

No roles assigned.

No comments have been made on this scenario.

What to discover ✓ *Policy: PCI [template] (5 rules)*

What to discover section summary is filled in with policy summary

Selected rules section is populated with policy rules

Selected Classification Rules

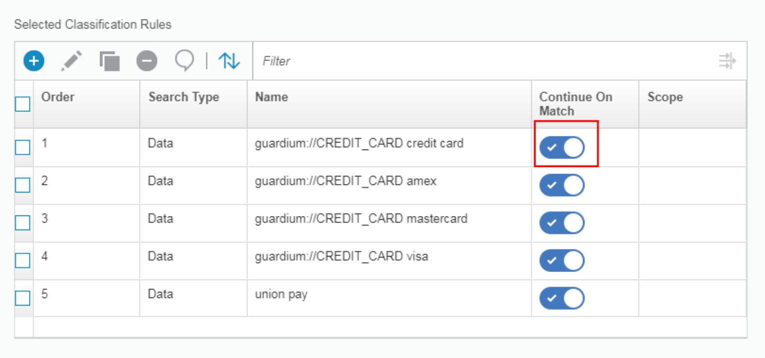
□	Order	Search Type	Name	Continue On Match	Scope
□	1	Data	guardium://CREDIT_CARD credit card	✓	
□	2	Data	guardium://CREDIT_CARD amex	✓	
□	3	Data	guardium://CREDIT_CARD mastercard	✓	
□	4	Data	guardium://CREDIT_CARD visa	✓	
□	5	Data	union pay	✓	

Convenience toggles have been added to Continue on Match column to allow changing the property without the need to edit the rule.

Overview - Description

Trying to modify a guardium predefined policy in any way (name change, rule add/remove/edit) will result in a clone of a policy being created and assigned to this DSD.

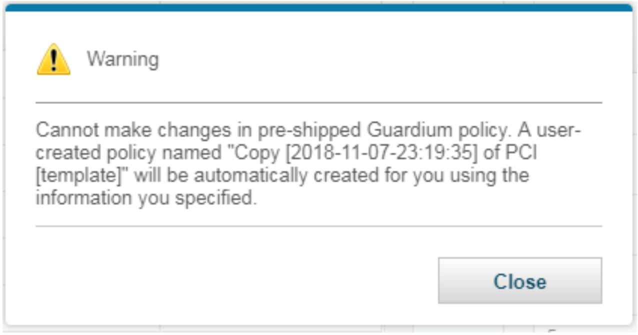
1



Selected Classification Rules

□	Order	Search Type	Name	Continue On Match	Scope
□	1	Data	guardium://CREDIT_CARD credit card	✓	
□	2	Data	guardium://CREDIT_CARD amex	✓	
□	3	Data	guardium://CREDIT_CARD mastercard	✓	
□	4	Data	guardium://CREDIT_CARD visa	✓	
□	5	Data	union pay	✓	

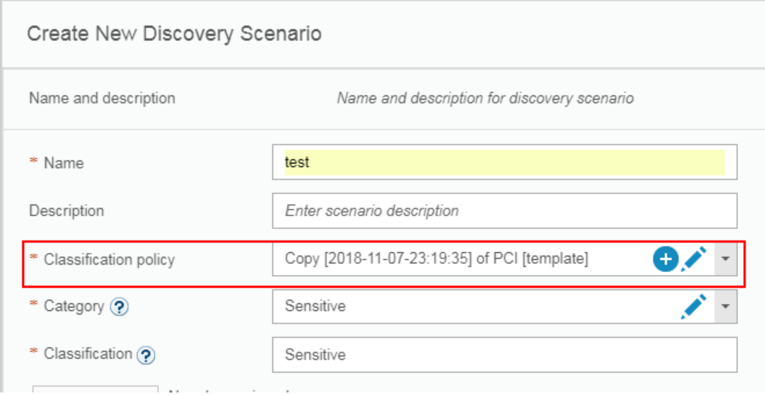
2



Warning

Cannot make changes in pre-shipped Guardium policy. A user-created policy named "Copy [2018-11-07-23:19:35] of PCI [template]" will be automatically created for you using the information you specified.

3

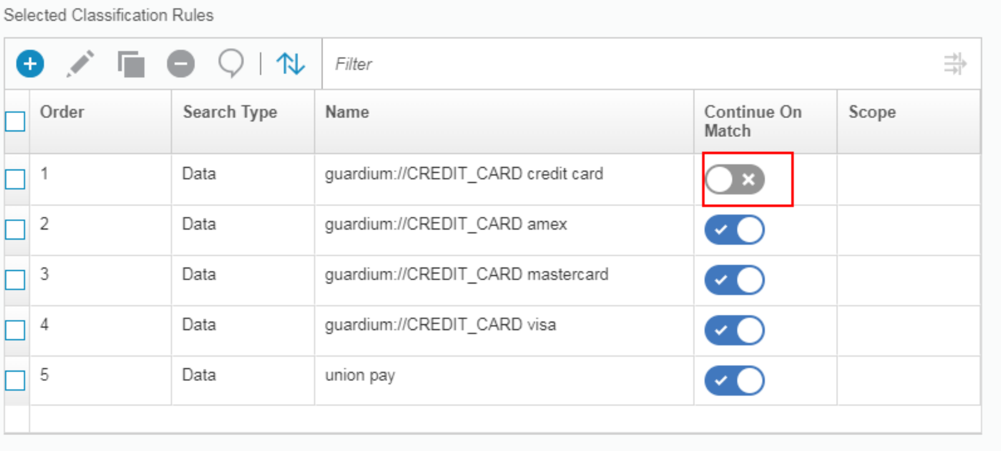


Create New Discovery Scenario

Name and description — *Name and description for discovery scenario*

* Name	test
Description	*Enter scenario description*
* Classification policy	Copy [2018-11-07-23:19:35] of PCI [template]
* Category ?	Sensitive
* Classification ?	Sensitive

4



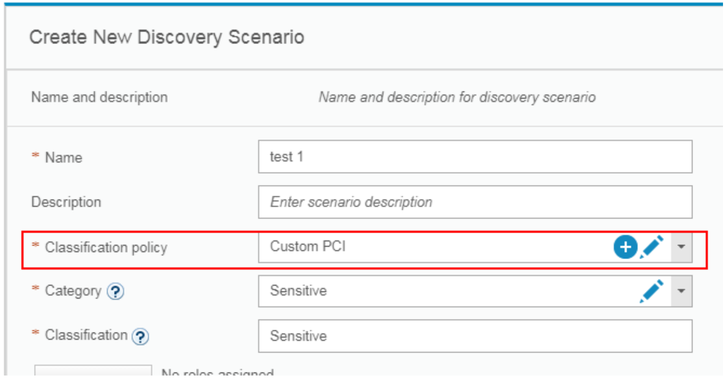
Selected Classification Rules

□	Order	Search Type	Name	Continue On Match	Scope
□	1	Data	guardium://CREDIT_CARD credit card	✗	
□	2	Data	guardium://CREDIT_CARD amex	✓	
□	3	Data	guardium://CREDIT_CARD mastercard	✓	
□	4	Data	guardium://CREDIT_CARD visa	✓	
□	5	Data	union pay	✓	

Overview - Description

Trying to modify a pre-defined policy in any way (name change, rule add/remove/edit) will result in a usage check of the policy. If policy is used in more then one DSD user will be notified of the impact of the change.

1



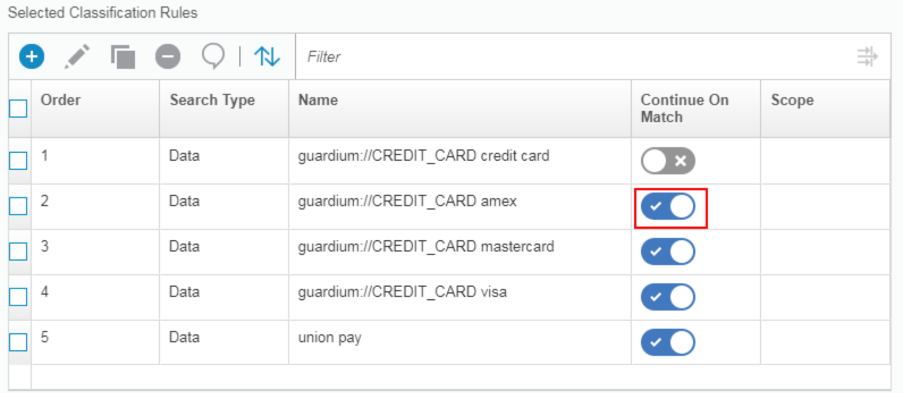
Create New Discovery Scenario

Name and description — *Name and description for discovery scenario*

* Name	test 1
Description	*Enter scenario description*
* Classification policy	Custom PCI
* Category	Sensitive
* Classification	Sensitive

No roles assigned

2

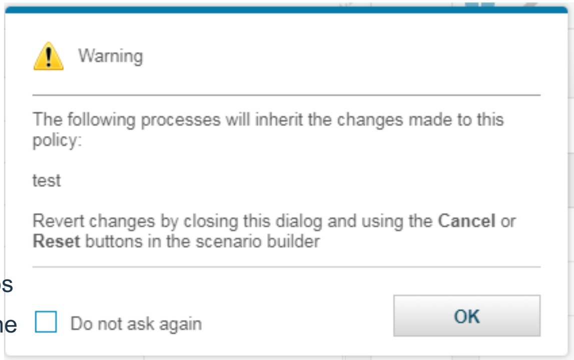


Selected Classification Rules

Filter

□	Order	Search Type	Name	Continue On Match	Scope
□	1	Data	guardium://CREDIT_CARD credit card	✗	
□	2	Data	guardium://CREDIT_CARD amex	✓	
□	3	Data	guardium://CREDIT_CARD mastercard	✓	
□	4	Data	guardium://CREDIT_CARD visa	✓	
□	5	Data	union pay	✓	

3



Warning

The following processes will inherit the changes made to this policy:

test

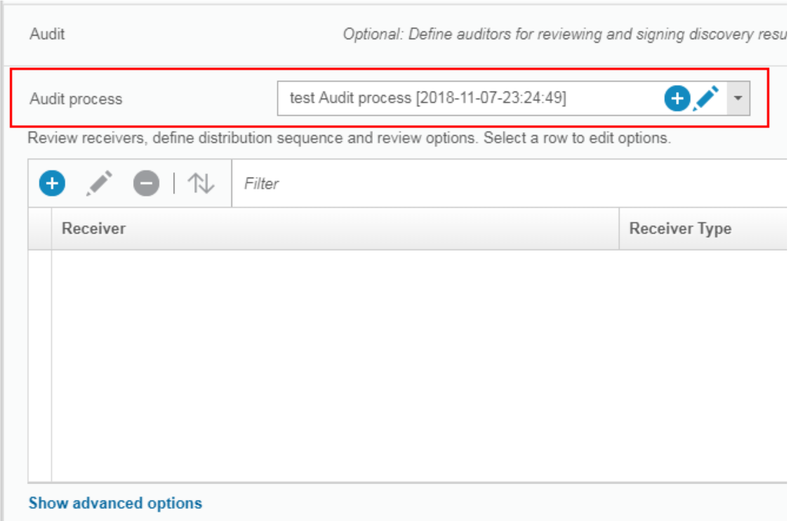
Revert changes by closing this dialog and using the **Cancel** or **Reset** buttons in the scenario builder

□ Do not ask again

Can click this to avoid repeated popups if multiple changes are planned to the policy. Will stop the popups only for the duration of the current DSD edit.

Overview - Description

Added the ability to explicitly select the audit process for running the DSD.



Audit

Optional: Define auditors for reviewing and signing discovery resu

Audit process: test Audit process [2018-11-07-23:24:49]

Review receivers, define distribution sequence and review options. Select a row to edit options.

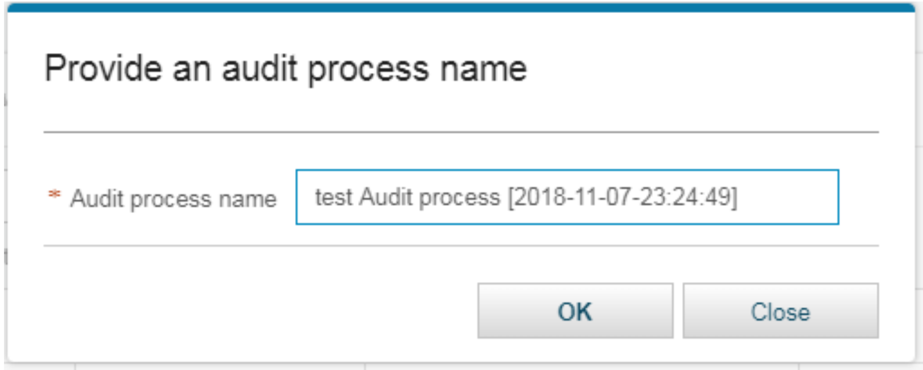
Receiver	Receiver Type

Show advanced options

For new DSD the control is automatically prefilled with a new generated audit process name.

NOTE: New audit process would only be created if either a at least one receiver is added or a schedule is assigned.

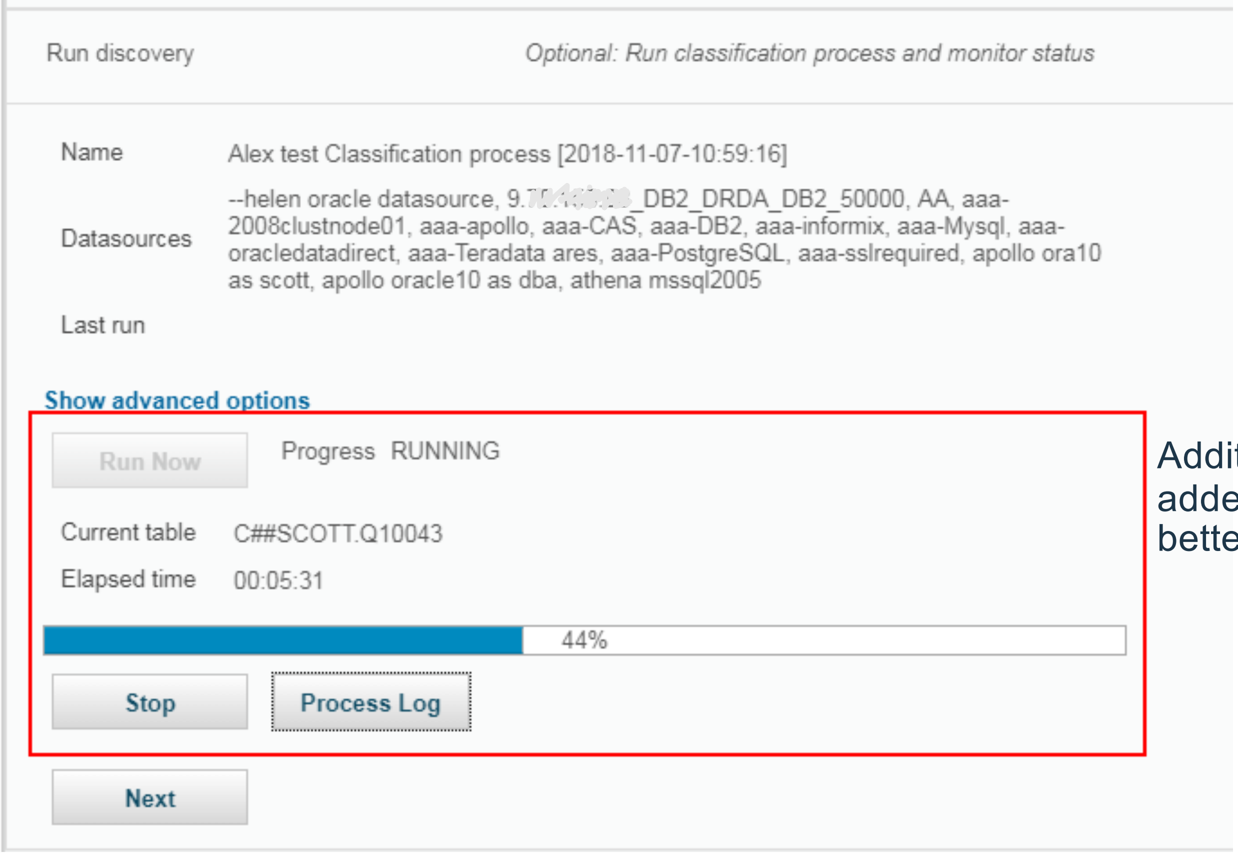
Process name can be edited by clicking the ✎



Provide an audit process name

* Audit process name: test Audit process [2018-11-07-23:24:49]

Overview - Description



Run discovery — *Optional: Run classification process and monitor status*

Name: Alex test Classification process [2018-11-07-10:59:16]

Datasources: --helen oracle datasource, 9.[redacted]_DB2_DRDA_DB2_50000, AA, aaa-2008clustnode01, aaa-apollo, aaa-CAS, aaa-DB2, aaa-informix, aaa-Mysql, aaa-oracledatadirect, aaa-Teradata ares, aaa-PostgreSQL, aaa-sslrequired, apollo ora10 as scott, apollo oracle10 as dba, athena mssql2005

Last run

Progress RUNNING

Current table C##SCOTT.Q10043

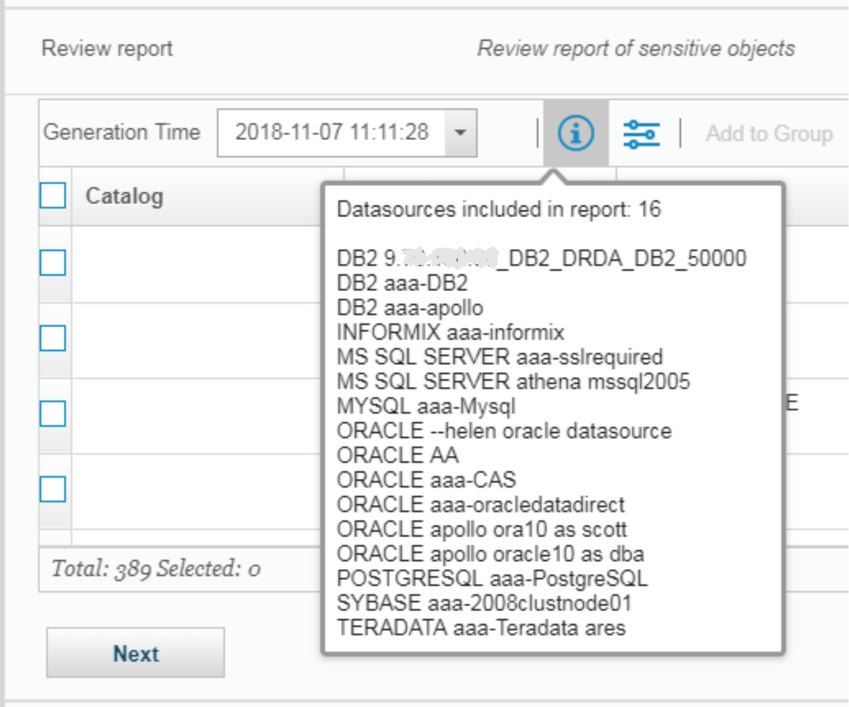
Elapsed time 00:05:31

44%

Additional run information has been added on “Run Now” to display better run progress.

Overview - Description

Added information hover to the report showing the list of datasources that was used in that process run



Review report

Review report of sensitive objects

Generation Time: 2018-11-07 11:11:28

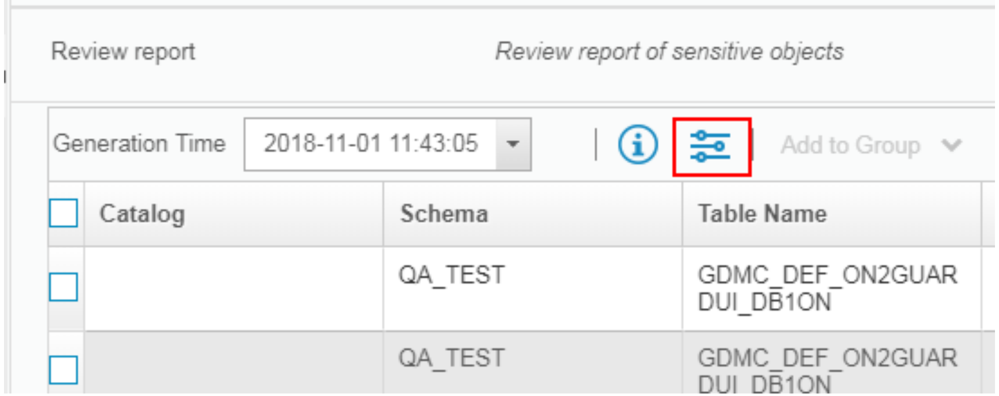
□ Catalog

Datasources included in report: 16

DB2 9.[redacted]_DB2_DRDA_DB2_50000
DB2 aaa-DB2
DB2 aaa-apollo
INFORMIX aaa-informix
MS SQL SERVER aaa-sslrequired
MS SQL SERVER athena mssql2005
MYSQL aaa-Mysql
ORACLE --helen oracle datasource
ORACLE AA
ORACLE aaa-CAS
ORACLE aaa-oracledatadirect
ORACLE apollo ora10 as scott
ORACLE apollo oracle10 as dba
POSTGRESQL aaa-PostgreSQL
SYBASE aaa-2008clustnode01
TERADATA aaa-Teradata ares

Total: 389 Selected: 0

Moved all the report options out into it's own configuration dialog.

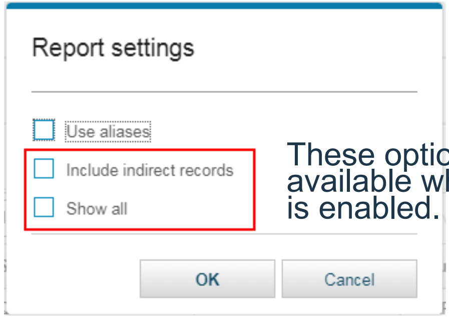


Review report

Review report of sensitive objects

Generation Time: 2018-11-01 11:43:05

□	Catalog	Schema	Table Name
□		QA_TEST	GDMC_DEF_ON2GUARDUI_DB1ON
□		QA_TEST	GDMC_DEF_ON2GUARDUI_DB1ON



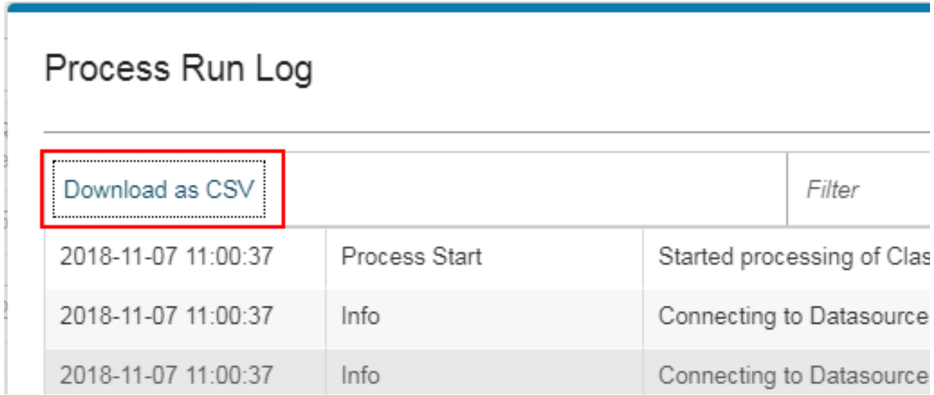
Report settings

□ Use aliases
□ Include indirect records
□ Show all

These options are only available when data security is enabled.

Overview - Description

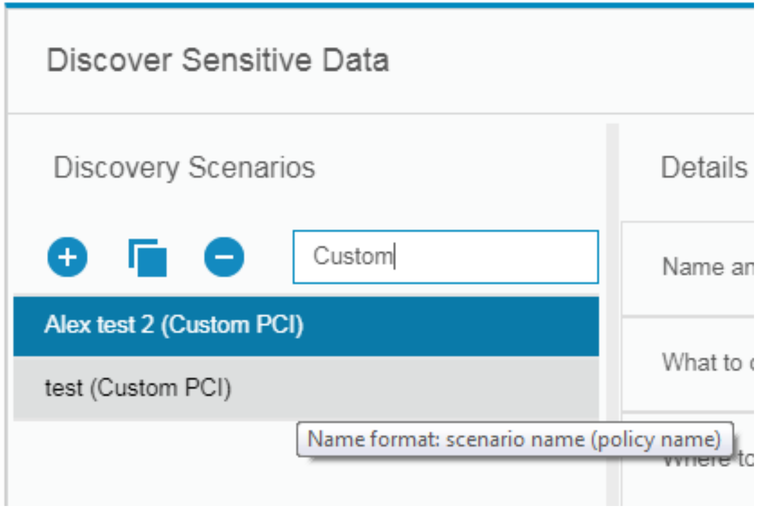
Added ability to export the classification log to CSV



Process Run Log

2018-11-07 11:00:37	Process Start	Started processing of Clas
2018-11-07 11:00:37	Info	Connecting to Datasource
2018-11-07 11:00:37	Info	Connecting to Datasource

Added ability to filter the scenario list on used policy name allowing users to quickly see where specific policy is used



Discover Sensitive Data

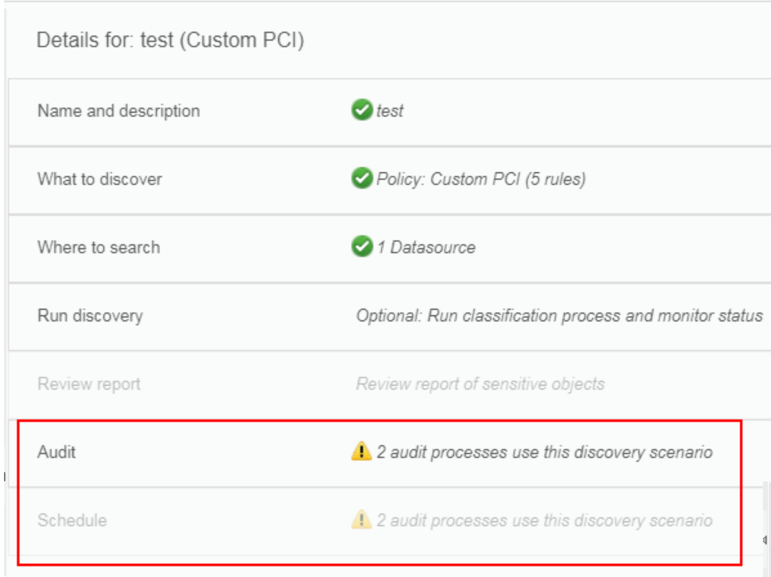
Discovery Scenarios

Custom

- Alex test 2 (Custom PCI)
- test (Custom PCI)

Name format: scenario name (policy name)

Overview - Description



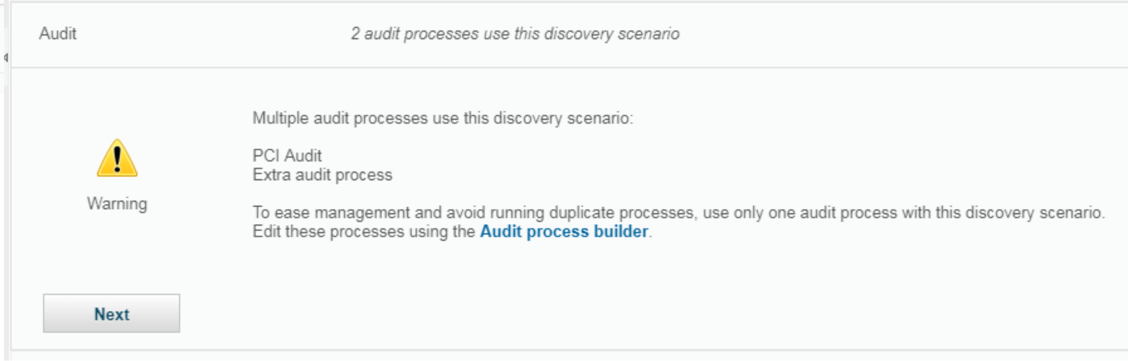
Details for: test (Custom PCI)

Name and description	✓ *test*
What to discover	✓ *Policy: Custom PCI (5 rules)*
Where to search	✓ *1 Datasource*
Run discovery	*Optional: Run classification process and monitor status*
Review report	*Review report of sensitive objects*
Audit	⚠ *2 audit processes use this discovery scenario*
Schedule	⚠ *2 audit processes use this discovery scenario*

Added detection of undesired conditions where same classification process appears in multiple audit processes.

When such condition is detected, DSD UI shows an appropriate warning and disallows editing of properties related to audit process (receivers and schedule) since we don’t know which one to pick.

User is directed to rectify this situation via Audit process builder (via provided link) while listing the offending audit process names.



Audit *2 audit processes use this discovery scenario*

Warning

Multiple audit processes use this discovery scenario:

PCI Audit
Extra audit process

To ease management and avoid running duplicate processes, use only one audit process with this discovery scenario. Edit these processes using the **Audit process builder**.

Platform Updates and enhancements

Redhat Updates

- Updated to Redhat 6.9 Santiago
- Guardium 10.6 uses kernel 2.6.32-696.20.1.el6.x86_64
  - Includes updates for Spectre and Meltdown OS issues
- Timezone updated to the latest version

Firmware Updates

- Coordinated block testing with Intel, Lenovo, IBM Manufacturing and Guardium Development
- Block testing to ensure entire firmware block is valid
- Released as both ISO and USB Images
- Releases for both x3550 M4 and M5 based Guardium appliances

Firmware Updates M5 versions

- The M5 Latest firmware versions:
- DSA = v10.3 (DSAOB2Q)
  IMM2 = v4.90 (TCOE44C)
  UEFI = v2.70 (TBEG36H)
  M5210 = v24.21.0-0052

- Guardium_FirmwareUpdate_X3550M5_USB_v3-20
  - https://www-945.ibm.com/support/fixcentral/swg/doSelectFixes?options.selectedFixes=Guardium_FirmwareUpdate_X3550M5_USB_v3-20&continue=1
- Guardium_FirmwareUpdate_X3550M5_DVD_v3-20
  https://www-945.ibm.com/support/fixcentral/swg/doSelectFixes?options.selectedFixes=Guardium_FirmwareUpdate_X3550M5_DVD_v3-20&continue=1

Firmware Updates M4 versions

- The M4 Latest firmware versions:

DSA =	9.54 (DSYTD8G)
IMM2 =	6.81 (1AOO84D)
UEFI =	2.70 (D7E164C)
M5210 =	24.21.0-0052

- Guardium_FirmwareUpdate_X3550M4_USB_v5-20
  - https://www-945.ibm.com/support/fixcentral/swg/doSelectFixes?options.selectedFixes=Guardium_FirmwareUpdate_X3550M4_USB_v5-20&continue=1

- Guardium_FirmwareUpdate_X3550M4_DVD_v5-20
  - https://www-945.ibm.com/support/fixcentral/swg/doSelectFixes?options.selectedFixes=Guardium_FirmwareUpdate_X3550M4_DVD_v5-20&continue=1

SNMP Enhancements

- SNMP cli support for Trap Hosts the Platform team first modified firewall so that second host could be seen.
- CLI commands were added to "show" and "store" the secondary trap host. CLI and code support was added to clean and reset the secondary trap host.
  - show alerter snmp secondary_traphost
  - store alerter snmp secondary_community
  - store alerter snmp secondary_traphost

  - There is also “show alerter snmp seconardy_community”, but that is exposed to end users.

Syslog enhancements

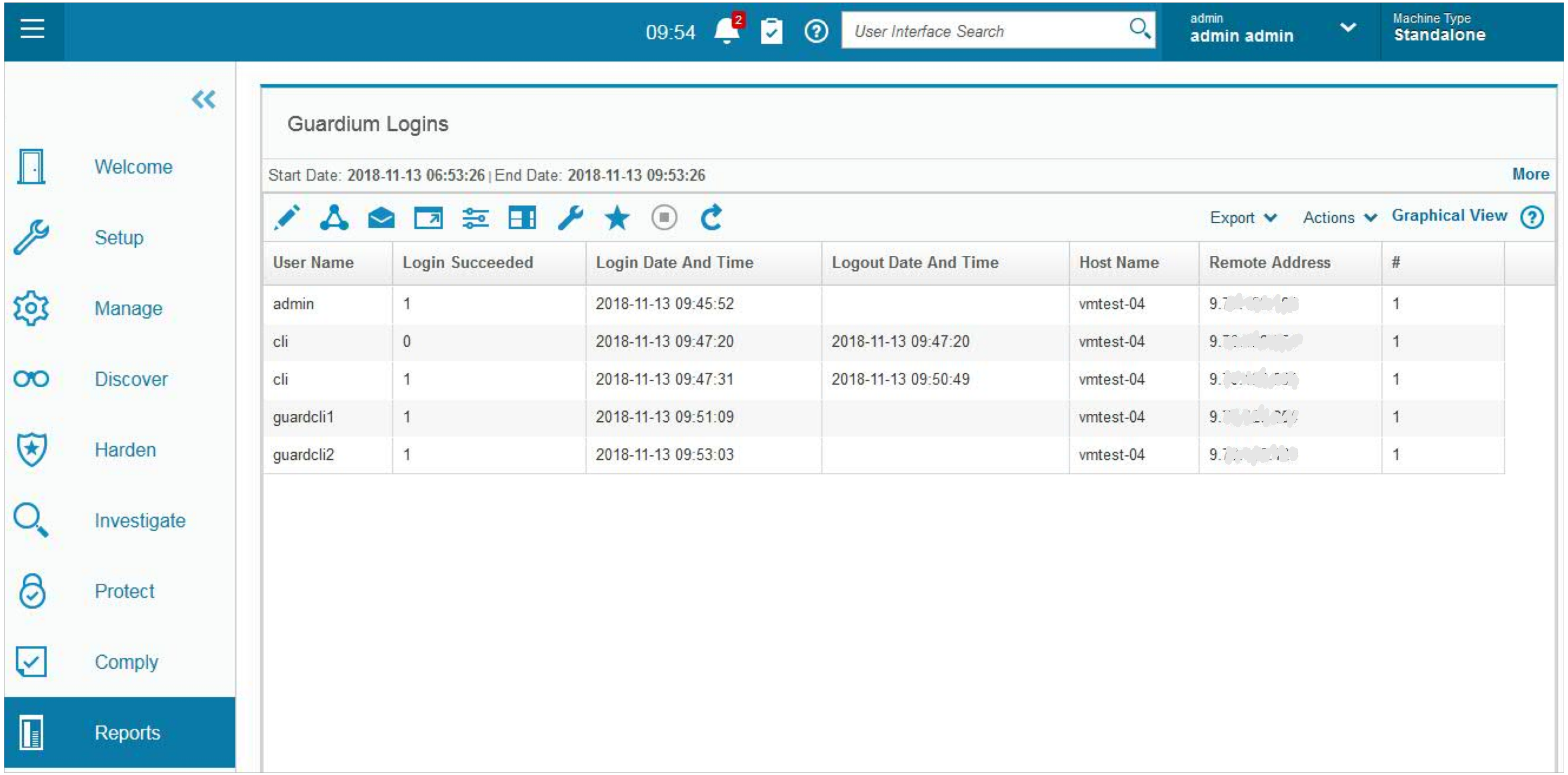
- A change was made between 10.1.4 and 10.6 on the output of syslog messages. It was found that a 3-digit octal number (#012 or #011) was getting added to syslog messages. This change caused SIEMs problems in parsing our syslog messages.
- New commands to enable or disable escape characters in syslog
  - show command to show if escape control characters are on
    - show remotelog escape_control_characters_on_receive
  - store command to set escape characters are on or off
    - store remotelog escape_control_characters_on_receive [on|off]
- When used, /etc/rsyslog.conf has this option modified (on or off depending on the command)
  - $EscapeControlCharactersOnReceive on
- By default, this option is not in /etc/rsyslog.conf

Guardium Logins Report

Guardium Logins is a report used for capturing who logged into the Guardium appliance.

The report was originally designed to only show the GUI users, "Admin", "Accessmgr” and "Guardium". Several customer required that it also display the guardcli users, “cli” and “guardcli[1-5]”. The report now captures logins data for “cli” and all “guardcli” users now. The report displays the login ,logout time and the remote address the user logged in from in the same manner GUI user login information is displayed. .

Guardium Logins Report with cli and guardcli users



Guardium Logins

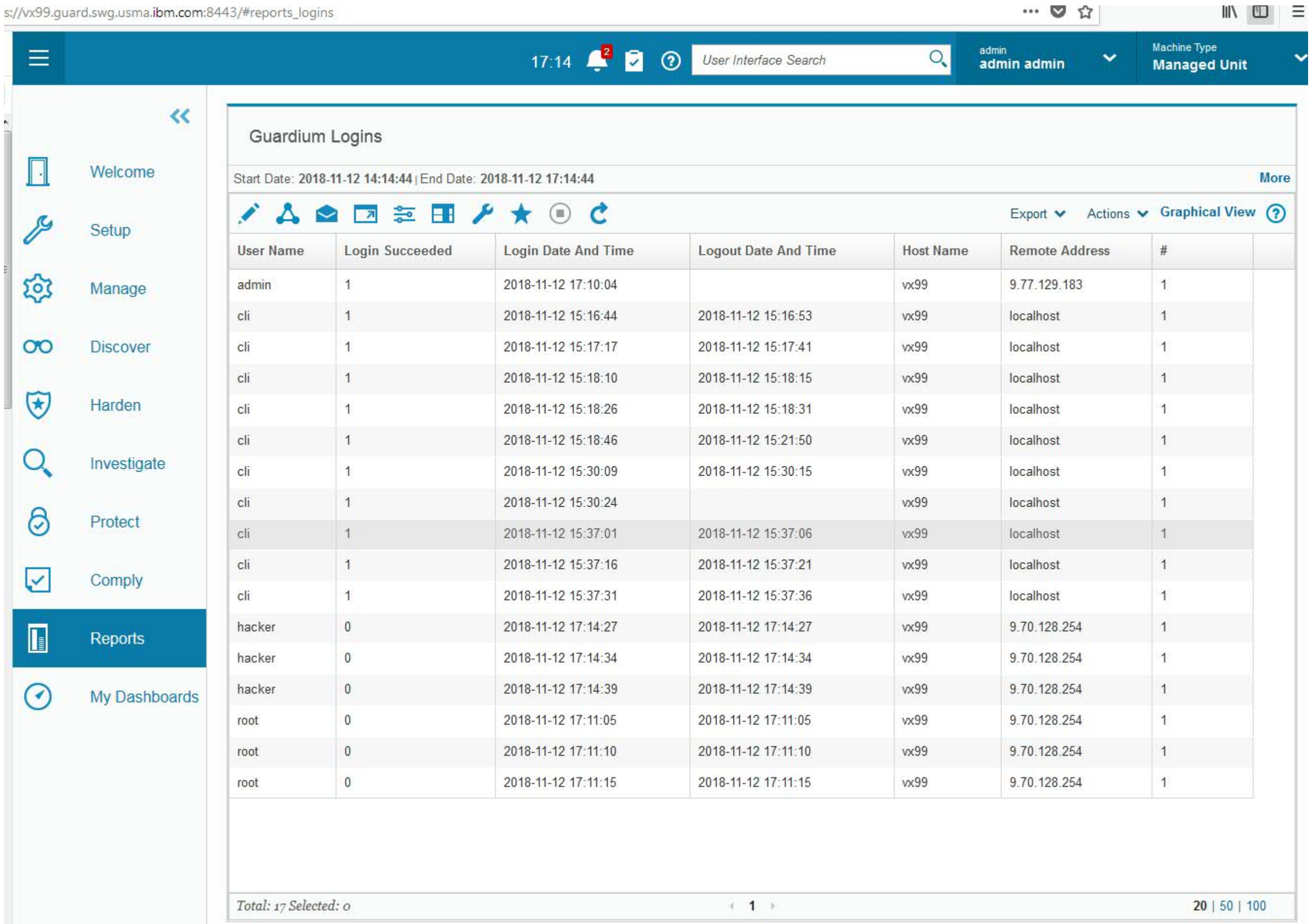
Start Date: 2018-11-13 06:53:26 | End Date: 2018-11-13 09:53:26

User Name	Login Succeeded	Login Date And Time	Logout Date And Time	Host Name	Remote Address	#
admin	1	2018-11-13 09:45:52		vmtest-04	9.7[redacted]	1
cli	0	2018-11-13 09:47:20	2018-11-13 09:47:20	vmtest-04	9.7[redacted]	1
cli	1	2018-11-13 09:47:31	2018-11-13 09:50:49	vmtest-04	9.[redacted]	1
guardcli1	1	2018-11-13 09:51:09		vmtest-04	9.[redacted]	1
guardcli2	1	2018-11-13 09:53:03		vmtest-04	9.7[redacted]	1

Guardium Logins Report

There were several customers who wanted to capture failed logins to the Guardium appliance. Using PAM we were able to capture failed logins and add the data to Guardium Login Reports. The user name, attempted log in time and remote host information gets captured upon a failed login. The log out time is set to equal the failed login time. The failed login time, logout time, user name and remote host information as well as if login succeeded or not can then be displayed in the Guardium Logins Report.

Guardium Logins Report with failed logins



Guardium Logins

Start Date: **2018-11-12 14:14:44** | End Date: **2018-11-12 17:14:44**

User Name	Login Succeeded	Login Date And Time	Logout Date And Time	Host Name	Remote Address	#
admin	1	2018-11-12 17:10:04		vx99	9.77.129.183	1
cli	1	2018-11-12 15:16:44	2018-11-12 15:16:53	vx99	localhost	1
cli	1	2018-11-12 15:17:17	2018-11-12 15:17:41	vx99	localhost	1
cli	1	2018-11-12 15:18:10	2018-11-12 15:18:15	vx99	localhost	1
cli	1	2018-11-12 15:18:26	2018-11-12 15:18:31	vx99	localhost	1
cli	1	2018-11-12 15:18:46	2018-11-12 15:21:50	vx99	localhost	1
cli	1	2018-11-12 15:30:09	2018-11-12 15:30:15	vx99	localhost	1
cli	1	2018-11-12 15:30:24		vx99	localhost	1
cli	1	2018-11-12 15:37:01	2018-11-12 15:37:06	vx99	localhost	1
cli	1	2018-11-12 15:37:16	2018-11-12 15:37:21	vx99	localhost	1
cli	1	2018-11-12 15:37:31	2018-11-12 15:37:36	vx99	localhost	1
hacker	0	2018-11-12 17:14:27	2018-11-12 17:14:27	vx99	9.70.128.254	1
hacker	0	2018-11-12 17:14:34	2018-11-12 17:14:34	vx99	9.70.128.254	1
hacker	0	2018-11-12 17:14:39	2018-11-12 17:14:39	vx99	9.70.128.254	1
root	0	2018-11-12 17:11:05	2018-11-12 17:11:05	vx99	9.70.128.254	1
root	0	2018-11-12 17:11:10	2018-11-12 17:11:10	vx99	9.70.128.254	1
root	0	2018-11-12 17:11:15	2018-11-12 17:11:15	vx99	9.70.128.254	1

Total: 17 Selected: 0

1

20 | 50 | 100

GUI Password Enhancements

Overview - Simple

Starting in IBM Security Guardium version 10.6, there are 2 new GUI user password related features.

User's passwords for the GUI are now hashed with a strong algorithm.

- By default, GUI user ids will be hashed with a strong hashing algorithm when the users log in.
  - Strong password hashing is on by default, no commands to run
  - User's will not see any difference in behavior when logging in.

Admin's have the ability to enforce strong password rules - STIG rule compliance APP3320.

- Admin can run new CLI command to enable strong password compliance
- User's that change their password post enablement, or new users must adhere to the new formatting and use rules.

Benefits/Value

- Customers that are concerned about passwords can be assured Guardium is using strong hashing algorithm.
- Customers that have requirements to be compliant with strong password rules will benefit with Guardium offering this choice.

Overview - Advanced

Strong password hashing

- By default, user passwords will be hashed with a strong hashing algorithm when users log in to the GUI on a IBM Security Guardium 10.6 appliance

- Admin’s may optionally run the CLI command “store disable_sha1_passwords true” to remove weak hashed passwords from their appliances.

- “store disable_sha1_passwords true” command dependencies:
  - In a CM environment, Admins must have all appliances at version 10.6 or later
  - In a CM environment, the command must be run on the CM and any backup CMs
  - Command only removes weak passwords for users that have logged in since the appliance was upgraded to 10.6
    - Post enablement, Admins can run the CLI command “show disable_sha1_passwords” to verify the enablement and see a list of users that have not logged in since the appliance was upgraded.
  - New customers can run this command after initial setup to ensure all UI passwords will always be hashed strong.

Overview - Advanced

Strong password rules

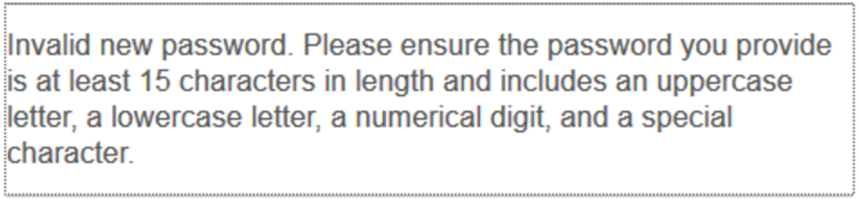
- Strong UI password rule compliance is now available for Admins to enable.
  - Admins can run new CLI command “store enable_strong_passwords true” to enable strong password compliance with STIG rule APP3320.
  - Admins can run new CLI command “show enable_strong_passwords” to see the state of password compliance.
  - GUI user’s that change their password post enablement must adhere to the following rules:
    - Passwords length must now be 15 characters minimum
      - Include at least one uppercase alphabetic character
      - Include at least one lowercase alphabetic character
      - Include at least one non-alphanumeric (special) character
    - Expire after 60 days
    - 10 iterations of passwords are now maintained for prohibiting re-use.
    - Inability to change password more than 1 time within a 24 hours period
    - Not contain any known dictionary words
    - Last unsuccessful and successful login date/time, are displayed in the UI after a successful login

Implementation Considerations – Strong Password Rules

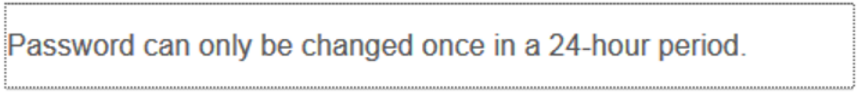
- Executing the CLI command “store strong_password_enabled true” will automatically restart the GUI.
- Admins that have configured LDAP will not see the new behavior changes for strong passwords since password compliance is enforced for local appliance users only.
- Admins that have configured the CLI command “password expiration gui” with a value greater than 60 days will see the value automatically changes to 60 days post running the command “store strong_password_enabled true”.
- Admins that wish to have all user password compliant can run command “store password expiration gui 1” to make all user’s passwords expire the following day, then set expiration back to a value of 60 or less. This would be done post running command “store strong_password_enabled true”

Implementation Considerations

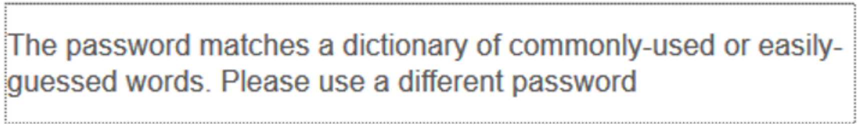
- Once strong password rules is enabled, UI dialogs will reference the new rules for password formatting and compliance errors similar to these:



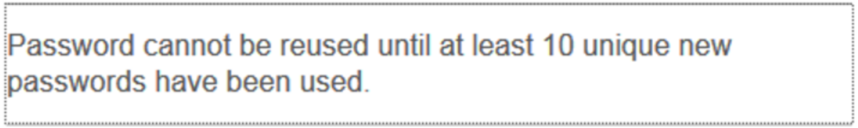
Invalid new password. Please ensure the password you provide is at least 15 characters in length and includes an uppercase letter, a lowercase letter, a numerical digit, and a special character.



Password can only be changed once in a 24-hour period.



The password matches a dictionary of commonly-used or easily-guessed words. Please use a different password



Password cannot be reused until at least 10 unique new passwords have been used.

Troubleshooting – Diagnostic Procedures

- General diagnostic procedure
  - Use the CLI command “show strong_password_enabled” to see if the strong password compliance is on or off.
  - Use the CLI command “show password expiration gui” to see how long user password are active before they get prompted to change them.
  - Admins can run the CLI command “show disable_sha1_passwords” to verify the enablement and see a list of users that have not logged in since the appliance was upgraded.

Certificate related changed and enhancements

Overview

- What is a SAN certificate?
  - Subject Alternative Name
  - An extension of X.509 standard
    - X.509 is a standard defining the format of public key certificate
  - Using `SubjectAlternativeName` field
- Usage/Benefits
  - Protect multiple domain names with a single certificate
  - Support only fully qualified domain names
  - Reduce SSL cost and maintenance
  - Names not required to belong to the same domain
  - Chrome 58 browser and later requires only SAN extension to match certificate

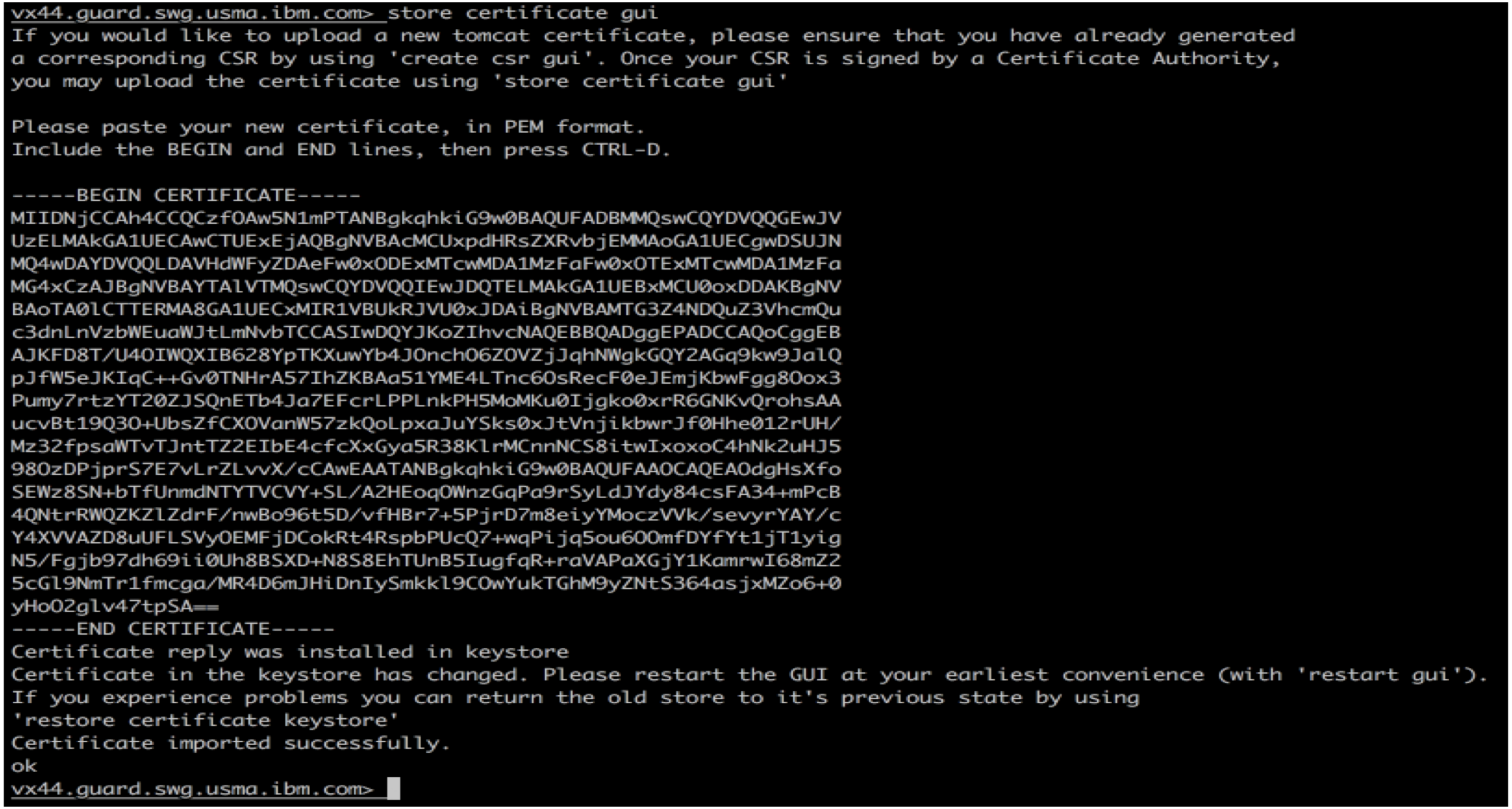
CLI Commands Enhancement

- Adds SAN as an optional feature in these CLI commands:
  - create csr gui
  - create csr external_stap
  - create csr gim
  - create csr alias
  - create csr sniffer
- Allow up to 9 SANs per CSR (certificate signing request) in fully qualified domain name format
- First SAN entry will automatically be CN (Common Name)

Steps to store the certificate

- Create a new CSR using CLI command “create csr gui”
- Self-sign the CSR or get it signed by a third-party
- Use CLI command “store certificate GUI” to store the signed certificate
- Run CLI Command “restart gui”

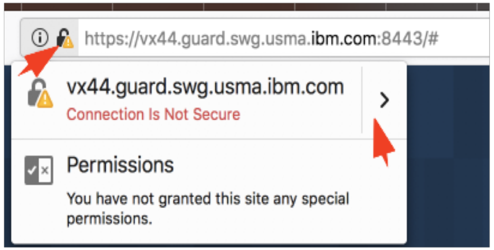
Screenshot of store certificate gui



```
vx44.guard.swg.usma.ibm.com> store certificate gui
If you would like to upload a new tomcat certificate, please ensure that you have already generated
a corresponding CSR by using 'create csr gui'. Once your CSR is signed by a Certificate Authority,
you may upload the certificate using 'store certificate gui'

Please paste your new certificate, in PEM format.
Include the BEGIN and END lines, then press CTRL-D.

-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQCzfOAw5N1mPTANBgkqhkiG9w0BAQUFADBMMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCTUExEjAQBgNVBAcMCUxpdHRsZXRvbjEMMAoGA1UECgwDSUJN
MQ4wDAYDVQQLDAVHdWFyZDAeFw0xODExMTcwMDA1MzFaFw0xOTExMTcwMDA1MzFa
MG4xCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTELMAkGA1UEBxMCU0oxDDAKBgNV
BAoTA0lCTTERMA8GA1UECxMIR1VBUkRJVU0xJDAiBgNVBAMTG3Z4NDQuZ3VhcmQu
c3dnLnVzbWEuaWJtLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AJKFD8T/U4OIWQXIB628YpTKXuwYb4JOnchO6ZOVZjJqhNWgkGQY2AGq9kw9JalQ
pJfW5eJKIqC++Gv0TNHrA57IhZKBAa51YME4LTnc6OsRecF0eJEmjKbwFgg8Oox3
Pumy7rtzYT20ZJSQnETb4Ja7EFcrLPPLnkPH5MoMKu0Ijgko0xrR6GNKvQrohsAA
ucvBt19Q3O+UbsZfCXOVanW57zkQoLpxaJuYSks0xJtVnjikbwrJf0Hhe012rUH/
Mz32fpsaWTvTJntTZ2EIbE4cfcXxGya5R38KlrMCnnNCS8itwIxoxoC4hNk2uHJ5
98OzDPjprS7E7vLrZLvvX/cCAwEAATANBgkqhkiG9w0BAQUFAAOCAQEAOdgHsXfo
SEWz8SN+bTfUnmdNTYTVCVY+SL/A2HEoqOWnzGqPa9rSyLdJYdy84csFA34+mPcB
4QNtrRWQZKZlZdrF/nwBo96t5D/vfHBr7+5PjrD7m8eiyYMoczVVk/sevyrYAY/c
Y4XVVAZD8uUFLSVyOEMFjDCokRt4RspbPUcQ7+wqPijq5ou6OOmfDYfYt1jT1yig
N5/Fgjb97dh69ii0Uh8BSXD+N8S8EhTUnB5IugfqR+raVAPaXGjY1KamrwI68mZ2
5cGl9NmTr1fmcga/MR4D6mJHiDnIySmkkl9COwYukTGhM9yZNtS364asjxMZo6+0
yHoO2glv47tpSA==
-----END CERTIFICATE-----
Certificate reply was installed in keystore
Certificate in the keystore has changed. Please restart the GUI at your earliest convenience (with 'restart gui').
If you experience problems you can return the old store to it's previous state by using
'restore certificate keystore'
Certificate imported successfully.
ok
vx44.guard.swg.usma.ibm.com> 
```

Steps to verify SAN in GUI certificate

- Open Guardium web-client on the browser (eg., Firefox)
  - For example: (https://vx44.guard.swg.usma.ibm.com:8443/#)
- To view the certificate:
  - Click on lock icon to the left of the address bar (screenshot 1)
  - Click on the right arrow (screenshot 1)
  - Click on "More information" (screenshot 2)



https://vx44.guard.swg.usma.ibm.com:8443/#

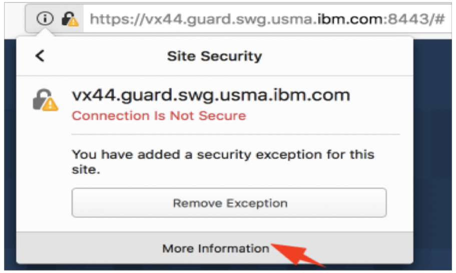
vx44.guard.swg.usma.ibm.com

Connection Is Not Secure

Permissions

You have not granted this site any special permissions.

(screenshot 1)



https://vx44.guard.swg.usma.ibm.com:8443/#

Site Security

vx44.guard.swg.usma.ibm.com

Connection Is Not Secure

You have added a security exception for this site.

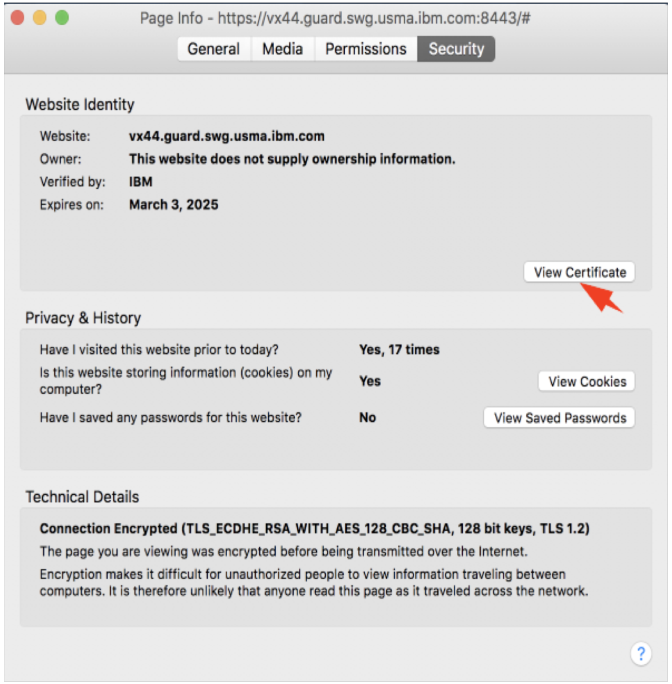
Remove Exception

More Information

(screenshot 2)

Steps to verify SAN in GUI certificate (contd ..)

- Click on “View Certificate”
- Click on “Details”



Website Identity

Website: **vx44.guard.swg.usma.ibm.com**
Owner: **This website does not supply ownership information.**
Verified by: **IBM**
Expires on: **March 3, 2025**

Privacy & History

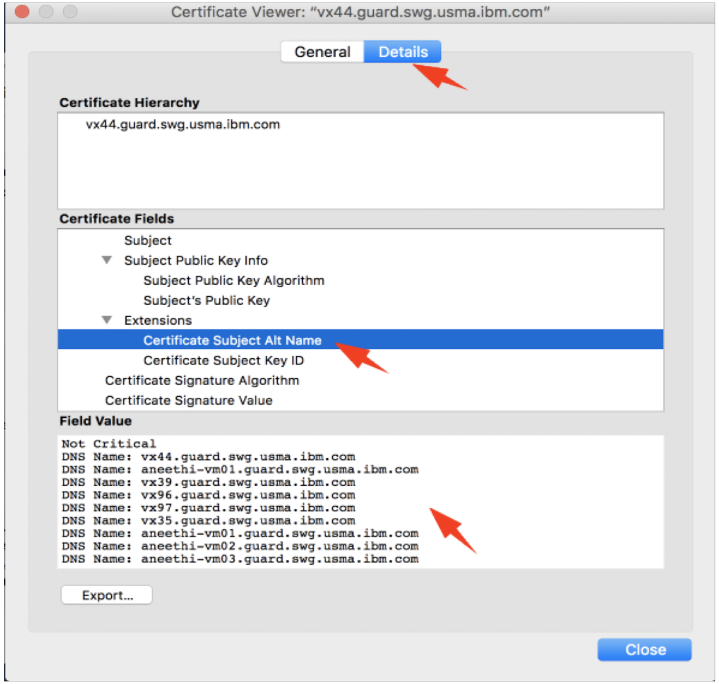
Have I visited this website prior to today?	**Yes, 17 times**	
Is this website storing information (cookies) on my computer?	**Yes**	View Cookies
Have I saved any passwords for this website?	**No**	View Saved Passwords

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, 128 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.



Certificate Hierarchy

vx44.guard.swg.usma.ibm.com

Certificate Fields

```
    Subject
  ▼ Subject Public Key Info
      Subject Public Key Algorithm
      Subject's Public Key
  ▼ Extensions
      Certificate Subject Alt Name
      Certificate Subject Key ID
  Certificate Signature Algorithm
  Certificate Signature Value
```

Field Value

```
Not Critical
DNS Name: vx44.guard.swg.usma.ibm.com
DNS Name: aneethi-vm01.guard.swg.usma.ibm.com
DNS Name: vx39.guard.swg.usma.ibm.com
DNS Name: vx96.guard.swg.usma.ibm.com
DNS Name: vx97.guard.swg.usma.ibm.com
DNS Name: vx35.guard.swg.usma.ibm.com
DNS Name: aneethi-vm01.guard.swg.usma.ibm.com
DNS Name: aneethi-vm02.guard.swg.usma.ibm.com
DNS Name: aneethi-vm03.guard.swg.usma.ibm.com
```

New certificate CLI commands

- Ability to store both private key and certificate
- Allow certificate keys that are generated externally to be stored in Guardium
- CLI commands:
  - `store certificate privatekey gui`

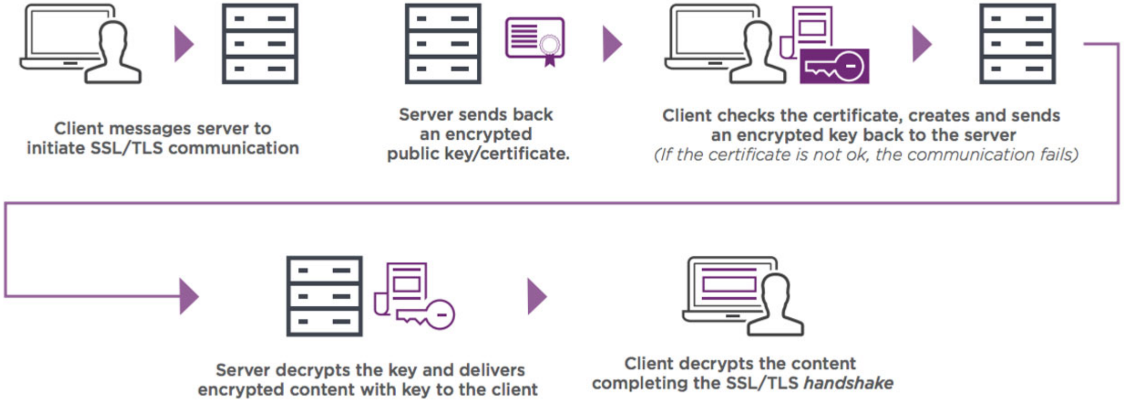
    - Stores GUI self-signed certificate and private key in the keystore
  - `store certificate privatekey gim`

    - Stores GIM self-signed certificate and private key in the keystore
  - Overwrite the current GUI/GIM certificate and private key
  - Certificate/Privatekey should be in PEM format
  - In case of problem, use CLI command `restore certificate keystore` to restore certificates to its previous state

Hostname certificate Validation in CM/MU Communications

Hostname certificate verification

- Certificates
  - Used in encrypting traffic
  - Used to validate host via hostname


Client messages server to initiate SSL/TLS communication
Server sends back an encrypted public key/certificate.
Client checks the certificate, creates and sends an encrypted key back to the server
(If the certificate is not ok, the communication fails)
Server decrypts the key and delivers encrypted content with key to the client
Client decrypts the content completing the SSL/TLS *handshake*

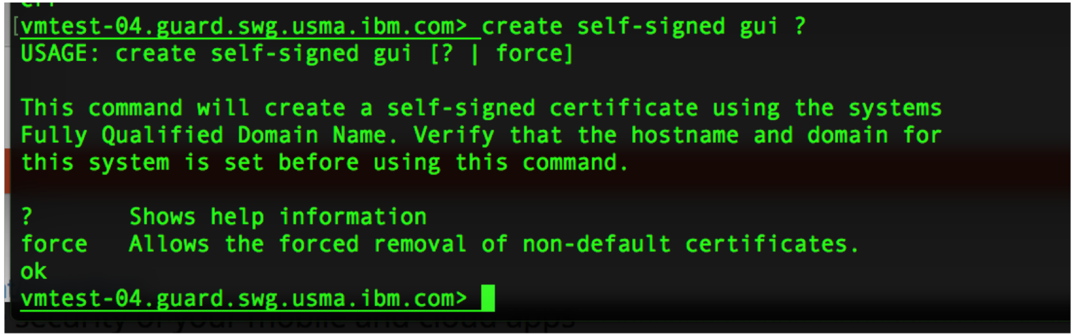
* From: https://www.entrustdatacard.com/pages/ssl

Hostname certificate verification in Guardium

- In 10.6,hostname certificate verification is disabled by default
- In 10.6, a GRDAPI command has been provided to enable enforcement of hostname verification
  - grdapi set_certificate_host_validation enable=[true|false]
- When enabled, the certificate **must** have the name used in the URL string in one of either the CN or SAN locations. Otherwise, communication will not be established

Self-Signed Certificate auto-regeneration

- Previously, we saw how to generate CSR's with SAN entries and get signed or self-signed certifcates for use in the Guardium appliance.
- In 10.6 certificate regeneration can be done for hostname changes. This allows CM/MU communications to continue even if the Customer does not want to obtain their own certificates.
  - Upon a hostname or domain name change, the system will check to see if the default Guardium self-signed certificate is installed. If it is the default self-signed certificate, the system will automatically regenerate the certificate using the Fully Qualified Domain Name of the appliance in both the CN and the First SAN slot. Otherwise, the system will not change any certificate
  - The customer may choose to manually create a self-signed certificate using the following commands:
    - CLI> create self-signed gui [force]



```
vmtest-04.guard.swg.usma.ibm.com> create self-signed gui ?
USAGE: create self-signed gui [? | force]

This command will create a self-signed certificate using the systems
Fully Qualified Domain Name. Verify that the hostname and domain for
this system is set before using this command.

?       Shows help information
force   Allows the forced removal of non-default certificates.
ok
vmtest-04.guard.swg.usma.ibm.com> 
```

IBM Security

MySQL CIS Benchmarks

MySQL 5.6 & 5.7 CIS Benchmark version 1.0 & 1.1

VA supports CIS's latest MySQL 5.6&5.7 benchmark version 1.0 & 1.1 in v10.6.

- All existing tests that reference CIS had their external references updated to this benchmark.
- There are 40 new query based tests that will be introduced and will be available as of 2018 Q4 DPS.
- MySQL 8.0 is NOT OFFICIALLY supported, however it is partially supported for the features that have not been deprecated from previous version (5.6.x & 5.7.x).

- To download the CIS benchmark, use the following URL:

https://www.cisecurity.org/cis-benchmarks/

MySQL 5.6 and 5.7 CIS Tests

New CIS Tests for MySQL 5.6 & 5.7 query based tests

TEST ID	TEST NAME
2649	Ensure the Test Database Is Not Installed
2650	Ensure the daemon_memcached Plugin Is Disabled
2651	Ensure --skip-symbolic-links Is Enabled
2652	Ensure secure_file_priv Is Not Empty
2653	Ensure Only Administrative Users Have Full Database Access - user Table
2654	Ensure sql_mode Contains STRICT_ALL_TABLES
2655	Ensure Only Administrative Users Have Full Database Access - db Table
2656	Ensure file_priv Is Not Set to Y for Non-Administrative Users
2657	Ensure super_priv Is Not Set to Y for Non-Administrative Users
2658	Ensure process_priv Is Not Set to Y for Non-Administrative Users
2659	Ensure shutdown_priv Is Not Set to Y for Non-Administrative Users
2660	Ensure create_user_priv Is Not Set to Y for Non-Administrative Users
2661	Ensure grant_priv Is Not Set to Y for Non-Administrative Users - user Table
2662	Ensure grant_priv Is Not Set to Y for Non-Administrative Users - db Table
2663	Ensure repl_slave_priv Is Not Set to Y for Non-Slave Users

MySQL 5.6 and 5.7 CIS Tests

New CIS Tests for MySQL 5.6 & 5.7 query based tests

TEST ID	TEST NAME
2664	Ensure DML/DDL Grants Are Limited to Specific Databases and Users
2665	Ensure log_error Is Not Empty
2666	Ensure log_warnings Is Set to 2 or Higher
2667	Ensure log_error_verbosity Is Set to 2 or Higher
2668	Ensure audit_log_connection_policy Is Not Set to NONE
2669	Ensure audit_log_exclude_accounts Is Set to NULL
2670	Ensure audit_log_include_accounts Is Set to NULL
2671	Ensure audit_log_policy Is Set to Log Logins and Connections
2672	Ensure audit_log_statement_policy Is Set to ALL
2673	Set audit_log_strategy to SYNCHRONOUS or SEMISYNCRONOUS
2674	Ensure the Audit Plugin Can Not be Unloaded
2675	Ensure sql_mode Contains NO_AUTO_CREATE_USER

MySQL 5.6 and 5.7 CIS Tests

New CIS Tests for MySQL 5.6 & 5.7 query based tests

```
TEST ID    TEST NAME
---------- ----------------------------------------------------------
2676       Ensure validate_password Plugin is Installed
2677       Ensure validate_password Plugin is Loaded at Startup
2678       Password Policy validate_password_length
2679       Password Policy validate_password_mixed_case_count
2680       Password Policy validate_password_number_count
2681       Password Policy validate_password_special_char_count
2682       Password Policy validate_password_policy
2683       Users With Password Identical To Username - MySQL 5.6
2684       Users With Password Identical To Username - MySQL 5.7 and Above
2685       Ensure No Users Have Wildcard Hostnames
2686       Ensure master_info_repository Is Set to TABLE
2687       Ensure super_priv Is Not Set to Y for Replication Users
2688       Ensure No Replication Users Have Wildcard Hostnames
```

IBM Security

Oracle 18c VA

IBM

VA on Oracle18c

VA scan for Oracle 18c

- Guardium 10.6 supports the scanning of Oracle 18c on the Oracle cloud and on premise.
- All functionality of the VA scan for 18c is supported except for CVE and patch tests.
- CVE and patch tests for Oracle 18c will be a feature for the future 10.7 release.
- Guardium 10.6 also supports datasource connections with SSL with server signed and mutual authentication.
- You can initiate an SSL connection using either the Datadirect or Oracle JDBC driver.

Oracle VA test enhancements

The following Oracle VA tests were enhanced to support Oracle 18c:

- The enhancements include: excluding default Oracle 18c grantees, short description and remediation text. The idea is to make these tests friendly to Oracle 18c and supporting previous Oracle releases as well.

Test ID 222, Only DBA Access To SYS.USER$
Test ID 31, GLOBAL_NAMES Is True
Test ID 27, OS_AUTHENT_PREFIX Is Not OPS$
Test ID 24, Access To The Selected Packages is restricted (**Not relevant to 18c scan**)
Test ID 29, UTL_FILE_DIR Should Not Point To Sensitive Directories (**Not relevant to 18c scan**)
Test ID 172, No authorization to BECOME USER Or ALTER USER Privileges
Test ID 2567, Oracle application administration roles enablement
Test ID 2378, No Authorization To DBA Role
Test ID 2019, Administrative privilege assignment
Test ID 2021, No PUBLIC access to critical packages
Test ID 2369, No Authorization To System SELECT ANY DICTIONARY Privilege
Test ID 2371, No Authorization To EXEMPT ACCESS POLICY Privilege

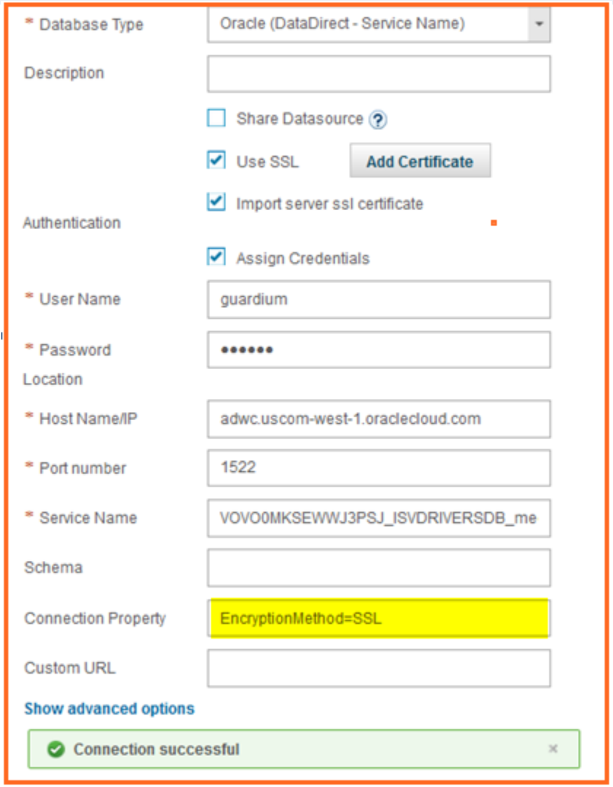
Oracle Datasource using SSL

Connecting Oracle with the SSL protocol using the DataDirect driver:

- Check the following in the datasource setup: Use SSL, check Import server SSL certificate. Upload the .pem file for Client certificate if it is using mutual authentication.

- For DataDirect SSL, add the following to the connection property field: **EncryptionMethod=SSL**

- This is an example of a datasource connecting to Oracle ADWC – Autonomous Data Warehouse Cloud.



* Database Type	Oracle (DataDirect - Service Name)
Description	
	□ Share Datasource ?
	☑ Use SSL Add Certificate
	☑ Import server ssl certificate
Authentication	
	☑ Assign Credentials
* User Name	guardium
* Password	••••••
Location	
* Host Name/IP	adwc.uscom-west-1.oraclecloud.com
* Port number	1522
* Service Name	VOVO0MKSEWWJ3PSJ_ISVDRIVERSDB_me
Schema	
Connection Property	EncryptionMethod=SSL
Custom URL	

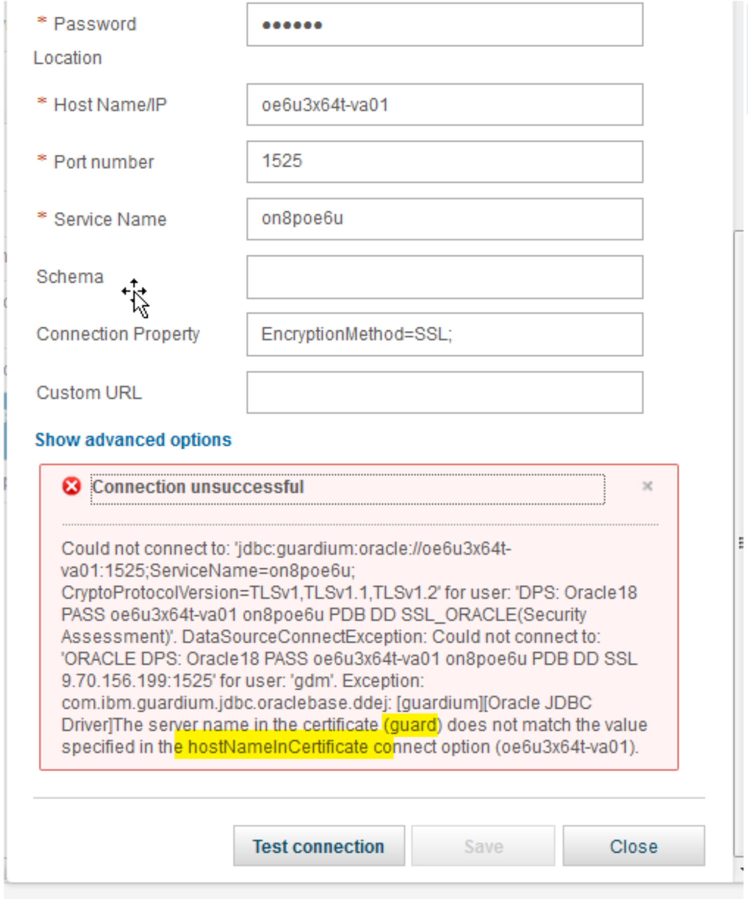
Show advanced options

Connection successful

Oracle Datasource using SSL

Troubleshooting the DataDirect Driver:

- When using the DataDirect SSL, when you get this error message, it complains the HostNameInCertificate doesn't match. It gives you the cert name in (). Just add the following parameter to the connection property using the certificate provided: HostNameInCertificate=guard
- From:
  - EncryptionMethod=SSL;
- To:
  - EncryptionMethod=SSL;HostNameInCertificate=guard



* Password	••••••
Location	
* Host Name/IP	oe6u3x64t-va01
* Port number	1525
* Service Name	on8poe6u
Schema	
Connection Property	EncryptionMethod=SSL;
Custom URL	

Connection unsuccessful

```
Could not connect to: 'jdbc:guardium:oracle://oe6u3x64t-
va01:1525;ServiceName=on8poe6u;
CryptoProtocolVersion=TLSv1,TLSv1.1,TLSv1.2' for user: 'DPS: Oracle18
PASS oe6u3x64t-va01 on8poe6u PDB DD SSL_ORACLE(Security
Assessment)'. DataSourceConnectException: Could not connect to:
'ORACLE DPS: Oracle18 PASS oe6u3x64t-va01 on8poe6u PDB DD SSL
9.70.156.199:1525' for user: 'gdm'. Exception:
com.ibm.guardium.jdbc.oraclebase.ddej: [guardium][Oracle JDBC
Driver]The server name in the certificate (guard) does not match the value
specified in the hostNameInCertificate connect option (oe6u3x64t-va01).
```

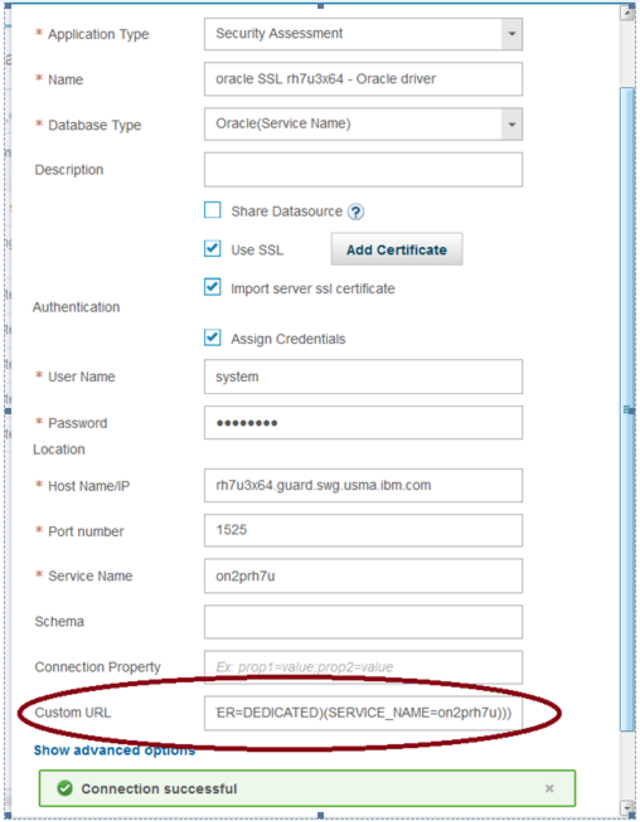
Oracle Datasource using SSL

SSL Using the Oracle JDBC Driver.

- Check the following in the datasource setup: Use SSL, check Import server SSL certificate. Upload the .pem file for Client certificate if it is using mutual authentication.
- Refer to the Oracle JDBC connection syntax.
- URL Example with a Service name:
  - jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCPS)(HOST=rh7u3x64.guard.swg.usma.ibm.com)(PORT=1525)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=on2prh7u)))
  - jdbc:oracle:thin:@(description= (address=(protocol=tcps)(port=1522)(host=adwc.uscom-west-1.oraclecloud.com))(connect_data=(service_name=VOVO0MKSEWWJ3PSJ_ISVDRIVERSDB_medium.dwcs.oracle.com))(security=(ssl_server_cert_dn="CN=adwc-dev.uscom-east-1.oraclecloud.com,OU=Testing Domain,O=End Point,L=Redwood Shores,ST=California,C=US")))
- URL Example with a SID:
  - jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCPS)(HOST=rh7u3x64.guard.swg.usma.ibm.com)(PORT=1525)))(CONNECT_DATA=(SERVER=DEDICATED)(SID=on2crh7u)))

Oracle Datasource using SSL

SSL Using the Oracle JDBC Driver:



* Application Type	Security Assessment
* Name	oracle SSL rh7u3x64 - Oracle driver
* Database Type	Oracle(Service Name)
Description	
	□ Share Datasource
	☑ Use SSL
	☑ Import server ssl certificate
Authentication	
	☑ Assign Credentials
* User Name	system
* Password	●●●●●●●●●
Location	
* Host Name/IP	rh7u3x64.guard.swg.usma.ibm.com
* Port number	1525
* Service Name	on2prh7u
Schema	
Connection Property	Ex: prop1=value;prop2=value
Custom URL	ER=DEDICATED)(SERVICE_NAME=on2prh7u)))

Connection successful

IBM Security

Multi threading VA

Multi-Threading Overview

What is new:

- Versions before 10.6 are single threaded
  - Jobs (Classification/Assessment) are serialized, only one running at a time.
- 10.6 supports Multi-Threading (MT)
  - Jobs can run in parallel, only limited by the CPU cores (1<= N <=2* #CPU_Core and N<=100)
- Performance improvement
  - Execution time greatly reduced

How to setup MT (Multi-Threading)

Steps

- Find your system CPU cores

  - nproc or put any number, the system will not allow you to go over the limit.

- Find the current system setting (default limit =1)

  - grdapi get_job_process_concurrency_limit

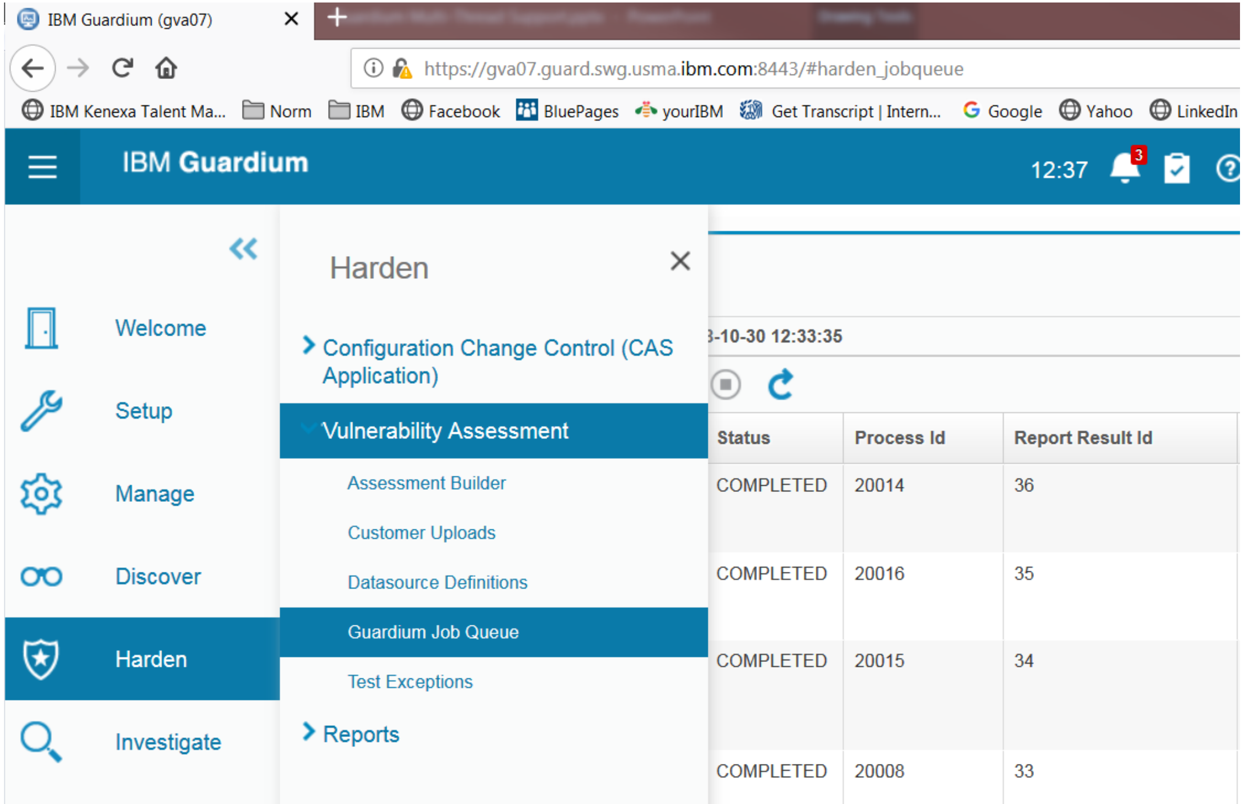
- Set MT

```
grdapi set_job_process_concurrency_limit limit=8
```

- Check the new setting

```
grdapi get_job_process_concurrency_limit
```

Monitor the Job queue via the GUI:



3-10-30 12:33:35

Status	Process Id	Report Result Id
COMPLETED	20014	36
COMPLETED	20016	35
COMPLETED	20015	34
COMPLETED	20008	33

Special in 10.x

- MT was initially implemented only for Classification
  - grdapi set_classification_concurrency_limit limit=n
  - grdapi get_classficiation_concurrency_limit

- Now it is changed to support BOTH classification and assessment combined:

  - grdapi get_job_process_concurrency_limit

  - grdapi set_job_process_concurrency_limit limit=N

IBM Security

DB2 v10.5 LUW STIG V1R1

DB2 v10.5 LUW STIG

VA now supports STIG's latest DB2 10.5 benchmark version 1, release 1.

- All existing tests that reference STIG had their external references updated to this benchmark.
- To download the STIG benchmark, use the following URL:
  - https://iase.disa.mil/stigs/app-security/database/Pages/index.aspx
- Customers should apply the latest gdmmonitor-db2.sql script to run DB2 LUW VA as there are additional privileges required to execute the new tests.
- There are twenty eight new query based tests that have been introduced and already available as of the 2018 Q2 DPS.
- There are three new CAS tests that will be released in 10.6.
- The 10.6 CAS agent will need to be installed to utilize the new CAS tests.

DB2 v10.5 LUW STIG

New STIG Tests for DB2 LUW Query based tests

TEST ID	TEST NAME
2621	Access To External Executables Must Be Restricted
2622	Audit Policy CHECKING Category
2623	Audit Policy CONTEXT Category
2624	Is Audit Policy ERRORTYPE Set to A
2625	Audit Policy EXECUTE Category
2626	Audit Policy EXECUTEWITHDATA is Enabled
2627	Audit Policy OBJMAINT Category
2628	Audit Policy SECMAINT Category
2629	Audit Policy SYSADMIN Category
2630	Audit Policy VALIDATE Category
2631	Audit On System Catalog Authority objects
2632	CONNECT_PROC is Defined
2633	Audit Routine Execute Privileges
2634	Routine Ownership
2635	Package Ownership
2636	Module Ownership

DB2 v10.5 LUW STIG

New STIG Tests for DB2 LUW Query based tests

TEST ID	TEST NAME
2637	Trigger Ownership
2638	Tablespace Ownership
2639	Table Ownership
2640	Schema Authority
2641	Session Termination Threshold
2642	SSL_CIPHERSPECS is Defined
2643	SSL_SVR_LABEL is Defined
2644	SSL_VERSIONS is Defined
2645	Is Database Native Encryption enabled
2646	No Sample Database
2647	DB2 Communication Protocol SSL
2648	Password Encryption

DB2 v10.5 LUW STIG

New STIG Tests for DB2 LUW CAS based tests

TEST ID	TEST NAME
570	Audit Data Path Permission
571	Log System Administrator Events
572	Log System Administrator Events - Windows

IBM Security

DB2 z/OS Enhancements

DB2 z/OS

VA now supports DB2 z/OS v12.

- The Guardium 10.6 release uses the latest DB2 JDBC driver.
- DB2 z/OS v12 has been added to the VA support matrix.
- There are two DB2 z/OS test enhancements:
  - Test ID 360, AUTHCACH subsystem parameter is set properly
  - Test ID 2166, z/OS Restrict system privilege - SYSOPRAUTH

DB2 z/OS Security APAR Tests

The DB2 z/OS security team required we mask our test description, recommendation, and APAR identifiers. We will be using a SIA number instead of an APAR ID.

- These changes apply to both v9 and v10 as security APAR tests are supported in Guardium v9. There will be a patch for v9 right around the 10.6 release time. This will include a patch as well as the DPS. Most likely this will happen during the 2018 Q4 DPS release which is 11/15/2018.

- We are deprecating all APAR tests that were enforced for DB2 v8.1 and v9.1. The current APAR tests will enforce DB2 v10.1, 11.1 and 12.1

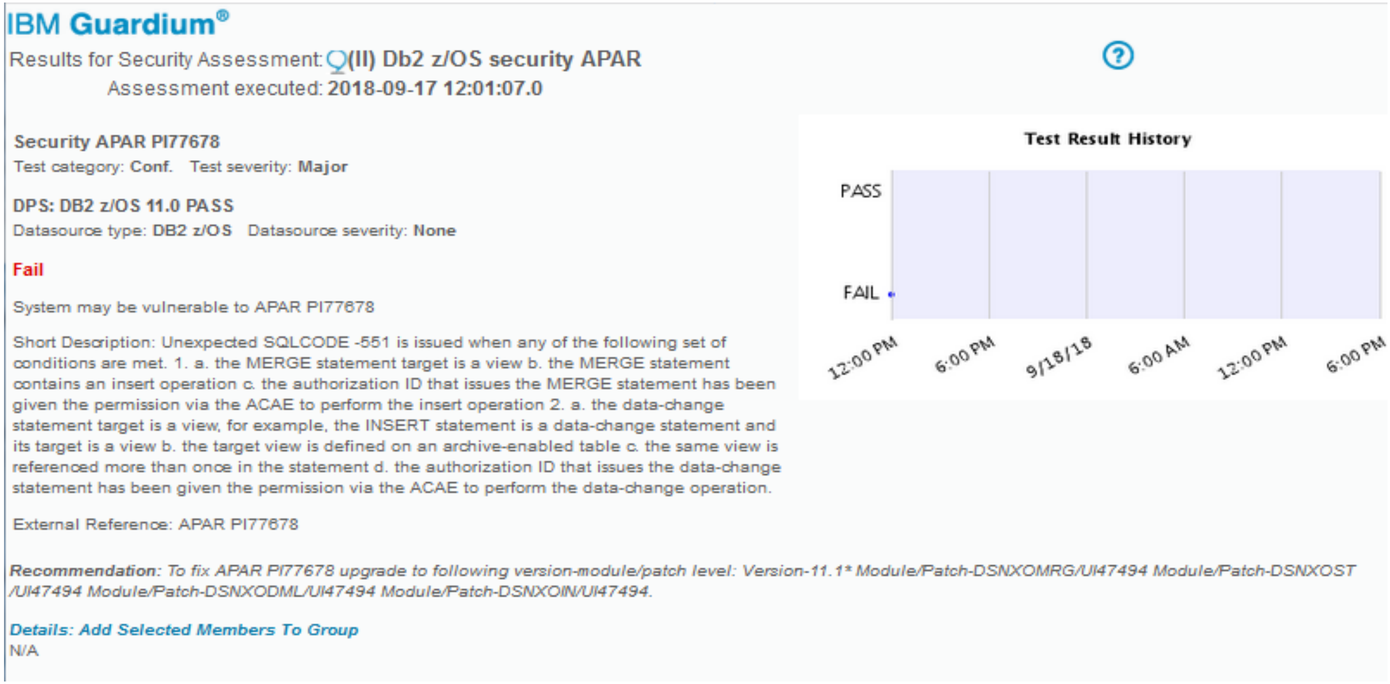
- All APAR tests that are not deprecated will now use a SIA number. Customers will use this information in the DB2 z/OS security portal and eventually find the APAR ID, description and remediation details.

- All short descriptions for the APAR tests will use the following same text: "Possible security vulnerability in DB2 for z/OS".

- All recommendations for the APAR tests will use the following same recommendation: "To fix SIA-DB2-2017.7-1 go to the IBM Z Security Portal, check the z/OS and z/VM SIA Cross Reference record for Guardium APAR information and apply all outstanding fixes. If you are not registered for access to the IBM Z Security Portal, please see https://www.ibm.com/it-infrastructure/z/capabilities/system-integrity"

DB2 z/OS Security APAR Tests

– Before the 10.6 changes:



IBM Guardium®

Results for Security Assessment: (II) Db2 z/OS security APAR

Assessment executed: **2018-09-17 12:01:07.0**

Security APAR PI77678

Test category: **Conf.** Test severity: **Major**

DPS: DB2 z/OS 11.0 PASS

Datasource type: **DB2 z/OS** Datasource severity: **None**

Fail

System may be vulnerable to APAR PI77678

Short Description: Unexpected SQLCODE -551 is issued when any of the following set of conditions are met. 1. a. the MERGE statement target is a view b. the MERGE statement contains an insert operation c. the authorization ID that issues the MERGE statement has been given the permission via the ACAE to perform the insert operation 2. a. the data-change statement target is a view, for example, the INSERT statement is a data-change statement and its target is a view b. the target view is defined on an archive-enabled table c. the same view is referenced more than once in the statement d. the authorization ID that issues the data-change statement has been given the permission via the ACAE to perform the data-change operation.

External Reference: APAR PI77678

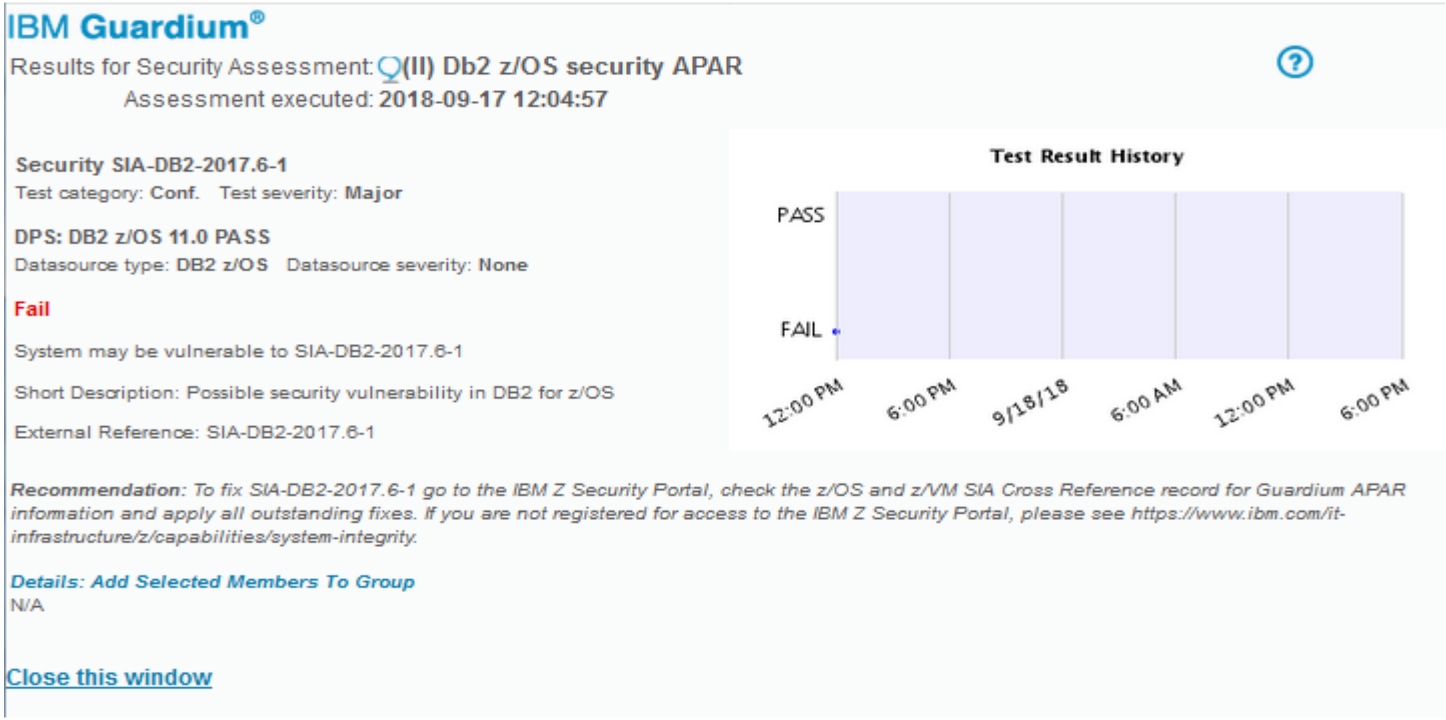
***Recommendation:** To fix APAR PI77678 upgrade to following version-module/patch level: Version-11.1* Module/Patch-DSNXOMRG/UI47494 Module/Patch-DSNXOST /UI47494 Module/Patch-DSNXODML/UI47494 Module/Patch-DSNXOIN/UI47494.*

Details: Add Selected Members To Group

N/A

DB2 z/OS Security APAR Tests

– After the 10.6 changes:



IBM Guardium®

Results for Security Assessment: (II) Db2 z/OS security APAR

Assessment executed: 2018-09-17 12:04:57

Security SIA-DB2-2017.6-1

Test category: **Conf.** Test severity: **Major**

DPS: DB2 z/OS 11.0 PASS

Datasource type: **DB2 z/OS** Datasource severity: **None**

Fail

System may be vulnerable to SIA-DB2-2017.6-1

Short Description: Possible security vulnerability in DB2 for z/OS

External Reference: SIA-DB2-2017.6-1

Recommendation: To fix SIA-DB2-2017.6-1 go to the IBM Z Security Portal, check the z/OS and z/VM SIA Cross Reference record for Guardium APAR information and apply all outstanding fixes. If you are not registered for access to the IBM Z Security Portal, please see https://www.ibm.com/it-infrastructure/z/capabilities/system-integrity.

Details: Add Selected Members To Group

N/A

Close this window

IBM Security

Outlier enhancements

IBM

Agenda

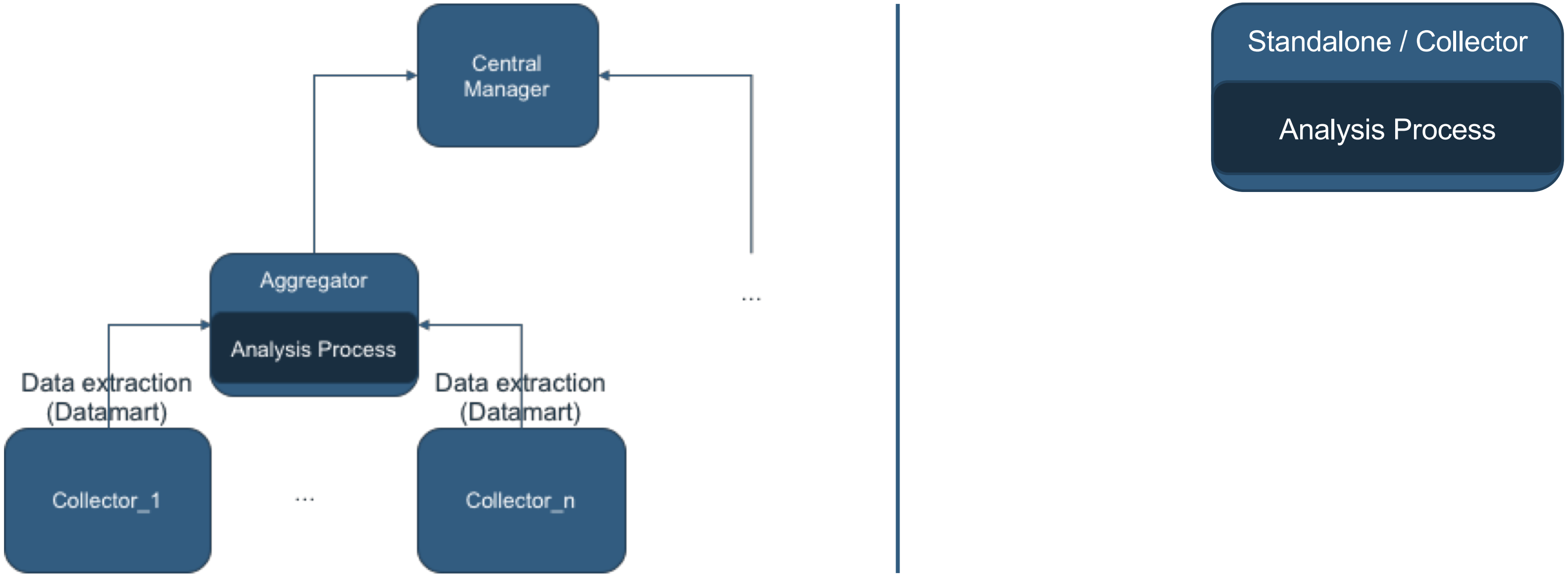
- Outliers detection API improvements.

- Outliers detection cross-cm support.
  - Architecture.
  - Implementation considerations.
  - Troubleshooting.

- Outliers mining status cross-cm support.

- Q&A

Outliers detection – Current architecture



Central Manager

Aggregator

Analysis Process

Data extraction (Datamart)

Data extraction (Datamart)

Collector_1

...

Collector_n

...

Standalone / Collector

Analysis Process

Outliers detection – Current API

User has two APIs to enable outliers:

- grdapi enable_outliers_detection_agg
  Parameters:
  - **aggregator_host_name**
  - **schedule_interval (NOT USED)**
  - **schedule_units (NOT USED)**
  - schedule_start
  - extraction_start
  - DAM / FAM (Default: DAM)

- grdapi enable_outliers_detection
  Parameters:
  - **schedule_interval (NOT USED)**
  - **schedule_units (NOT USED)**
  - schedule_start
  - extraction_start
  - DAM / FAM (Default: DAM)
  - api_target_host

Outliers detection – New API

grdapi enable_outliers_detection

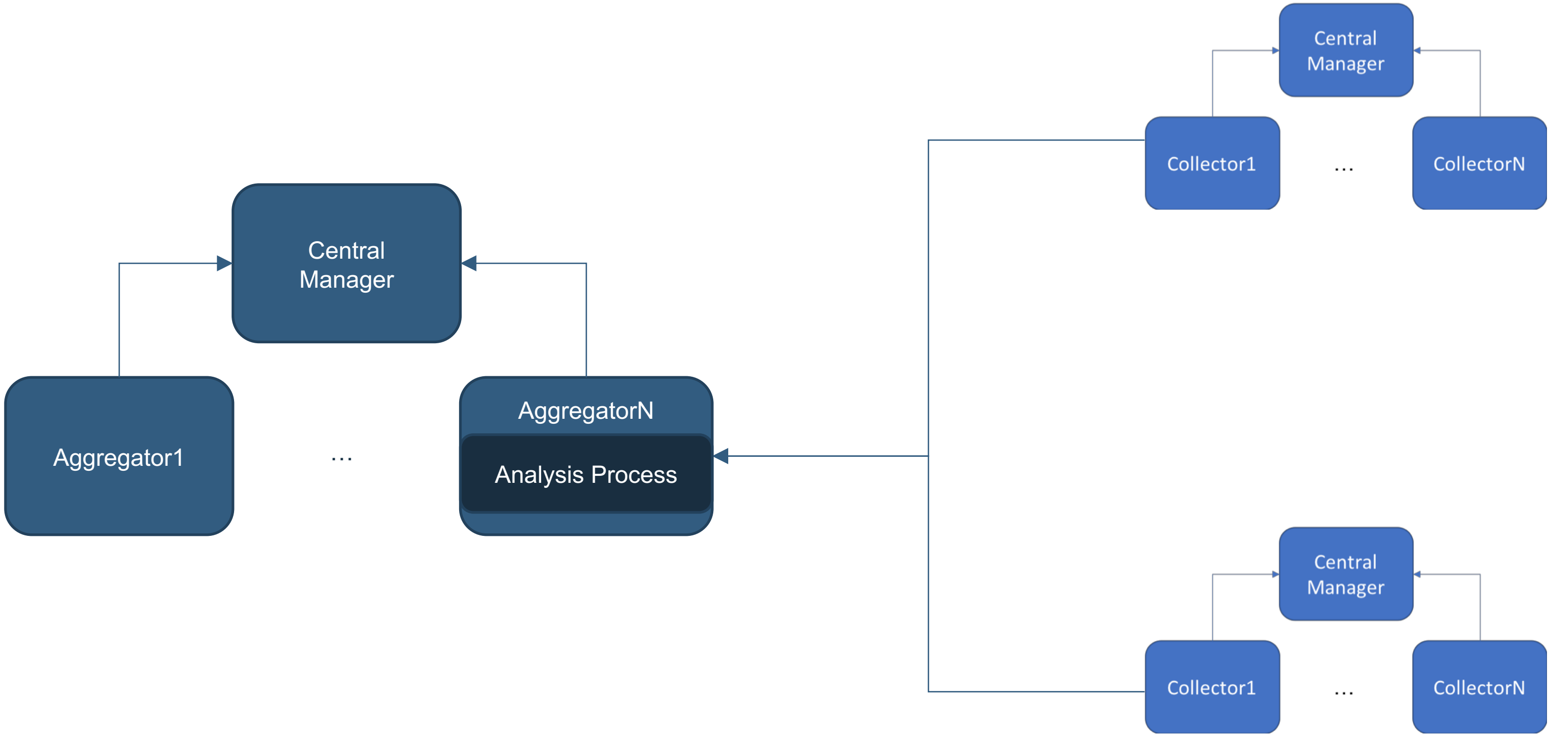
Parameters:

- managed_units_hostnames
- group_descriptions
- schedule_interval (Not used)
- schedule_units (Not used)
- schedule_start
- extraction_start
- DAM / FAM (Default: DAM)
- api_target_host

Key changes:

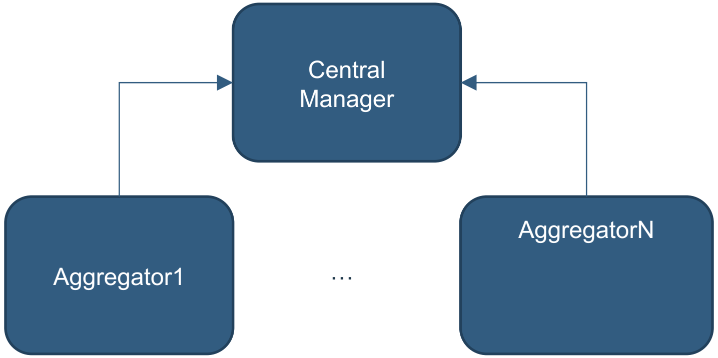
1. Nothing is mandatory.
2. If no managed units are inserted, will enable on all the environment.
3. If running on collector will act the same as the old API.
4. if running on aggregator will act the same as enable_outliers_detection_agg

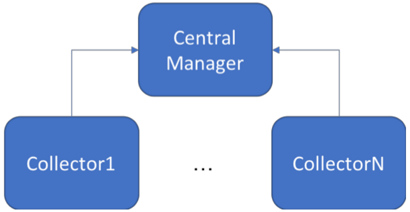
Cross CM Architecture

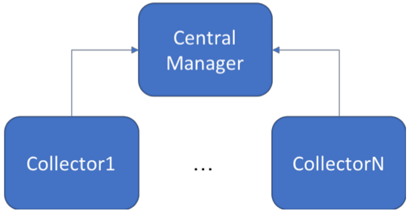


Steps to enable:

Outliers – Current architecture

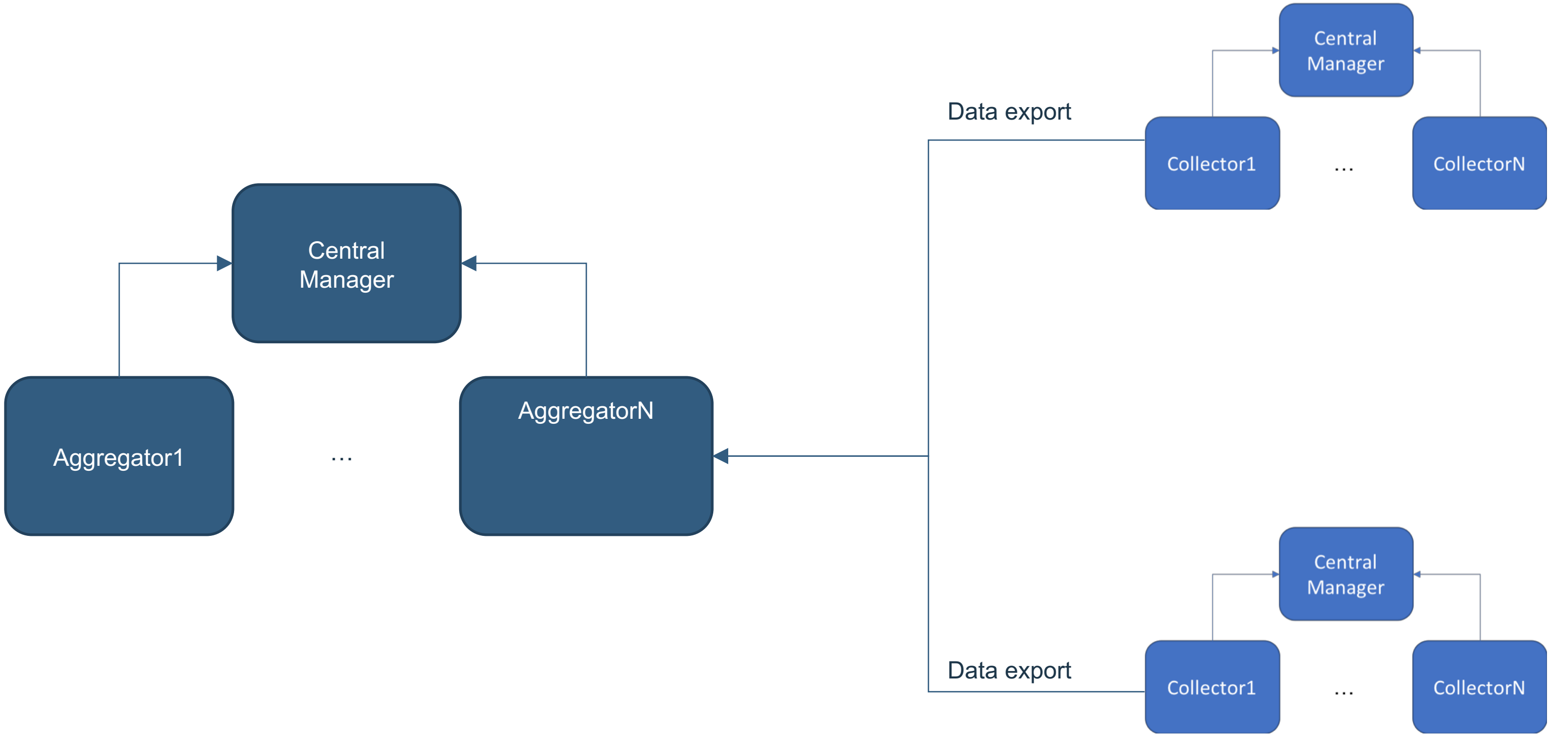






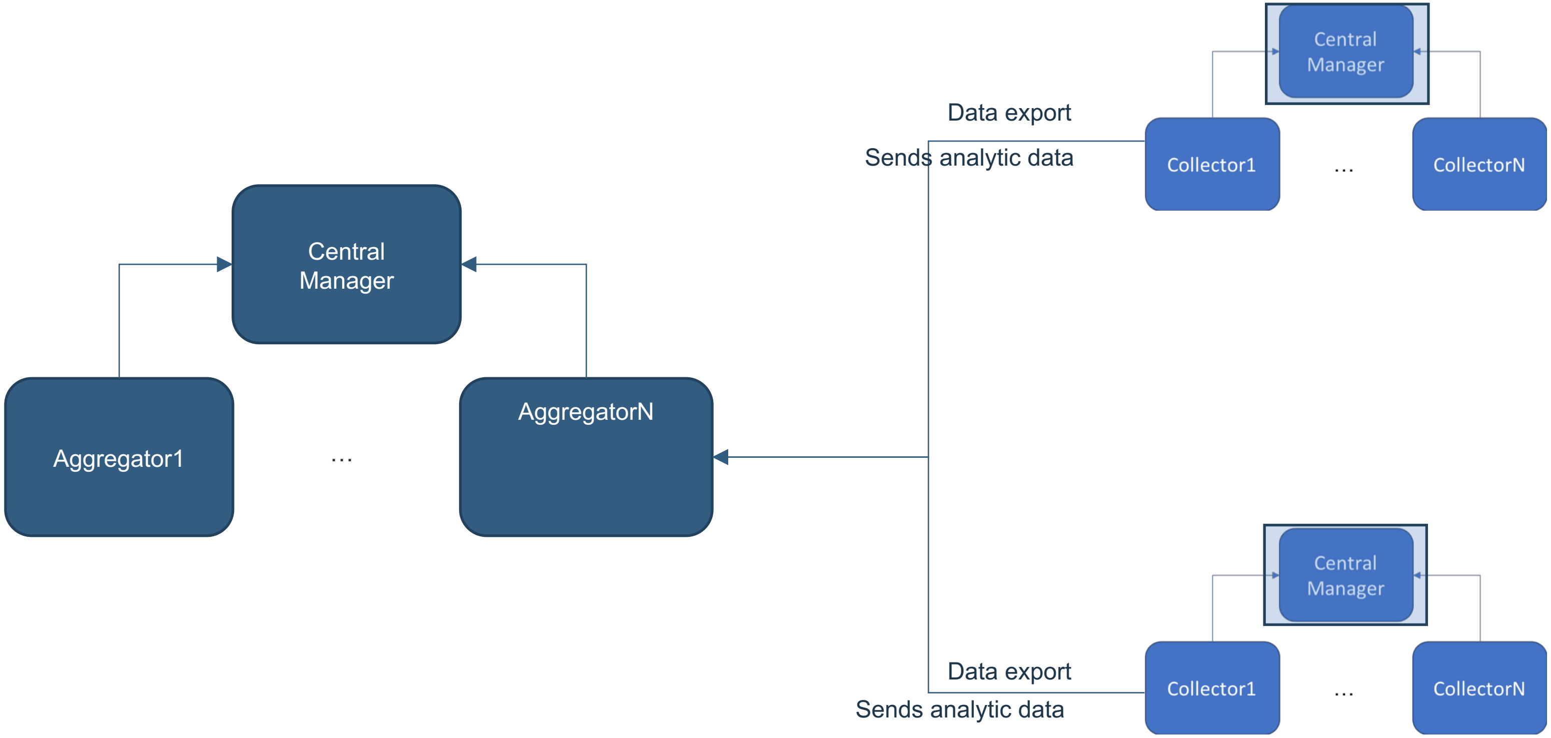
Steps to enable:

1. Set **Data export** target to be an aggregator from another CM.



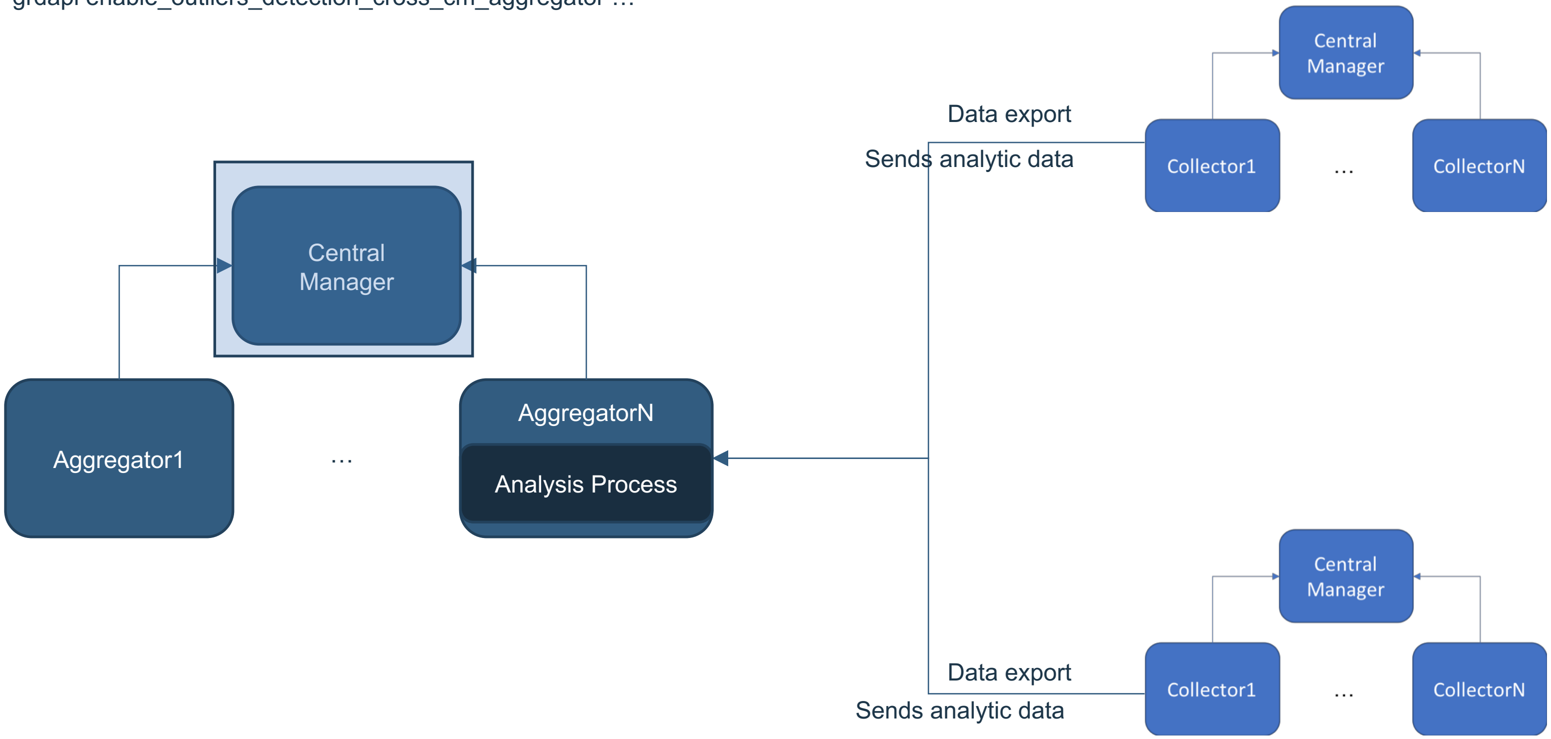
Steps to enable:

1. Set **Data export** target to be an aggregator from another CM.
2. grdapi enable_outliers_detection_cross_cm_collectors …



Steps to enable:

1. Set **Data export** target to be an aggregator from another CM.
2. grdapi enable_outliers_detection_cross_cm_collectors …
3. grdapi enable_outliers_detection_cross_cm_aggregator …



Outliers detection – Newly added APIs

User has two APIs to enable outliers:

- grdapi enable_outliers_detection_cross_cm_agg
  Parameters:
  - **aggregator_host_name**

- grdapi enable_outliers_detection_cross_cm_collector
  Parameters:
  - **collector_host_names**

Outliers detection – New API

grdapi enable_outliers_detection

Parameters:

- managed_units_hostnames
- group_descriptions
- schedule_interval (Not used)
- schedule_units (Not used)
- schedule_start
- extraction_start
- DAM / FAM (Default: DAM)
- api_target_host

Key changes:

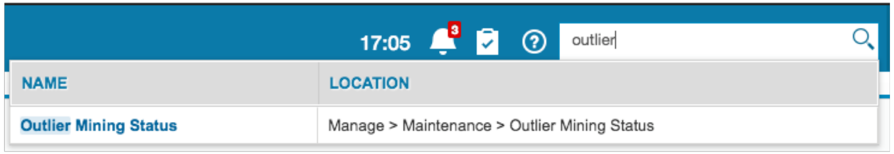
...

5. Fully supports cross CM.

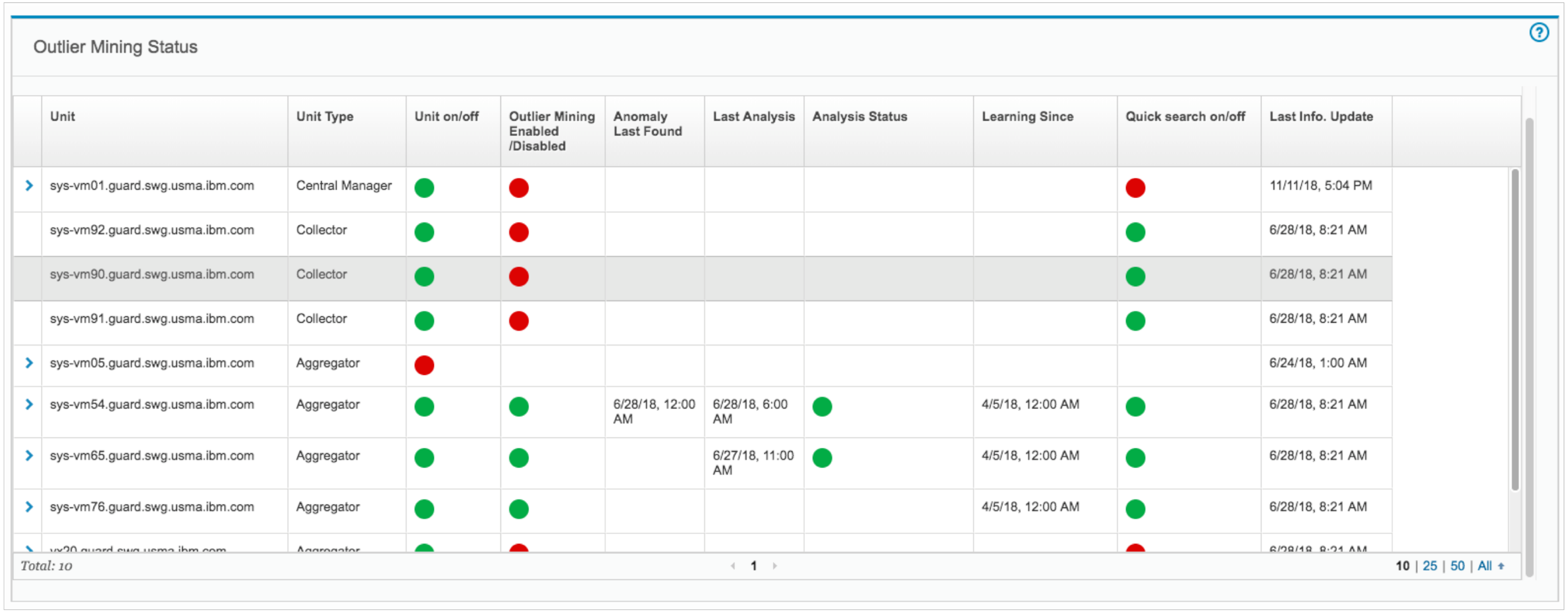
   Collector that exports data to an aggregator not within the environment will be considered cross cm collector.

   Aggregator that receives data from collectors not within the environment is considered cross cm aggregator.

Outlier mining status



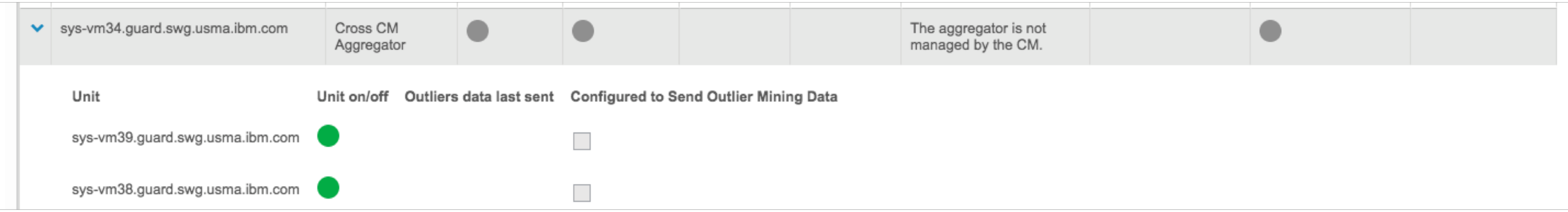
NAME	LOCATION
Outlier Mining Status	Manage > Maintenance > Outlier Mining Status


Outlier Mining Status

	Unit	Unit Type	Unit on/off	Outlier Mining Enabled /Disabled	Anomaly Last Found	Last Analysis	Analysis Status	Learning Since	Quick search on/off	Last Info. Update
›	sys-vm01.guard.swg.usma.ibm.com	Central Manager	🟢	🔴					🔴	11/11/18, 5:04 PM
	sys-vm92.guard.swg.usma.ibm.com	Collector	🟢	🔴					🟢	6/28/18, 8:21 AM
	sys-vm90.guard.swg.usma.ibm.com	Collector	🟢	🔴					🟢	6/28/18, 8:21 AM
	sys-vm91.guard.swg.usma.ibm.com	Collector	🟢	🔴					🟢	6/28/18, 8:21 AM
›	sys-vm05.guard.swg.usma.ibm.com	Aggregator	🔴							6/24/18, 1:00 AM
›	sys-vm54.guard.swg.usma.ibm.com	Aggregator	🟢	🟢	6/28/18, 12:00 AM	6/28/18, 6:00 AM	🟢	4/5/18, 12:00 AM	🟢	6/28/18, 8:21 AM
›	sys-vm65.guard.swg.usma.ibm.com	Aggregator	🟢	🟢		6/27/18, 11:00 AM	🟢	4/5/18, 12:00 AM	🟢	6/28/18, 8:21 AM
›	sys-vm76.guard.swg.usma.ibm.com	Aggregator	🟢	🟢				4/5/18, 12:00 AM	🟢	6/28/18, 8:21 AM
›	vx20.guard.swg.usma.ibm.com	Aggregator	🟢	🔴					🔴	6/28/18, 8:21 AM

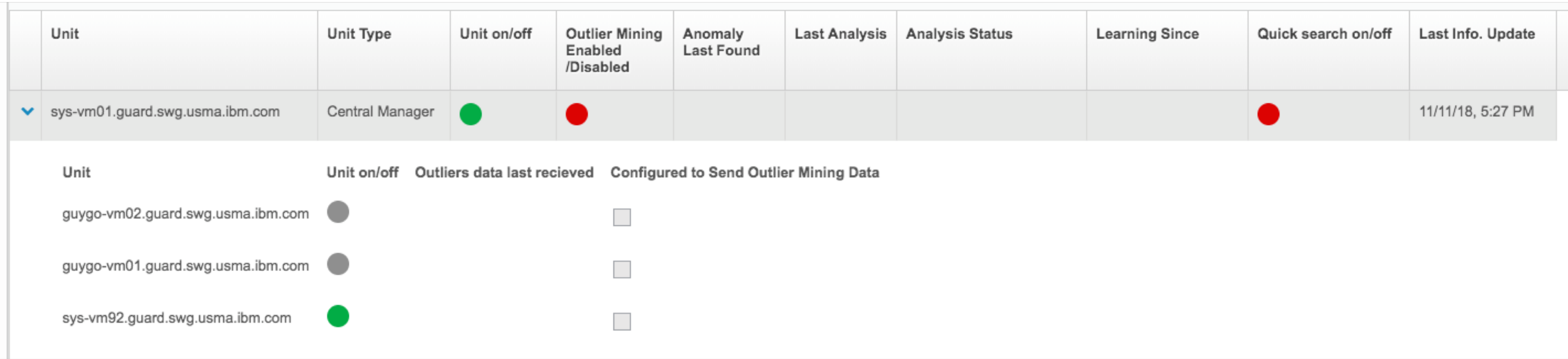
Total: 10 ‹ 1 › 10 | 25 | 50 | All

Outlier mining status – Cross CM



⌄	sys-vm34.guard.swg.usma.ibm.com	Cross CM Aggregator	●	●			The aggregator is not managed by the CM.		●

Unit	Unit on/off	Outliers data last sent	Configured to Send Outlier Mining Data
sys-vm39.guard.swg.usma.ibm.com	🟢		□
sys-vm38.guard.swg.usma.ibm.com	🟢		□



	Unit	Unit Type	Unit on/off	Outlier Mining Enabled /Disabled	Anomaly Last Found	Last Analysis	Analysis Status	Learning Since	Quick search on/off	Last Info. Update
⌄	sys-vm01.guard.swg.usma.ibm.com	Central Manager	🟢	🔴					🔴	11/11/18, 5:27 PM

Unit	Unit on/off	Outliers data last recieved	Configured to Send Outlier Mining Data
guygo-vm02.guard.swg.usma.ibm.com	●		□
guygo-vm01.guard.swg.usma.ibm.com	●		□
sys-vm92.guard.swg.usma.ibm.com	🟢		□

Limitations:

- **Outliers enablement is still prune to architecture changes.**
  E.g: Adding a managed unit under an aggregator with outliers on will not automatically set the relevant meta-data for the collector.

- **(enable/disable)_outliers_detection is still not append-able API.**

- **Analysis status is not yet as accurate as we want it to.**
  If the internal analysis process has failed, we will not be able to see it through the screen.

- **Cross-CM Analysis status requires two views to get maximum visibility.**