

What's new in Guardium 11.0

Backup Slides

Shay Harel – Director of Engineering / Data Security

June 2019

Notices and disclaimers

- © 2019 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.
- .

Guardium V11 New Release Training

—
v11.0 Upgrade

Contents

Overview

Use cases

Prior to Upgrade

Upgrade Information

Upgrade Process

Upgrade Speed

Upgrade considerations and limitations

Known Issues

Troubleshooting

Q & A

Overview

The v11.0 Upgrade is a daunting task simply because of what it is going to accomplish. The upgrade is similar in process as the v9 to v10 upgrade.

The upgrade process will start on the v10 side by saving essential information, files, and data. The upgrade will then boot into a Custom installer that will install RedHat 7. Finally, the upgrade will restore the saved information, files, and data and then start operation as a Guardium v11.0 system.

What's New

- The system is based on RedHat 7.6

Benefits

- Ability to push upgrades in a CM/MU environment
- Uses newer version of GCC to support advanced features
- Ability to receive Security fixes from RedHat

Use Cases

Upgrade Guardium v10.1.3 through v10.6, any machine type to v11.0

Upgrading to v11 uses the standard Top Down procedure for a CM/MU environment, utilizing the same workflow as other Guardium Patches, GPUs, or Bundles.

Central Manager

Aggregator Managed Units

Collector Managed Units

Agents

Prior to Upgrade – BCS and DR

Although it is expected the upgrade to perform smoothly and error free, Customers, Business Partners, and users of Guardium software should have a planned and tested Business Continuity Strategy and Disaster Recover plan in place that includes a robust and tested backup and recovery process.

Before any upgrade, a tested backup of the system should be taken and located separate from the appliance to be upgraded.

Prior to Upgrade

Physical systems

Customer should upgrade their firmware to the latest versions provided by their vendor. Customers with Guardium Appliances should check on FixCentral for the latest firmware for their appliance.

Any Media mounted on the physical appliance such as DVDs or USB Disks, either directly connected or through remote virtual mounting through systems such as IMM2 or iDRAC need to be unmounted prior to upgrade. Having media mounted may cause the upgrade to not complete.

Upgrade Information

Requires health Check 9997 (Date TBD)

Current ISO Build Sizes (Approximately 4.4GB):

```
4654710784 May 31 16:17 11.0.0_r106730_v11_0_1-el76-20190531_0753-DVD-auto.iso  
4654710784 May 31 16:16 11.0.0_r106730_v11_0_1-el76-20190531_0753-DVD.iso
```

Current Upgrade Size (Approximately 6GB):

```
6240825697 May 31 16:31 SqlGuard-10.0p11000_Upgrade_to_Version_11.0_May_2019.tgz.enc.sig
```

Be mindful of the sizes of the files when pushing from a CM or pushing via SCP.

Upgrade Process - standalone

```
jbelog-vm01.guard.swg.usma.ibm.com> show build
Build: 10.0
Release: 10.1.4_r102651_v10_1_4_1-el67-20171123_0009
external_r1286-20171123_0009
ID tags:
    BUILD_ID_APPLIANCE="appliance-v10_1_4-20171123_0009"
Snif version:
    BUILD_ID_CORE="core-snif_10.0p4029-20170919_1341"
    BUILD_TAG="10.5.0_r102137_snif_10.0p4029_1"
    BUILD_TIME="20170919_1340"
    BUILD_BUILD="102137"
    BUILD_MODULE="collector/snif"
    BUILD_PLATFORM="Linux_2.6.32-573.7.1.el6.x86_64"
    BUILD_NUM=102137
    BUILD_SHARED_LIB_VERSION=1.0.0
ok
jbelog-vm01.guard.swg.usma.ibm.com> show system patch available
No patch available
ok
jbelog-vm01.guard.swg.usma.ibm.com>
```

Upgrade Process - standalone ... continued

Copy files to standalone unit. In the Guardium Littleton Lab network, the Upgrade takes approximately 2 minutes to copy to the unit using scp. This is heavily dependent on network traffic and configuration.

Reminder, in a CM/MU environment, the patch is pulled in batches.

SqlGuard-10.0p11000_Upgrade_to_Version_11.0_May_2019.tgz.enc.sig	100%	5952MB	36.3MB/s	02:44
SqlGuard-10.0p9997.tgz.enc.sig	100%	40KB	40.4KB/s	00:00

Upgrade Process – standalone ... continued

show system patch available

```
jbelog-vm01.guard.swg.usma.ibm.com> show system patch available
Please wait - getting information for patch SqlGuard-10.0p11000_Upgrade_to_Version_11.0_May_2019.tgz.enc.sig
gpg: 3DES encrypted data
gpg: encrypted with 1 passphrase

gpg: WARNING: message was not integrity protected
Please wait - getting information for patch SqlGuard-10.0p9997.tgz.enc.sig
gpg: 3DES encrypted data
gpg: encrypted with 1 passphrase
gpg: WARNING: message was not integrity protected

Attempting to retrieve the patch information. It may take time. Please wait.

P#      Description                                     Version Md5sum                                     Dependencies
9997    Health Check for GPU installation (Apr 11 201 10.0 67dcb683682db202551ad16dd3312a95
11000   Upgrade to Version 11.0 (May 24 2019) 10.0 31211d19a57573e6a3f961b622ceca76 9997
ok
jbelog-vm01.guard.swg.usma.ibm.com>
```

Upgrade Process – standalone ... continued

store system patch install sys

```
Please don't forget to remove your media if necessary.
ok
[jbelog-vm01.guard.swg.usma.ibm.com> show system patch install
P#      Who      Description      Request Time      Status
230     CLI      Guardium Patch Update (GPU) for 2017-11-28 13:51:04  DONE: Patch installation Succeeded.
9997    CLI      Health Check for GPU installati 2017-11-28 15:51:31  DONE: Patch installation Succeeded.
400     CLI      Guardium Patch Update (GPU) for 2017-11-28 15:53:53  DONE: Patch installation Succeeded.
ok
[jbelog-vm01.guard.swg.usma.ibm.com> store system patch install sys

List the files in the patches directory:

1. SqlGuard-10.0p11000_Upgrade_to_Version_11.0_May_2019.tgz.enc.sig
2. SqlGuard-10.0p9997.tgz.enc.sig

Please choose patches to install (1-2, or multiple numbers separated by ",", or q to quit): 2,1
Install item 2
Patch 10.0 9997 has already installed successfully. Don't need to install it again.
Do you really want to install again (yes or no)?
yes
Install item 1
█
```

Upgrade Process – standalone ... continued

show system patch install sys

```
[jbelog-vm01.guard.swg.usma.ibm.com> show system patch install sys
```

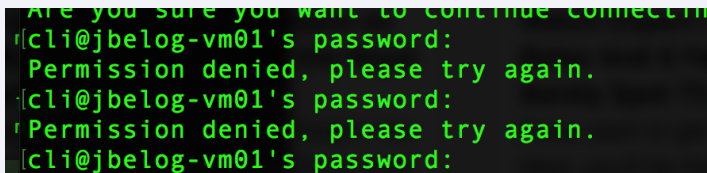
P#	Who	Description	Request Time	Status
230	CLI	Guardium Patch Update (GPU) for	2017-11-28 13:51:04	DONE: Patch installation Succeeded.
400	CLI	Guardium Patch Update (GPU) for	2017-11-28 15:53:53	DONE: Patch installation Succeeded.
9997	CLI	Health Check for GPU installati	2019-06-07 00:03:22	DONE: Patch installation Succeeded.
11000	CLI	SqlGuard-10.0p11000_Upgrade_to_	2019-06-07 00:06:22	STEP: Copy the patch file: "/var/IBM/Guardium/log/pa

```
tches/SqlGuard-10.0p11000_Upgrade_to_Ver  
ok  
[jbelog-vm01.guard.swg.usma.ibm.com>
```

Upgrade Process – standalone ... continued

Once the patch is copied, the Migrator on the v10 side copies files, data, information. The Upgrade then reboots into the upgrade mode. At this time, the system will rebuild the partitions, and if needed, creating a bios boot segment that is required for RedHat 7.

You will not be able to log into the system during this time frame as cli.

A terminal window with a black background and green text. The text shows a sequence of login attempts. The first line is partially cut off at the top. The subsequent lines show the prompt '[cli@jbelog-vm01's password:' followed by the message 'Permission denied, please try again.' This sequence is repeated three times.

```
Are you sure you want to continue connecting?  
[cli@jbelog-vm01's password:  
Permission denied, please try again.  
[cli@jbelog-vm01's password:  
Permission denied, please try again.  
[cli@jbelog-vm01's password:
```

Once this phase is completed, the system will reboot into Guardium to continue the upgrade, but now as a RedHat 7 system.

Upgrade Process – standalone ... continued

When the system reboots, you will be able to log into CLI with the previous password. The upgrade is now booted into v11. However, the upgrade has not completed.

```
IBM Guardium, Command Line Interface (CLI)

[cli@jbelog-vm01's password:
gpg-agent[17813]: directory `/home/cli/.gnupg/private-keys-v1.d' created
gpg-agent[17816]: gpg-agent (GnuPG) 2.0.22 started
The cli database login failed

Note:
The system is in the process of being upgraded, so CLI is being put into
'recovery mode' where only a limited set of commands will be available.
Please use the 'show upgrade-status' command to monitor upgrade progress.
Once you verify that upgrade is complete (Phase 5.0), please exit CLI and
log back in to enter regular CLI mode.
guard.yourcompany.com> █
```

Upgrade Process – standalone ... continued

show upgrade-status

The Error for the Missing V9MIGRATIONLOG is known, and because of the upgrade Framework dependencies, it was not removed.

```
guard.yourcompany.com> show upgrade-status
ERROR: V9MIGRATIONLOG missing
Fri Jun 7 00:29:27 UTC 2019 INFO [upgrade.ks]: GUARDIUM_V11_UPGRD_PHASEMSG:3.0:INFO:Booted onto Installation Kernel
Fri Jun 7 00:29:27 UTC 2019 INFO [upgrade.ks]: GUARDIUM_V11_UPGRD_PHASEMSG:3.1:SUCCESS:Found Migration Directory
Fri Jun 7 00:29:27 UTC 2019 INFO [upgrade.ks]: GUARDIUM_V11_UPGRD_PHASEMSG:3.2:INFO:Protecting data on /dev/sda3
Fri Jun 7 00:29:27 UTC 2019 INFO [upgrade.ks]: GUARDIUM_V11_UPGRD_PHASEMSG:3.2:INFO:Could not find old /var/tmp to remove
Fri Jun 7 00:29:27 UTC 2019 INFO [upgrade.ks]: GUARDIUM_V11_UPGRD_PHASEMSG:3.3:INFO>About to start V11 and OS Installation
Fri Jun 7 10:34:55 UTC 2019 INFO [base_upgrade_perms_fixups.sh]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.0:Start of base-upgrade-perms-fixups
Fri Jun 7 10:34:55 UTC 2019 INFO [base_upgrade_perms_fixups.sh]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.0:End of base-upgrade-perms-fixups
GUARDIUM_V11_UPGRADE_PHASEMSG:4.0:BEGIN:firstboot.post
GUARDIUM_V11_UPGRADE_PHASEMSG:4.0:FirstBoot Post: Force into upgrade mode, setting upgrade flag
GUARDIUM_V11_UPGRADE_PHASEMSG:4.0:SUCCESS:Upgrade mode detected, setting upgrade flag
GUARDIUM_V11_UPGRADE_PHASEMSG:4.0:SUCCESS:Applying Permission and security adjustments
GUARDIUM_V11_UPGRADE_PHASEMSG:4.0:SUCCESS:Post RPM Installation Upgrade Log Saving
GUARDIUM_V11_UPGRADE_PHASEMSG:4.0:SUCCESS:Post RPM Installation Configuration
GUARDIUM_V11_UPGRADE_PHASEMSG:4.0:SSH Key Propagation
GUARDIUM_V11_UPGRADE_PHASEMSG:4.0:Propagating SSH RSA Host Keys to SSH configuration
GUARDIUM_V11_UPGRADE_PHASEMSG:4.0:Propagating insecure SSH DSA Host Keys to SSH configuration as inactive
GUARDIUM_V11_UPGRADE_PHASEMSG:4.0:INFO>About to Shutdown and Reboot onto V11
GUARDIUM_V11_UPGRADE_PHASEMSG:4.1:INFO:Firstboot onto V11
GUARDIUM_V11_UPGRADE_PHASEMSG:4.1:SUCCESS:Upgrade flag detected, starting upgrade
GUARDIUM_V11_UPGRADE_PHASEMSG:4.1:Guard FirstBoot: Preserving Configuration Hint
Fri Jun 7 10:43:32 EDT 2019 INFO [pre-guard-upgrade]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.2:INFO:Upgrading a Unit of type 76
Fri Jun 7 10:43:32 EDT 2019 INFO [pre-guard-upgrade]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.2:INFO:Moving Solr files
Fri Jun 7 10:43:32 EDT 2019 INFO [pre-guard-upgrade]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.2:INFO:Copying TIVOLI files
Fri Jun 7 10:43:32 EDT 2019 INFO [pre-guard-upgrade]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.2:INFO:Copying CENTERA files
Fri Jun 7 10:43:32 EDT 2019 INFO [pre-guard-upgrade]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.2:INFO:Copying Previous Login Banner Files
Fri Jun 7 10:43:32 EDT 2019 INFO [pre-guard-upgrade]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.2:INFO:Copying Previous Network Configuration Files
```

Upgrade Process -- Phases

Phase 1: Verify ISO for upgrade

Phase 2: shutdown DB, Create Migration Tree, Setup Grub, prepare for RHEL7

Phase 3: Boot into installation kernel and install RHEL7

Phase 4: Reboot into RHEL7 and begin First Boot process

- 4.0 and 4.1: System upgrades including SOLR
- 4.2 and 4.3 : Backup and Network information
- 4.4 through 4.12: DB copy and migration
- 4.13: Certificates migration
- 4.14: Search Data migration
- 4.15: Password migration
- 4.16: Alerter and policies migration
- 4.17: Migrator Cleanup

Phase 5: Completion

Upgrade Process -- standalone ... completed

```
1 Schema
Fri Jun 7 06:46:01 EDT 2019 INFO [mysql-mig-setup]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.12:INFO:Restarting Database with V11 C
onfig
Fri Jun 7 06:46:04 EDT 2019 INFO [mysql-mig-setup]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.12:INFO:Database now on V11 Config
Fri Jun 7 06:46:37 EDT 2019 INFO [guard-upgrade]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.13:INFO:Starting Key and Certificate Mig
ration
Fri Jun 7 06:47:23 EDT 2019 INFO [guard-upgrade]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.13:INFO:Completed Key and Cert Migration
Fri Jun 7 06:47:23 EDT 2019 INFO [guard-upgrade]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.14:INFO:Completed Migration of Search Da
ta
Fri Jun 7 06:47:23 EDT 2019 INFO [guard-upgrade]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.15:INFO:Completed Migration of Passwords
Fri Jun 7 06:47:23 EDT 2019 INFO [guard-upgrade]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.16:INFO:Alerts not enabled; will not ru
n on start-up
Fri Jun 7 06:47:23 EDT 2019 INFO [guard-upgrade]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.16:INFO:Alerts configured to run as in
V10
Fri Jun 7 07:19:33 EDT 2019 INFO [post-guard-upgrade]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.16:INFO:About to apply Security Pol
icies
Fri Jun 7 07:19:37 EDT 2019 INFO [post-guard-upgrade]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.16:INFO:Security Policies applied
Fri Jun 7 07:19:37 EDT 2019 INFO [post-guard-upgrade]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.17:INFO:About to Clean up after Mig
ration
Fri Jun 7 07:19:37 EDT 2019 INFO [post-guard-upgrade]: GUARDIUM_V11_UPGRADE_PHASEMSG:4.17:INFO:Cleaved up after Migration
Fri Jun 7 07:21:40 EDT 2019 INFO [post-guard-upgrade]: GUARDIUM_V11_UPGRADE_PHASEMSG:5.0:INFO:Migration Complete
ok
guard.yourcompany.com>
```

```
guard.yourcompany.com> show build
Build: 11.0
Release: 11.0.0_r106705_v11_0_1-e176-20190523_2258
ID tags:
  BUILD_ID_APPLIANCE="appliance-v11_0-20190523_2258"
Snif version:
  BUILD_ID_CORE="core-trunk-20190503_1904"
  BUILD_TAG="11.1.0_r106561_trunk_1"
  BUILD_TIME="20190503_1903"
  BUILD_BUILD="106561"
  BUILD_MODULE="collector/snif"
  BUILD_PLATFORM="Linux_3.10.0-862.el7.x86_64"
  BUILD_NUM=106561
  BUILD_SHARED_LIB_VERSION=2.0.1
ok
guard.yourcompany.com>
```


How long does an upgrade take

Difficult to judge as each environment is different. Customers should model their systems in a test environment to gauge the upgrade speed.

A GAT system in a vmware Environment:

4 vCPU

24 GB RAM

300 GB Disk

http://glab-jenkins01.guard.swg.usma.ibm.com/job/CIC_BuildInstall/28093/console

5:28 health patch started

5:31 health patch done

5:31 p11000 started

6:20 p11000 finished

6:34 MySQL is running

Be patient, make sure the Customer doesn't unnecessarily reboot the appliance as doing this in the middle of the upgrade will require to fall back to backup and restore process.

Upgrade considerations and limitations

UUID

- Disk Block ID is now used for the upgrade instead of hard coding to `/dev/sda`

Custom Partitions and naming

- Due to the nature of custom partitions that deviate from the standard Guardium single disk install, custom partitions are not candidates for the upgrade process. Use backup and restore.

Pane is Dead

- In rare instances, we have found a virtual appliance that has hung and has not progressed. In console, you can see an error in the bottom left screen that states "Pane is Dead". This states that the system has hung and is not able to continue forward.
- Reboot system to continue upgrade

Upgrade considerations and limitations continued

Vmware and virtual Distributed Switches

- Late in testing, Intel released additional speculative-execution vulnerabilities known as “Microarchitectural Data Sampling (MDS)”. This triggered network connectivity issues during the upgrade. Although the upgrade was completed, the network was not connected. This was traced back to the use of virtual Distributed Switches (vDS) using ephemeral port binding.
- Switch the vDS to use static port binding – this is the vmware recommended configuration
- Or after the upgrade is completed, use vmware admin console to connect the network
- Or use a virtual standard switch for the upgrade

Upgrade considerations and limitations continued

Vmware and Dracut

- An additional affect of the MDS vulnerabilities is that it some instances, it has triggered a performance issue. In some occurrences, the system exits into Dracut emergency mode because of soft locks and/or I/O errors.
- Dracut is a RedHat system that checks devices prior to booting into the RedHat OS.
- The upgrade attempts to work around these issues by increasing the retry values for Dracut, and also will reboot the system to restart the Dracut analysis. As there are no changes to the system at this point, this is a safe practice.
- In rare occurrences – this has not been seen -- the system may reboot continuously. For this to happen, there is an underlying problem with the system. Shutdown the vm and resolve the underlying issues. Then, reboot the appliance. If needed, from the grub menu, select “Upgrade_To_V11” to the Dracut emergency shell to troubleshoot.

Upgrade considerations for cloud images

- V11 Upgrade from v10.x not supported on: Azure, Google, Oracle Compute, Oracle OCI, SoftLayer. Use backup/restore.
- V11 Upgrade from 10.x is supported on AWS

Guardium V11 New Release Training

Active Threat Analytics

Contents

Overview

Use cases

Demo

Architecture

Implementation considerations

Troubleshooting

Overview

Active threat analytics is a new approach of looking at malicious events in the system.

It takes all of Guardium's monitored data and summarizes it to meaningful events you should look at.

It integrates a lot of different components in order to show as much data as possible.

What's New

- Use-cases.
- Textual Descriptions.
- Model exposure.
- Fully integrated with other Guardium features.

Benefits

- Simple.
- Informative.
- Take action.

Use Cases

- **Detect potential malicious activities in the system.**

Using 'Outliers detection' we can pinpoint on user / databases changes in behavior.

- **Detect possible database attacks on the system.**

Using 'Threat Detection Analytics' which scans and analyzes audited data to detect symptoms that may indicate SQL injection or Stored Procedure database attacks.

Security Threat Vectors (V11.0)

- SQL injection
- Malicious stored procedure
- Data leak
- Denial of service
- Account take-over
- Schema tempering
- Data tempering
- Anomaly

Demo

Active Threat Analytics

Cases are derived from Guardium data collection and analysis. All high severity cases indicate a potential threat, and should be thoroughly analyzed.
H- High severity, M- Medium severity, L- Low severity

[Risk Spotter](#) [Outlier Mining Administration](#)

Last 1 Day



Top Cases

H6M8L130

Databases
with open cases

H1M1L0

DB Users
with open cases

H1M1L92

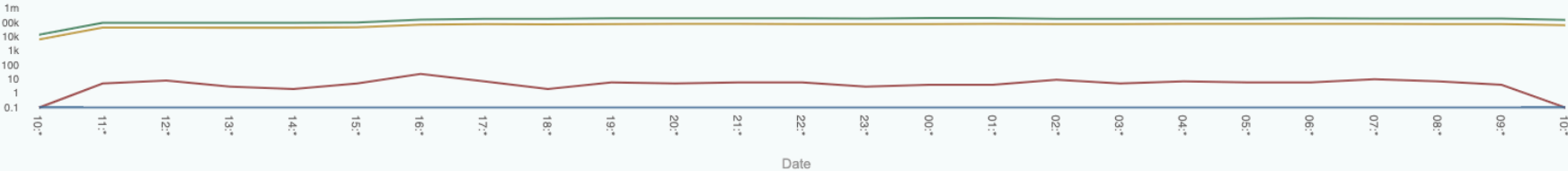
File Systems
with open cases

H0M0L0

File Users
with open cases

H0M0L0

Violation Outlier Error Activities



Actions		Filter					
Case #	Threat Category	Severity	Observations	Source	Date	Assigned	
612	Insider Threat: Possible data leak	Low	High volume of data extraction by privileged DB user	Server: 9.32.164.142 Database: DB2INST1 DB User: DB2INST1	2019-06-06, 09:00:00 AM	No	
603	SQL Injection	Low	Evidence of attempts to access unauthorised tables or stored procedures. Tables that contain information about the database structure were accessed. Evidence of attempts to identify the structure of a dynamic SQL query. Go to Actions>Full report to check if there are more observations for this case.	Server: 9.32.164.142 Database: DB2INST1 DB User: DB2_2V7H	2019-06-06, 07:15:00 AM	No	
568	SQL Injection	Low	Evidence of attempts to access unauthorised tables or stored procedures. Tables that contain information about the database structure were accessed. Evidence of attempts to identify the structure of a dynamic SQL query. Go to Actions>Full report to check if there are more observations for this case.	Server: 9.32.164.142 Database: DB2INST1 DB User: DB2_4Z8G	2019-06-06, 02:15:00 AM	No	

Demo

Actions

Assign Case

Add to Group

Close Case










Open Case Dashboard

Source Behavioral Analytics

Full Report

Filter							
Case #		Severity	Observations	Source	Date	Assigned	
<input type="checkbox"/> 612	able data leak	Low	High volume of data extraction by privileged DB user	Server: 9.32.164.142 Database: DB2INST1 DB User: DB2INST1	2019-06-06, 09:00:00 AM	No	
<input checked="" type="checkbox"/> 603		Low	Evidence of attempts to access unauthorised tables or stored procedures. Tables that contain information about the database structure were accessed Evidence of attempts to identify the structure of a dynamic SQL query Go to Actions>Full report to check if there are more observations for this case.	Server: 9.32.164.142 Database: DB2INST1 DB User: DB2_2V7H	2019-06-06, 07:15:00 AM	No	
<input type="checkbox"/> 568		Low	Evidence of attempts to access unauthorised tables or stored procedures. Tables that contain information about the database structure were accessed Evidence of attempts to identify the structure of a dynamic SQL query Go to Actions>Full report to check if there are more observations for this case.	Server: 9.32.164.142 Database: DB2INST1 DB User: DB2_4Z8G	2019-06-06, 02:15:00 AM	No	

Demo

SQL Injection Case Symptoms					
<div></div> <div>Export Actions Graphical View</div>					
Description	Details	Seen From	Count	Original SQL	
Tables that contain information about the database structure have been accessed	SYSCAT.COLUMNS	2019-06-06 07:15:00	54	SELECT COUNT(*) FROM SYSCAT.COLUMNS WHERE TABSCHEMA = ? AND TABNAME = ? AND COLNAME = ?	
Someone is trying to access unauthorised tables or stored procedures	does not have the privilege to perform operation operation on object object-name.	2019-06-06 07:15:00	321	INSERT INTO ancient.tbl_table0_i13s (CLINICIAN_ID, CFNAME, CINITIAL, CLNAME, CSPECIALITY, CSSN, CBIRTH - DATE, CSTATE, CPROVINCE, COUNTRY, CZIP_CODE, CEMAIL, CEMERGENCY_CONTACT, CEMERGENCY_PHONE, CMOBILE_PHONE, CHOME_PHONE) VALUES (?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?)	
Someone might be trying to work out the structure of a dynamic SQL query	is not valid in the context where it is used.	2019-06-06 07:15:00	5	select a.CFNAME as Doctor_FirstName, a.CLNAME as Doctor_LastName, a.CSPECIALITY as Doctor_Speciality, a.CBIRTH_DATE as Doctor_DateOfBirth, a.CSTATE as Doctor_State, a.CZIP_CODE as Doctor_ZIP, a.CEMAIL as Doctor_EMAIL, a.CMOBILE_PHONE as Doctor_CELLPHONE, b.PATIENT_ID, b.FNAME as PATIENT_FIRSTNAME, b.LNAME as PATIENT_LASTNAME, b.STREET_ADDR1 as PATIENT_ADDR1, b.STREET_ADDR2 as PATIENT_ADDR2, b.CITY as PATIENT_CITY, b.SSTATE as PATIENT_STATE, b.ZIP_CODE as PATIENT_ZIP, b.EMAIL as PATIENT_EMAIL, b.CO_PAY_AMOUNT as PATIENT_COPAY_AMOUNT, b.INSURANCE_ID as PATIENT_INSURANCE_ID, b.HOME_PHONE as PATIENT_HOMEPHONE, c.BILL_ID as PATIENT_BILL_ID, c.PATIENT_ID as BILLING_PATIENTID, c.CLINICIAN_ID as BILLING_CLINICIANID, c.INSURANCE_ID as BILLING_INSURANCEID, c.ENCOUNTER_ID as BILLING_ENCOUNTER, c.BILL_DATE as BILLING_DATE, c.BILL_ICD_10_CODE as BILLING_ICD10Code, c.BILL_TOTAL as BILLING_TOTAL, c.BILL_LINEITEM_AMT, c.BILL_DESCRIPTION from ancient.tbl_table0_i13s a JOIN ancient.tbl_table1_7gkv b on a.CLINICIAN_ID = b.PRIMARY_CLINICIAN_ID where a.CLINICIAN_ID in (select distinct(c.CLINICIAN_ID) from ancient.tbl_table4_hau2 c INNER JOIN ancient.tbl_table5_kyd6 d on c.PATIENT_ID=d.PATIENT_ID where c.BILL_ICD_10_CODE = ?)	

Demo

Actions

Assign Case

Add to Group

Close Case

Open Case Dashboard

Source Behavioral Analytics

Full Report

Filter							
Case #		Severity	Observations	Source	Date	Assigned	
<input type="checkbox"/> 612	able data leak	Low	High volume of data extraction by privileged DB user	Server: 9.32.164.142 Database: DB2INST1 DB User: DB2INST1	2019-06-06, 09:00:00 AM	No	
<input checked="" type="checkbox"/> 603		Low	Evidence of attempts to access unauthorised tables or stored procedures. Tables that contain information about the database structure were accessed Evidence of attempts to identify the structure of a dynamic SQL query Go to Actions>Full report to check if there are more observations for this case.	Server: 9.32.164.142 Database: DB2INST1 DB User: DB2_2V7H	2019-06-06, 07:15:00 AM	No	
<input type="checkbox"/> 568		Low	Evidence of attempts to access unauthorised tables or stored procedures. Tables that contain information about the database structure were accessed Evidence of attempts to identify the structure of a dynamic SQL query Go to Actions>Full report to check if there are more observations for this case.	Server: 9.32.164.142 Database: DB2INST1 DB User: DB2_4Z8G	2019-06-06, 02:15:00 AM	No	

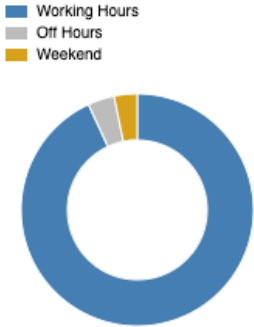
DB User Behavioral Analytics

DB User: DB_USER_20
Database: ON2PILRH
Server IP: 9.32.164.216

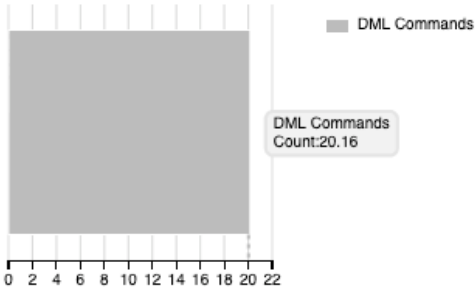
Tracked since: 2019-06-06 07:00
Avg. activities per hour: 20.16
Max. activities in any one hour: 3357
Avg. exceptions per hour: 1.12

User Risk Indicators

Distribution of Working Hours

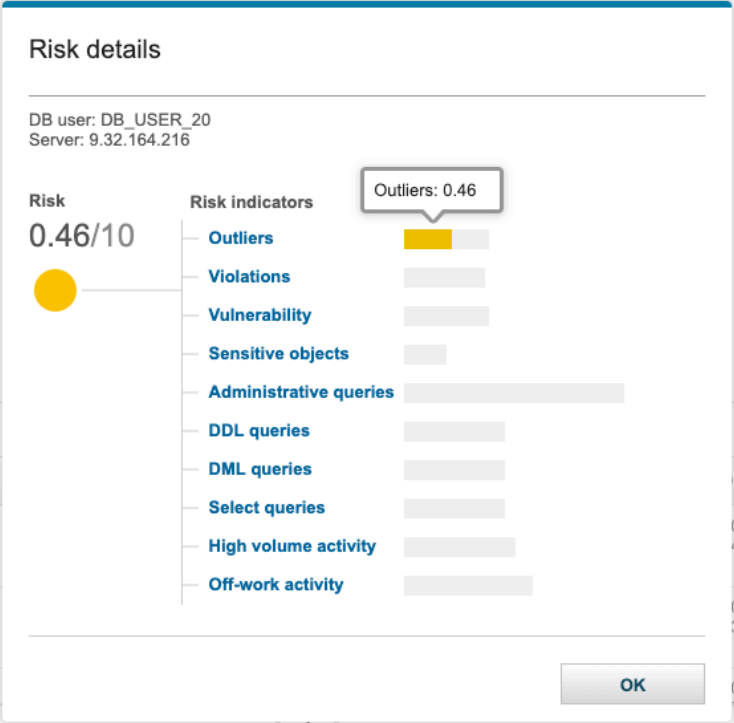


Distribution of Verbs



Actions				Filter		
<input type="checkbox"/>	Case #	Threat Category	Severity	Observations	Date	Assigned
<input type="checkbox"/>	512	Denial Of Service	Low	Exceptionally high volume of activities of some type: verb, verb/object, application, connection, etc. Exceptionally high level of activity	2019-06-05, 14:00:00 PM	No
<input type="checkbox"/>	501	Denial Of Service	Low	Exceptionally high volume of activities of some type: verb, verb/object, application, connection, etc. Exceptionally high level of activity	2019-06-05, 13:00:00 PM	No
<input type="checkbox"/>	495	Anomaly	Low	Exceptionally high volume of different types of activities, for ex-	2019-06-05, 13:00:00 PM	No
Total: 3 Selected: 0				1		

Demo



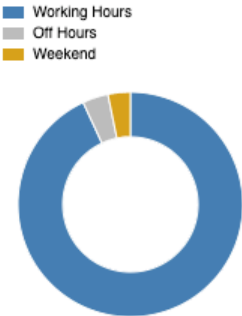
DB User Behavioral Analytics

DB User: DB_USER_20
Database: ON2PILRH
Server IP: 9.32.164.216

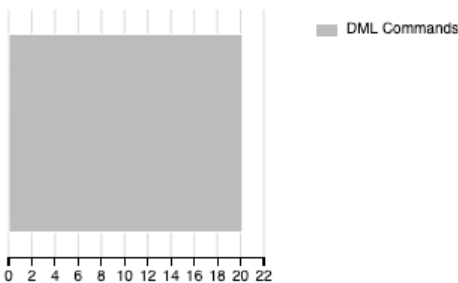
Tracked since: 2019-06-06 07:00
Avg. activities per hour: 20.16
Max. activities in any one hour: 3357
Avg. exceptions per hour: 1.12







User Risk Indicators

Distribution of Working Hours



Distribution of Verbs



 		Actions 	Filter 			
<input type="checkbox"/>	Case #		Severity	Observations	Date	Assigned
<input checked="" type="checkbox"/>	512	Assign Case Add to Group Close Case	Low	Exceptionally high volume of activities of some type: verb, verb/object, application, connection, etc. Exceptionally high level of activity	2019-06-05, 14:00:00 PM	No
<input type="checkbox"/>	501	Open Case Dashboard Source Behavioral Analytics	Low	Exceptionally high volume of activities of some type: verb, verb/object, application, connection, etc. Exceptionally high level of activity	2019-06-05, 13:00:00 PM	No
<input type="checkbox"/>	495	Full Report	Low	Exceptionally high volume of different types of activities, for ex-	2019-06-05, 12:00:00 PM	No
Total: 3 Selected: 1  1 						

Demo

Detailed outlier description

The outlier type, the associated DB or DB user, the outlier characteristics, and a comparison of (the outlier count : the average hourly count)

Excessive activity related to DB User on IL-RHVM01; ROOT (3256:15.53)

Excessive activity related to DB User on JDBC THIN CLIENT (3256:15.53)

Excessive activity related to DB User on DML Commands (3256:15.53)

Excessive activity related to DB User on system.OBJECT_23; DML Commands (599:8.38)

Excessive activity related to DB User on system.OBJECT_13; DML Commands (1132:11.59)

Excessive activity related to DB User on system.OBJECT_37; DML Commands (929:14.14)

Excessive activity related to DB User on 9 (3256:40.62)

Excessive errors related to DB User such as system.OBJECT_13_ERROR; DML Commands (5:1.01)

Excessive errors related to DB User such as system.OBJECT_1_ERROR; DML Commands (5:1.01)

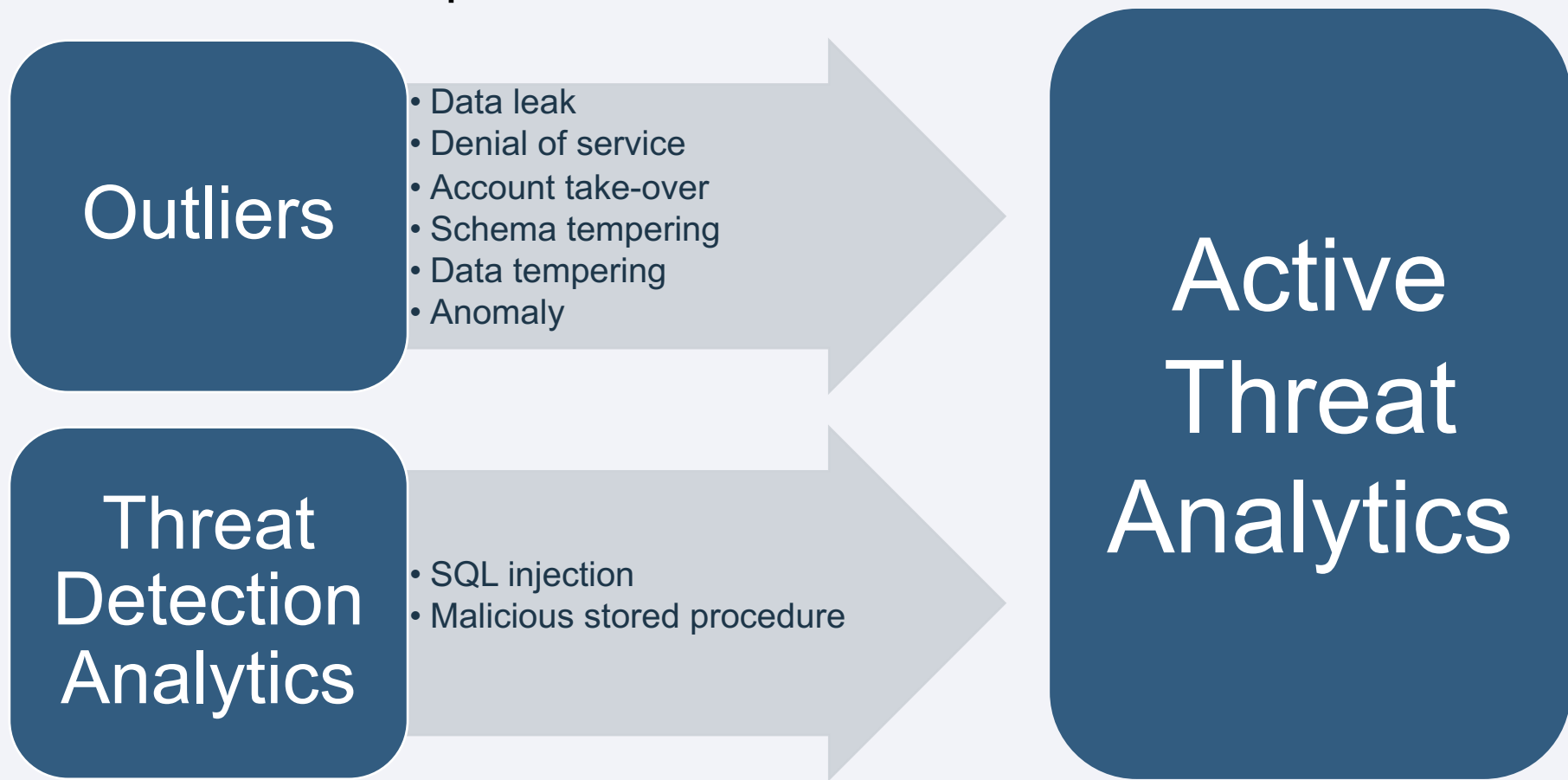
Excessive errors related to DB User such as system.OBJECT_37_ERROR; DML Commands (5:1.01)

Excessive errors related to DB User such as system.OBJECT_67_ERROR; DML Commands (5:1.01)

Excessive errors related to DB User such as DML Commands (5:1.01)

Close

Architecture – Input Flow



Implementation considerations: Installation

- **Dependencies:**
 - Outliers Detection / Threat Detection Analytics. (At least one enabled)
 - (Optional) Quick Search / Risk Spotter.
- **Standard install sequence:**
 - grdapi **enable_outliers_detection** (on CM) / Outlier Mining Administration
 - grdapi **enable_advanced_threat_scanning** (On each collector / api_target_host=all)
- **Verifying successful installation:**
 - Outlier mining administration screen.
- **Backup and restore considerations:**
 - Use-case data is saved on CM.
 - Statistics and details are saved on aggregator / collector.

Implementation considerations: Upgrade Considerations

- After upgrade to the new version 'Active Threat Analytics' is attached to Outliers detection and Threat Detection Analytics status.
- Old outliers / attacks will not be declared as use-cases.
- New events will be automatically added as use-cases.

Implementation considerations: Configuration

- Outliers Detection / Threat Detection Analytics configurations will directly impact Active Threat Analytics.
- Default configurations should be enough for most cases.
 - Outliers detection – up to 1 alert per hour on average for each process.
 - Threat Detection Analytics – Event per potential attack.
- Advanced Configurations:
 - Running outliers without Active Threat Analytics:
 - » `runCaseAnalysis=false`.

Guardium V11.0 New Release Training

Risk Spotter

Contents

Challenges

Risk spotter flow

Demo

Configuration

Troubleshooting

Q & A

Reference materials

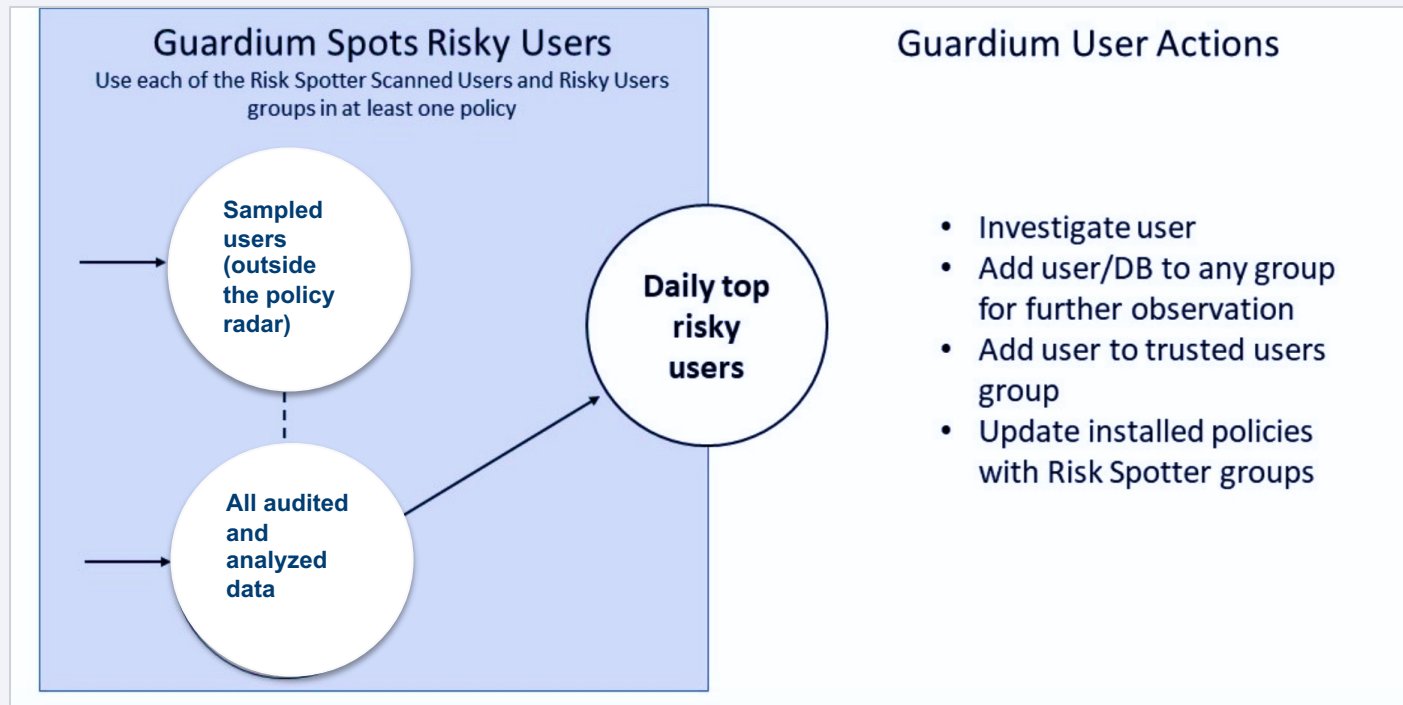
Overview

Goal: Semi-Automatic process for auto-focusing on Most Risky Users

- Dynamic Risk Assessment
 - Based on all risks factors (outliers, vulnerability, volume of activities, access to sensitive data, etc.)
- Sampling strategies
 - Scanning un-monitored users' activities
 - Find less familiar → Audit → Analyze → Assess
 - Expand our focus area



Risk Spotter - Flow



Risk Spotter demo - Configure, view and take action

The screenshot shows the IBM Guardium user interface. On the left is a navigation sidebar with icons for Protect, Database Intrusion Detection, Security Policies, and Uncover Threat Vectors. The 'Uncover Threat Vectors' section is expanded, showing 'Active Risk Spotter' and 'Active Threat Analytics'. A blue arrow points from this section to the 'Discover sensitive data' card. The main area features a 'Get Started' section with three cards: 'Discover sensitive data' (with a magnifying glass icon), 'Set up compliance monitoring' (with a padlock icon), and 'Active threat analytics' (with a head and network icon). A second blue arrow points from the 'Active threat analytics' card to a table. The table has two columns: 'NAME' and 'LOCATION'. It lists three items: 'Active Risk Spotter', 'Active Risk Spotter - Risky Users Scores', and 'Active Risk Spotter - Risky Users Scores'. A third blue arrow points from the table to the 'Active threat analytics' card. The top of the interface shows the time (09:52), user interface dropdown, and search bar with 'active risk' entered. The top right corner shows the user 'admin' and machine type 'Central Manager - Aggregator'.

NAME	LOCATION
Active Risk Spotter	Protect > Uncover Threat Vectors > Active Risk Spotter
Active Risk Spotter - Risky Users Scores	My Dashboards > My Custom Dashboards > My Dashboard [2019-01-20-14.01.20]
Active Risk Spotter - Risky Users Scores	My Dashboards > My Custom Dashboards > My Dashboard [2019-01-28 14.01.20]

IBM Guardium

05:49User Interface▼

User Interface Search

Machine Type
admin admin ▼Central Manager - Aggregator

>>

Active Risk Spotter

Actions▼?

Risk Spotter is running

Disable

>Policy and related modules

Average risk score

Risky users

Scanned users

Scanned Server IPs

Date

4.07/10

12

100

2

May 30, 2019▼

Users by risk level: 5/30/19

Low risk

Medium risk

High risk

Users average risk during:

Last month▼

Risky users

Scanned users

View the top 50 risky users, see the evidence, and take action.

Risk▼	Auditing	DB User	Server	Actions
		DB_USER_11	9.42.29.160	Actions▼
		ENCORE\SPFARM	9.70.164.153	Actions▼
		DB_USER_16	9.42.135.95	Actions▼
		DB_USER_15	9.42.135.95	Actions▼

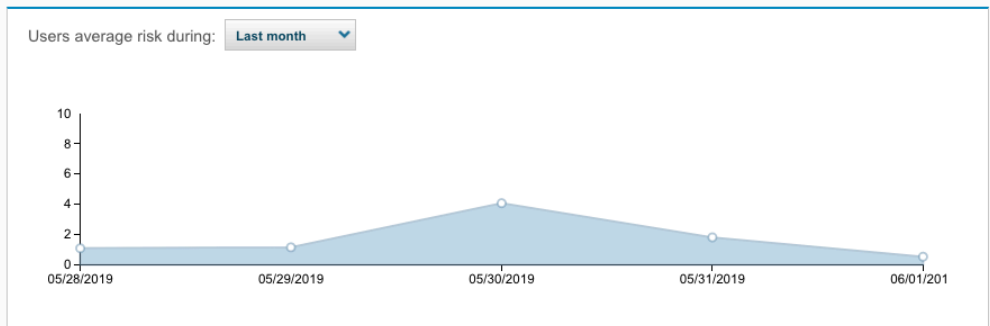
Actions

Disable

Scanned Server IP's

2.

May 30, 2019



Scanned users

Risk ▾	Auditing	DB User	Server	Actions
🔴	👁️	DB_USER_11	9.42.29.160	Actions ▾
🟡	👁️	ENCORE\SPFARM	9.70.164.153	Actions ▾
🟡	👁️	DB_USER_16	9.42.135.95	Actions ▾
🟡	👁️	DB_USER_15	9.42.135.95	Actions ▾

Actions

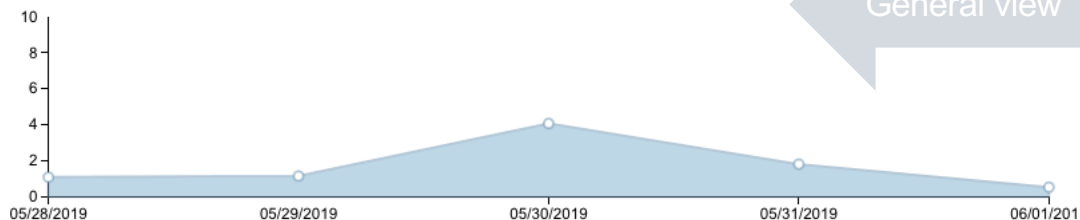
Disable

- > Policy and related modules

Date _____

May 30, 2019 

Users average risk during: **Last month** 



Risk ▾	Auditing	DB User	Server	Actions
🔴	👁	DB_USER_11	9.42.29.160	Actions ▾
🟡	👁	ENCORE\SPFARM	9.70.164.153	Actions ▾
🟡	👁	DB_USER_16	9.42.135.95	Actions ▾
🟡	👁	DB_USER_15	9.42.135.95	Actions ▾

IBM Guardium

05:49

User Interface

User Interface Search

admin admin

Machine Type
Central Manager - Aggregator

Active Risk Spotter

✓ Risk Spotter is running

Disable

> Policy and related modules

Average risk score
4.07 /10

Risky users
12

Scanned users
100

Scanned Server IPs
2

Date
May 30, 2019

Users by risk level: 5/30/19

Low risk

Medium risk

High risk

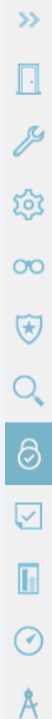
Users average risk during: Last month

Risky users

Scanned users

View the top 50 risky users, see the evidence, and take action.

Risk	Auditing	DB User	Server	Actions
High	Yes	DB_USER_11	9.42.29.150	Actions
Medium	Yes	ENCORE\SPFARM		Actions
Medium	Yes	DB_USER_16	9.42.135.	Actions
Medium	Yes	DB_USER_15	9.42.135.95	Actions



Active Risk Spotter

Actions

> Policy and related modules

Average risk score

4.07 /10

Risky users

12

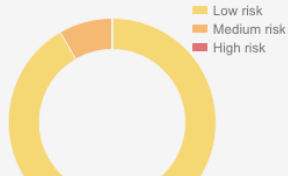
Scanned users

Scanned Server IPs

Date

May 30, 2019

Users by risk level: 5/30/19



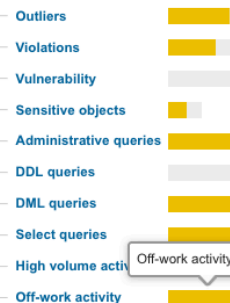
Risk details

Risk details

DB user: DB_USER_11
Server: 9.42.29.160

Risk
6.77/10

Risk indicators



OK

Risky users

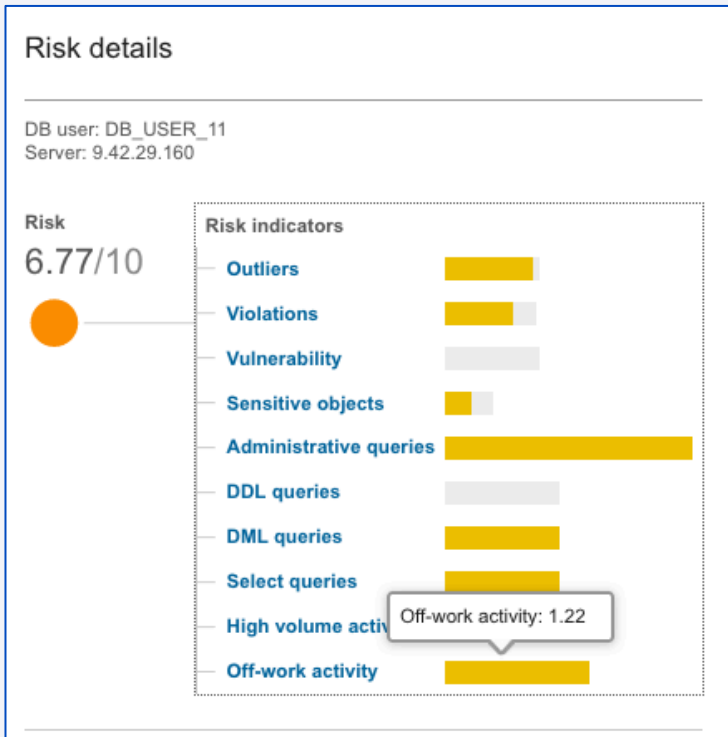
Scanned users

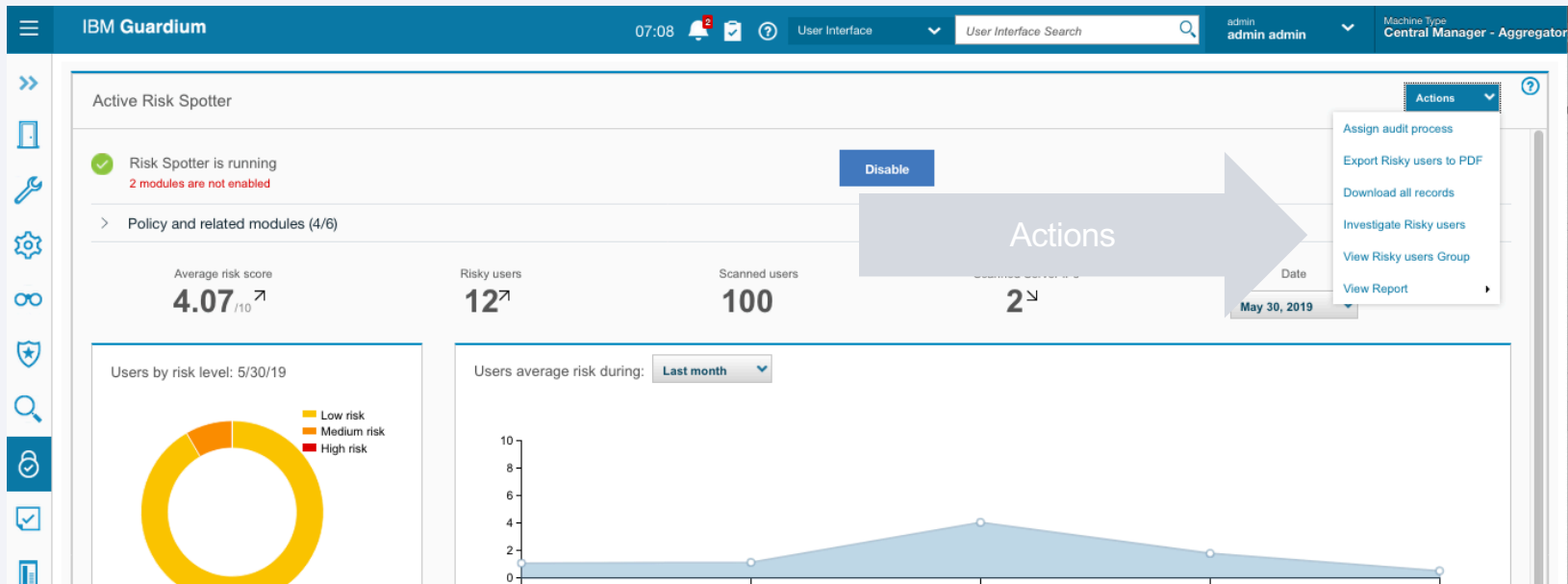
View the top 50 risky users, see the evidence, and take action.

Risk	Auditing	DB User		Actions
		DB_USER_11	9.42.29.160	Actions
		ENCORE\SPFARM	9.70.164.153	Actions
		DB_USER_16	9.42.135.95	Actions
		DB_USER_15	9.42.135.95	Actions

Risk assessment

Outliers	The number and severity of anomalies related to the user.
Violations	The number of high and medium severity violations related to the user.
Vulnerability	The number of failed vulnerability assessments for a user.
Sensitive objects	The number of queries on sensitive data related to the user.
Off-work activity	Activity related to the user that occurred in non-work hours.
DDL queries	The relative amount of DDL queries related to the user, out of the total activity.
DML queries	The relative amount of DML queries related to the user, out of the total activity.
Administrative queries	The relative number of administrative queries related to the user, out of the total activity.
Select queries	The relative number of select queries related to the user, out of the total activity.
High volume activity	High volume activities as compared to the average activities of users.





Risky users

Scanned users

View the top 50 risky users, see the evidence, and take action.

Risk	Auditing	DB User	
High	✓	DB_USER_11	9.42.29.160
Medium	✓	ENCORE\SPFARM	9.70.164.153
Medium	✓	DB_USER_16	9.42.135.95
Medium	✓	DB_USER_15	9.42.135.95

Actions

Actions

Risk details

Investigate

Add to "Risk Spotter - Trusted Users" Group

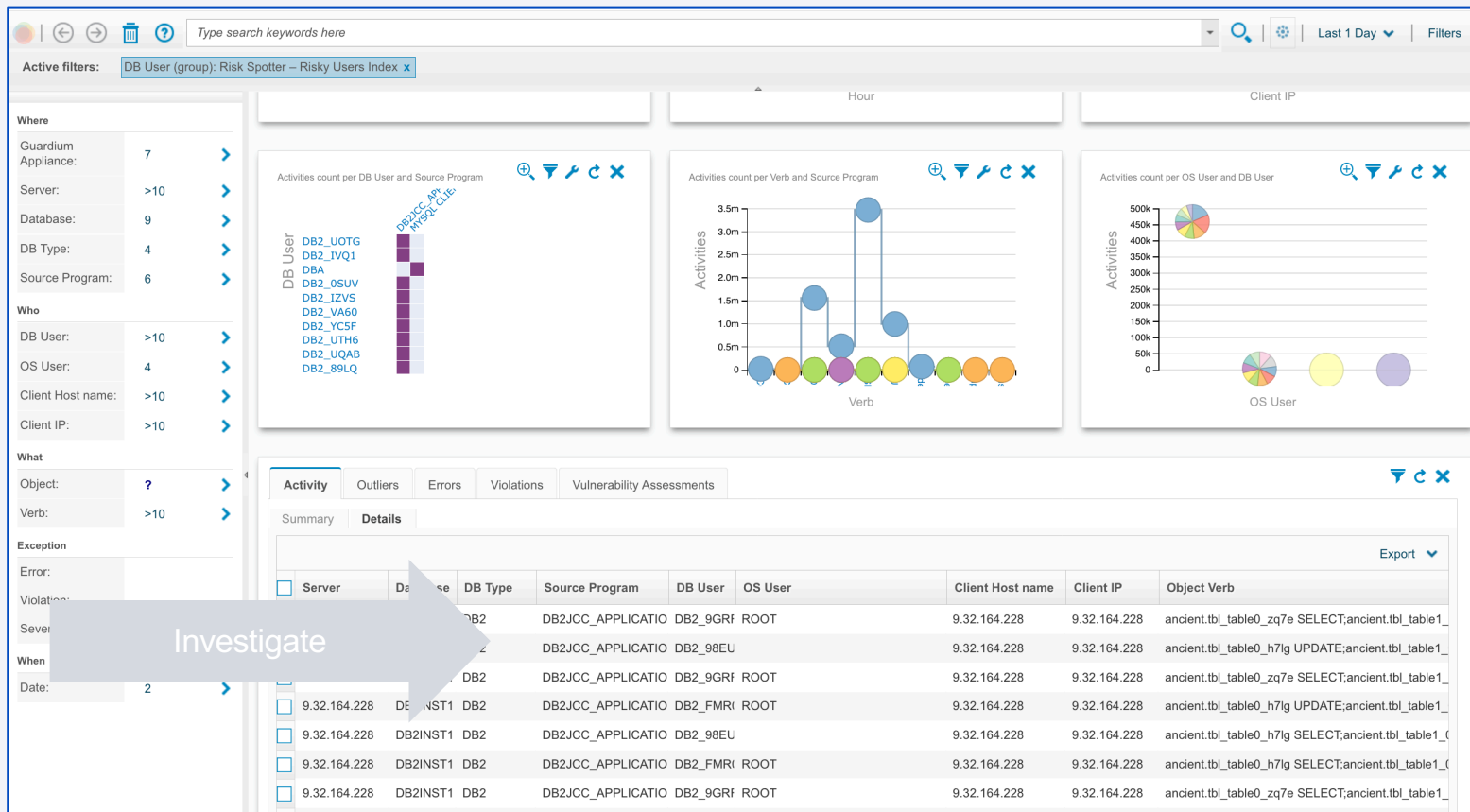
Add DB User to Group...

Add Server IP to Group...

Actions

Actions

Investigate risks



Configuration



Risk Spotter is running

Identifies and grades risky users using multiple risk indicators, spots potential risky users beyond your installed policies, and continuously updates both the Risky Users and Scanned Users groups. You can investigate the top risky users, assign audit processes, and adjust your policy to mitigate risks.

[Disable](#)

Policy and related modules



Audit users with the Risk Spotter policy (recommended)

Installed on 2/3 managed units

[View](#)[Install](#)

Related modules



Enterprise search (required)

Configured on central manager and 2/3 managed units



Database Protection Subscription service (recommended)

[Upload file](#)

Unit utilization data processing (required)



S-TAP information (required)



Outlier detection (recommended)

Status and
Configuration

Risk spotter policy

IBM Guardium

05:47

admin admin

Machine Type
Central Manager - Aggregator

Active Risk Spotter

View Risk Spotter Policy

Name and properties

Risk Assessment Dynamic Policy Selective [template]

Expand

Rules

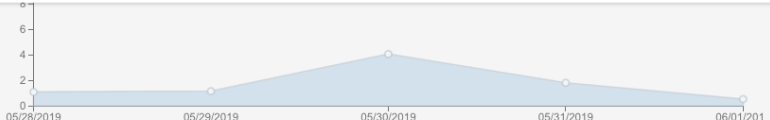
Define policy rules

Collapse

Filter

Order	Rule type	Rule name	Criteria	Actions	Continue to next rule
1	Access	Risk Spotter - Scanned Users	Severity = Info, Client IP/Source application/Database user/Server IP/Service name In group Risk Spotter - Scanned Users	AUDIT ONLY	<input checked="" type="checkbox"/>
2	Access	Risk Spotter - Risky Users	Severity = Info, Client IP/Source application/Database user/Server IP/Service name In group Risk Spotter - Risky Users	AUDIT ONLY	<input checked="" type="checkbox"/>

Close



Date	Risk Level
05/28/2019	1
05/29/2019	1
05/30/2019	4
05/31/2019	2
06/01/2021	1

Troubleshooting

















- **Status and Control** - Expand the *Policy and Related modules* to see the status of all the modules

The screenshot displays a web interface for managing Risk Spotter. At the top, a green checkmark icon indicates 'Risk Spotter is running', with a blue 'Disable' button to its right. Below this, a section titled 'Policy and related modules' is expanded, showing a green checkmark and the text 'Audit users with the Risk Spotter policy (recommended)'. To the right of this text are two buttons: 'View' and 'Install'. Underneath, a section titled 'Related modules' lists five items, each with a green checkmark: 'Enterprise search (required)', 'Database Protection Subscription service (recommended)', 'Unit utilization data processing (required)', 'S-TAP information (required)', and 'Outlier detection (recommended)'. To the right of the 'Database Protection Subscription service' item is a blue 'Upload file' button.

- Enterprise search – enabled by default, verify that `includeViolations=true`
- Solr logs - `grdapi test_solr details=true, $GUARD_LOG_DIR/solr7-upgrade.log`

Troubleshooting

- Outlier mining administration page

Outlier Mining Administration											
Actions 											
	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	
<input type="checkbox"/>	shlomit-vm01.guard.swg.usma.ibm.com	Central Manager								6/5/19, 5:46 AM	
<input type="checkbox"/>	il-vm10.guard.swg.usma.ibm.com	Collector				6/5/19, 5:06 AM		6/4/19, 12:00 AM		6/5/19, 5:43 AM	
<input type="checkbox"/>	gpart1-col15.guard.swg.usma.ibm.com	Collector				6/5/19, 5:01 AM		6/4/19, 12:00 AM		6/5/19, 5:43 AM	
<input type="checkbox"/>	il-vm11.guard.swg.usma.ibm.com	Collector				6/5/19, 5:01 AM		6/4/19, 12:00 AM		6/5/19, 5:43 AM	

- GRDAPI - on CM and standalone - enable_riskspotter and disable_riskspotter
- Risk Spotter Logs `~/opt/IBM/Guardium/log/debug-logs/` on Debug mode search for "----DynamicPolicy----" and go from each daily iteration starts with "DynamicPolicy Start iteration"

Troubleshooting

- Users are not audited?
- Check the Risky users group. If it's empty:
- Make sure all dependencies are green in Risk Spotter page
- Verify that "Riskspotter Managed Units" group in Central Management / Managed Unit Groups contains relevant collectors (those that run our policy or have our groups in rules)
- Check that "Unit Utilization Distribution" report in Central Management / Unit Utilization has statuses on all collectors that from the "Riskspotter Managed Units" group (if empty/missing - check configuration according to

Reference Materials

Related articles

[CyberRank: Knowledge elicitation for risk assessment of database security](#)

[Sampling high throughput data for anomaly detection for database activity](#)

Guardium V11 New Release Training

Policy analyzer

Contents

Overview

Use cases

Demo

Architecture

Limitations

Troubleshooting

Q & A

Reference materials

Overview

Policy analyzer provides rule counts for *installed* DAM policy rules.

Collection profiles, FAM and session-level policies are **not** supported.

What's New

- 2 modes: continuous and ad hoc
- Continuous mode runs in the background and provides historical graphs for comparison
- Ad hoc mode run for a specified time period. It can be scheduled.

Benefits

- Can identify which rules fire the most
- Can identify which rules are NOT firing at all
- Can view impact of things like rule ordering on fire counts.

Use Cases

1. A customer wants to understand which DAM policy rules fire the most, so she can optimize the rule installation order.
2. A customer wants to see the impact of something like a rule change or running a batch job
3. A customer wants to identify if any DAM policy rules are not firing at all

Where to launch: Policy grid toolbar on Managed Unit (not from CM)

IBM Guardium 11:38 User Interface Search admin admin Machine Type Managed Unit

Security Policies

Download as CSV View logs and violation Install Analyze Include templates Filter

Name	Rules	Last changed	Last installed	Installed	Installation order	Selective audit trail
<input type="radio"/> Default - Ignore Data Activity for Unknown Connections [template]	1	2019-06-04 06:33:22	2019-06-04 06:31:18	<input checked="" type="checkbox"/>	1	false
<input type="radio"/> Allow-All [template]	0	2019-06-04 06:33:22		<input type="checkbox"/>	0	false
<input type="radio"/> Basel II [template]	11	2019-06-04 06:33:22		<input type="checkbox"/>	0	true
<input type="radio"/> Data Privacy - PII [template]	19	2019-06-04 06:33:22		<input type="checkbox"/>	0	true
<input type="radio"/> Data Privacy [template]	17	2019-06-04 06:33:22		<input type="checkbox"/>	0	true
<input type="radio"/> Default Sharepoint Auditing [template]	5	2019-06-04 06:33:22		<input type="checkbox"/>	0	false
<input type="radio"/> GDPR for Db2 for z/OS [template]	7	2019-06-04 06:33:22		<input type="checkbox"/>	0	true
<input type="radio"/> GDPR [template]	10	2019-06-04 06:33:22		<input type="checkbox"/>	0	true
<input type="radio"/> Hadoop Policy [template]	3	2019-06-04 06:33:22		<input type="checkbox"/>	0	false
<input type="radio"/> HIPAA [template]	18	2019-06-04 06:33:22		<input type="checkbox"/>	0	true
<input type="radio"/> PCI [template]	18	2019-06-04 06:33:22		<input type="checkbox"/>	0	true
<input type="radio"/> PCI, Oracle EBS [template]	18	2019-06-04 06:33:22		<input type="checkbox"/>	0	true
<input type="radio"/> PCI, SAP [template]	18	2019-06-04 06:33:22		<input type="checkbox"/>	0	true
<input type="radio"/> Privileged Users Monitoring (black list) [template]	10	2019-06-04 06:33:22		<input type="checkbox"/>	0	false

Total: 20 Selected: 0 1

Menu

Security Policies

Download as CSV

View logs and violation

Install

Analyze

☒ Include templates

Filter

Name	Policy analyzer is currently running	Stop policy analyzer	Change policy analyzer settings	Run ad hoc analysis	View results	Installed	Installed	Installation order	Selective audit trail
<input type="radio"/> Default - Ignore Data Activity for Unknown Connections [template]	19	2019-06-04 06:33:22				06-04 06:31:18	<input checked="" type="checkbox"/>	1	false
<input type="radio"/> Allow-All [template]	17	2019-06-04 06:33:22						0	false
<input type="radio"/> Basel II [template]	5	2019-06-04 06:33:22						0	true
<input type="radio"/> Data Privacy - PII [template]	17	2019-06-04 06:33:22						0	true
<input type="radio"/> Data Privacy [template]	5	2019-06-04 06:33:22						0	false
<input type="radio"/> Default Sharepoint Auditing [template]	7	2019-06-04 06:33:22						0	true
<input type="radio"/> GDPR for Db2 for z/OS [template]	10	2019-06-04 06:33:22						0	true
<input type="radio"/> GDPR [template]	3	2019-06-04 06:33:22						0	false
<input type="radio"/> Hadoop Policy [template]	18	2019-06-04 06:33:22						0	true
<input type="radio"/> HIPAA [template]	18	2019-06-04 06:33:22						0	true
<input type="radio"/> PCI [template]	18	2019-06-04 06:33:22						0	true
<input type="radio"/> PCI, Oracle EBS [template]	18	2019-06-04 06:33:22						0	true
<input type="radio"/> PCI, SAP [template]	10	2019-06-04 06:33:22						0	false
<input type="radio"/> Privileged Users Monitoring (black list) [template]									

Total: 20 Selected: 0

1

Stop/start policy analyzer

Current state is shown by icon and text in the drop down menu

Menu toggles from start to stop based on state.

Security Policies

+ ✎ 📁 - ↺ 🗨 | Download as CSV | View logs and violation | Install | Analyze ▼ | ☒ Include templates | Filter

Name	Frequency	First	Next	Installed	Installation order	Selective audit trail
Default - Ignore Data Activity for Unknown Connections [template]	1	2019-06-04 06:31:18		✓	1	false
Allow-All [template]	0				0	false
Basel II [template]	0				0	true
Data Privacy - PII [template]	19	2019-06-04 06:33:22			0	true
Data Privacy [template]	17	2019-06-04 06:33:22			0	true

⏸ Policy analyzer is currently not running

Start policy analyzer

Change policy analyzer settings

Run ad hoc analysis

View results ▶

Security Policies

+ ✎ 📁 - ↺ 🗨 | Download as CSV | View logs and violation | Install | Analyze ▼ | ☒ Include templates | Filter

Name	Frequency	First	Next	Installed	Installation order	Selective audit trail
Default - Ignore Data Activity for Unknown Connections [template]	1	2019-06-04 06:31:18		✓	1	false
Allow-All [template]	0				0	false
Basel II [template]	0				0	true
Data Privacy - PII [template]	19	2019-06-04 06:33:22			0	true

✓ Policy analyzer is currently running

Stop policy analyzer

Change policy analyzer settings

Run ad hoc analysis

View results ▶

Change policy analyzer settings

Interval is how often data is written to Guardium tables.

Results report is impacted by interval. For example, if interval is 30 min, choosing last 10 min in the report may not show results.

Security Policies

+ ✎ 📁 - ↺ 🗨 | Download as CSV | View logs and violation | Install | Analyze ▾ | ☒ Include templates | Filter

	Name	Rules	Last changed	Last installed	Installed
<input type="radio"/>	Default - Ignore Data Activity for Unknown Connections [template]	1	2019-06-04 06:33:22	2019-06-04 06:31:18	<input checked="" type="checkbox"/>
<input type="radio"/>	Allow-All [template]				
<input type="radio"/>	Basel II [template]				
<input type="radio"/>	Data Privacy - PII [template]				
<input type="radio"/>	Data Privacy [template]				
<input type="radio"/>	Default Sharepoint Auditing [template]				
<input type="radio"/>	GDPR for Db2 for z/OS [template]				
<input type="radio"/>	GDPR [template]				
<input type="radio"/>	Hadoop Policy [template]	3	2019-06-04 06:33:22		
<input type="radio"/>	HIPAA [template]	18	2019-06-04 06:33:22		
<input type="radio"/>	PCI [template]	18	2019-06-04 06:33:22		
<input type="radio"/>	PCI, Oracle EBS [template]	18	2019-06-04 06:33:22		
<input type="radio"/>	PCI, SAP [template]	18	2019-06-04 06:33:22		
<input type="radio"/>	Privileged Users Monitoring (black list) [template]	10	2019-06-04 06:33:22		

Total: 20 Selected: 0

◀ 1 ▶

Change policy analyzer settings

* Interval minutes

OK Cancel

Run ad hoc analysis

Start must be in the future

Count taken at start and end of duration

Security Policies

+ ✎ 📄 - ↺ 🗨 | Download as CSV | View logs and violation | Install | Analyze ▾ | ☒ Include templates | Filter

Name	Rules	Last changed	Last installed	Installed	Installation order	Selective audit trail
<input type="radio"/> Default - Ignore Data Activity for Unknown Con				<input checked="" type="checkbox"/>	1	false
<input type="radio"/> Allow-All [template]					0	false
<input type="radio"/> Basel II [template]					0	true
<input type="radio"/> Data Privacy - PII [template]					0	true
<input type="radio"/> Data Privacy [template]					0	true
<input type="radio"/> Default Sharepoint Auditing [template]					0	false
<input type="radio"/> GDPR for Db2 for z/OS [template]					0	true
<input type="radio"/> GDPR [template]					0	true
<input type="radio"/> Hadoop Policy [template]					0	false
<input type="radio"/> HIPAA [template]	18	2019-06-04 06:33:22			0	true
<input type="radio"/> PCI [template]	18	2019-06-04 06:33:22			0	true
<input type="radio"/> PCI, Oracle EBS [template]	18	2019-06-04 06:33:22			0	true
<input type="radio"/> PCI, SAP [template]	18	2019-06-04 06:33:22			0	true
<input type="radio"/> Privileged Users Monitoring (black list) [template]	10	2019-06-04 06:33:22			0	false
Total: 20 Selected: 0						
< 1 >						

Run ad hoc analysis

Collect statistics for a specific time range to understand impact of specific applications or policy rule changes

[Show currently schedule](#)

* Start date

* Duration

OK Cancel

View results menu

Security Policies						
<div><div><div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div></div><div>Download as CSV</div><div>View logs and violation</div><div>Install</div><div>Analyze ▾</div><div><input checked="" type="checkbox"/> Include templates</div><div>Filter</div></div></div>						
Name					installed	Installed
<input type="radio"/> Default - Ignore Data Activity for Unknown Connections [template]			<div><div>✓</div><div>Policy analyzer is currently running</div></div> <div><div>Stop policy analyzer</div><div>Change policy analyzer settings</div><div>Run ad hoc analysis</div></div> <div><div>View results</div><div>Ad hoc analysis</div><div>Continuous analysis</div></div>		06-04 06:31:18	<div>✓</div>
<input type="radio"/> Allow-All [template]						
<input type="radio"/> Basel II [template]						
<input type="radio"/> Data Privacy - PII [template]	19	2019-06-04 06:33:22				
<input type="radio"/> Data Privacy [template]	17	2019-06-04 06:33:22				

Difference in ad hoc vs. continuous analysis results

Continuous

- Can adjust time frame and view impact on results
- Line graph (no history for ad hoc)

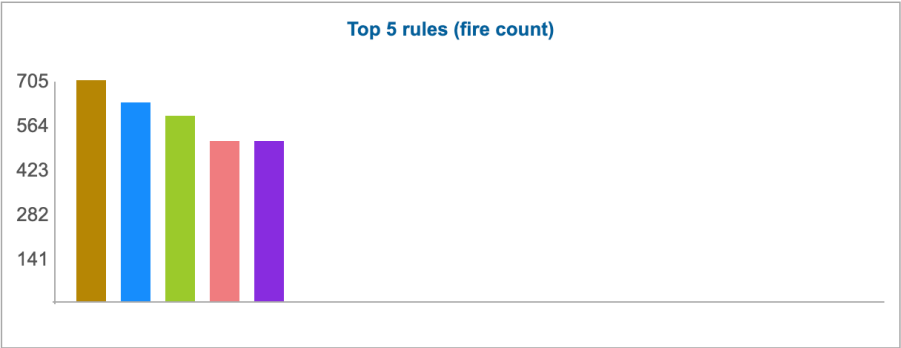
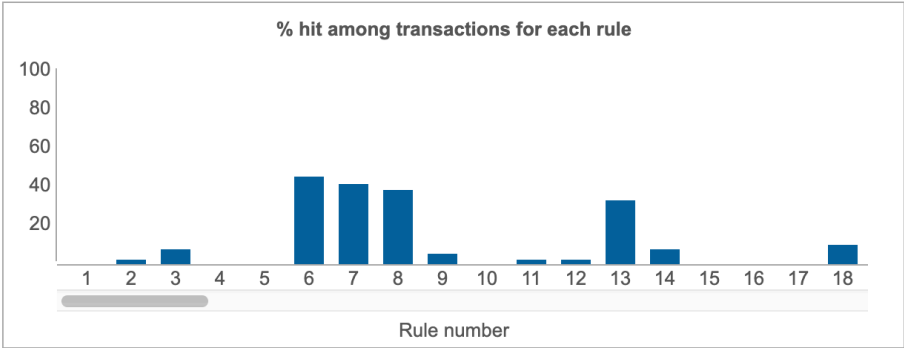
Ad hoc

- Single time frame
- But can select previous results from the drop down

Continuous analysis result

View continuous analysis results

Time frame: Last 10 Minutes 



Details for all policy rules

Download as CSV *Filter*

Number	Rule	Action	Fire count	% hit among transactions	% hit among rules	Policy
1	Failed Login - GDPR Personal Data - Log Violation by Admin Users	LOG ONLY	0	0	0	Smart Assistant GDPR
2	Failed Login - GDPR Personal Data - Alert if repeated	ALERT PER MATCH	10	2	0	Smart Assistant GDPR
3	SQL Error - GDPR Personal Data - Alert on Risk Indicative errors	ALERT PER MATCH	104	7	1	Smart Assistant GDPR
4	REVOKE Commands, GDPR Personal Data Sensitive Objects - Log full details	ALERT PER MATCH,LOG FULL DETAILS	0	0	0	Smart Assistant GDPR

View continuous analysis results

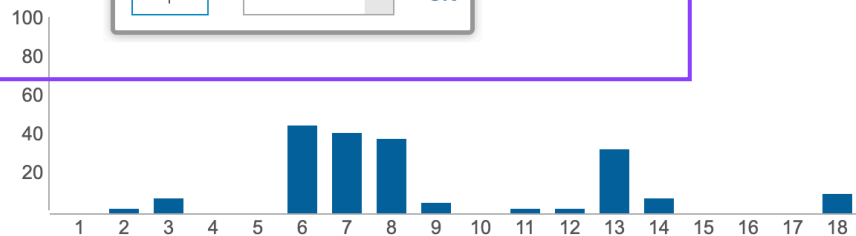
Time frame: Last 10 Minutes



Minutes

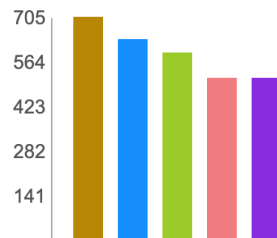
OK

ons for each rule



Rule number

Top 5 rules (fire count)



Details for all policy rules

Download as CSV

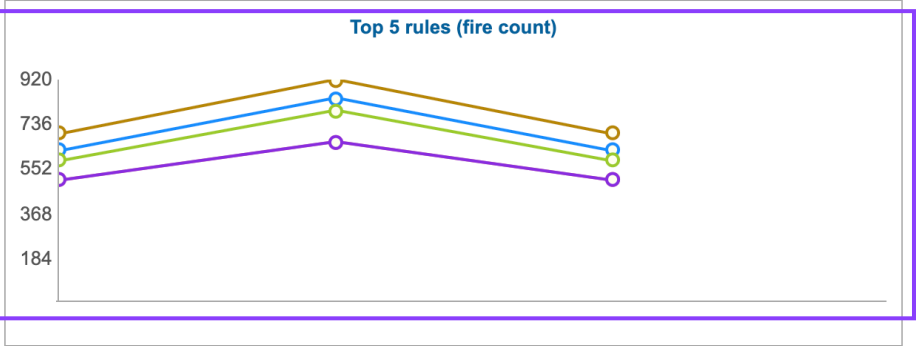
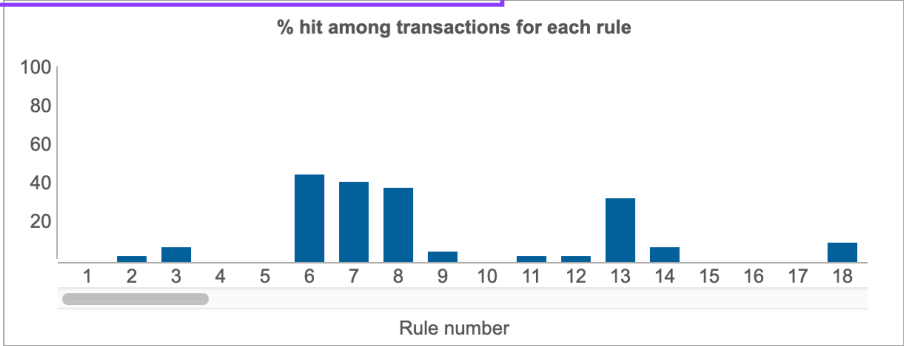
Filter



Number	Rule	Action	Fire count	% hit among transactions	% hit among rules	Policy
1	Failed Login - GDPR Personal Data - Log Violation by Admin Users	LOG ONLY	0	0	0	Smart Assistant GDPR
2	Failed Login - GDPR Personal Data - Alert if repeated	ALERT PER MATCH	10	2	0	Smart Assistant GDPR
3	SQL Error - GDPR Personal Data - Alert on Risk Indicative errors	ALERT PER MATCH	104	7	1	Smart Assistant GDPR
4	REVOKE Commands, GDPR Personal Data Sensitive Objects - Log full details	ALERT PER MATCH,LOG FULL DETAILS	0	0	0	Smart Assistant GDPR

View continuous analysis results

Time frame: Last 30 Minutes



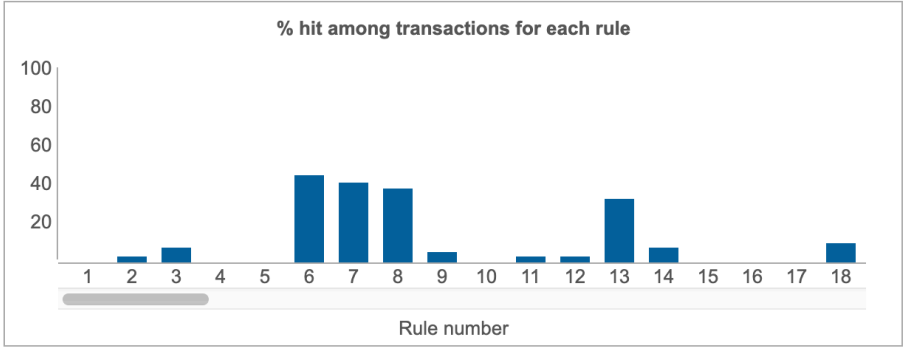
Details for all policy rules

Download as CSV		Filter					
Number	Rule	Action	Fire count	% hit among transactions	% hit among rules	Policy	
1	Failed Login - GDPR Personal Data - Log Violation by Admin Users	LOG ONLY	0	0	0	Smart Assistant GDPR	
2	Failed Login - GDPR Personal Data - Alert if repeated	ALERT PER MATCH	54	3	1	Smart Assistant GDPR	
3	SQL Error - GDPR Personal Data - Alert on Risk Indicative errors	ALERT PER MATCH	337	7	1	Smart Assistant GDPR	
4	REVOKE Commands, GDPR Personal Data Sensitive Objects - Log full details	ALERT PER MATCH,LOG FULL DETAILS	0	0	0	Smart Assistant GDPR	


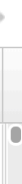
Ad hoc result

View ad hoc analysis results

Start time: 2019-06-10 14:15:00 

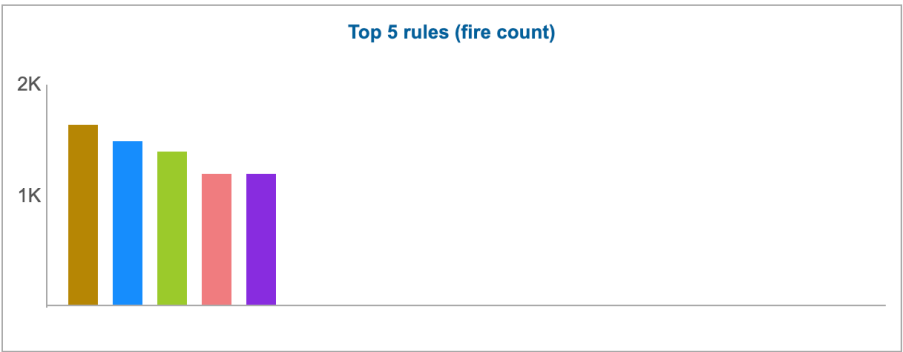
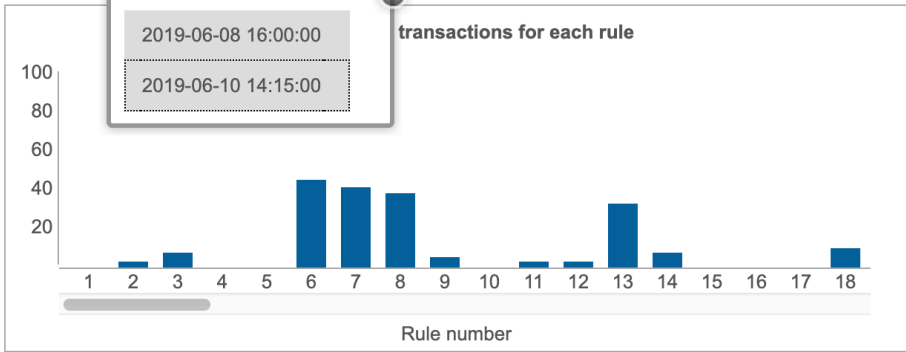


Details for all policy rules

Download as CSV		Filter					
Number	Rule	Action	Fire count	% hit among transactions	% hit among rules	Policy	
1	Failed Login - GDPR Personal Data - Log Violation by Admin Users	LOG ONLY	0	0	0	Smart Assistant GDPR	
2	Failed Login - GDPR Personal Data - Alert if repeated	ALERT PER MATCH	39	3	1	Smart Assistant GDPR	
3	SQL Error - GDPR Personal Data - Alert on Risk Indicative errors	ALERT PER MATCH	233	7	1	Smart Assistant GDPR	
4	REVOKE Commands, GDPR Personal Data Sensitive Objects - Log full details	ALERT PER MATCH,LOG FULL DETAILS	0	0	0	Smart Assistant GDPR	

View ad hoc analysis results

Start time: 2019-06-10 14:15:00



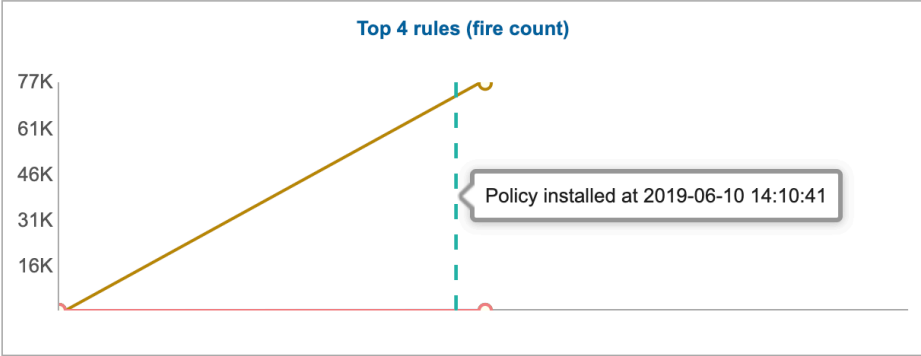
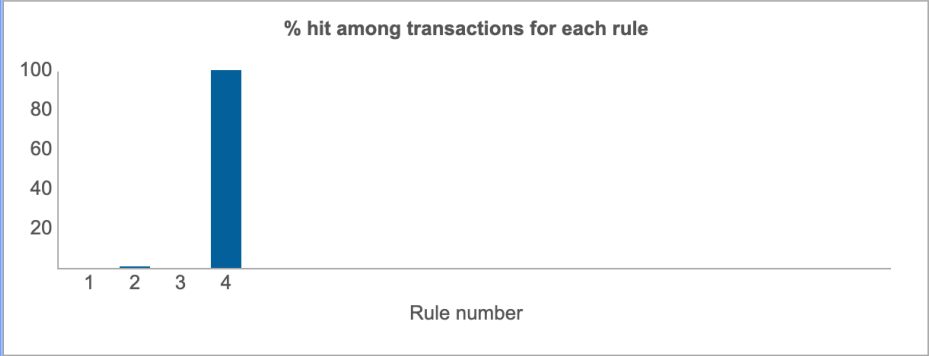
Details for all policy rules

<div>Download as CSV</div> <div>Filter</div>							<div></div>
Number	Rule	Action	Fire count	% hit among transactions	% hit among rules	Policy	
1	Failed Login - GDPR Personal Data - Log Violation by Admin Users	LOG ONLY	0	0	0	Smart Assistant GDPR	
2	Failed Login - GDPR Personal Data - Alert if repeated	ALERT PER MATCH	39	3	1	Smart Assistant GDPR	
3	SQL Error - GDPR Personal Data - Alert on Risk Indicative errors	ALERT PER MATCH	233	7	1	Smart Assistant GDPR	
4	REVOKE Commands, GDPR Personal Data Sensitive Objects - Log full details	ALERT PER MATCH,LOG FULL DETAILS	0	0	0	Smart Assistant GDPR	

Handles case where policy is
reinstalled/installed

View continuous analysis results

Time frame: Last 20 Minutes 

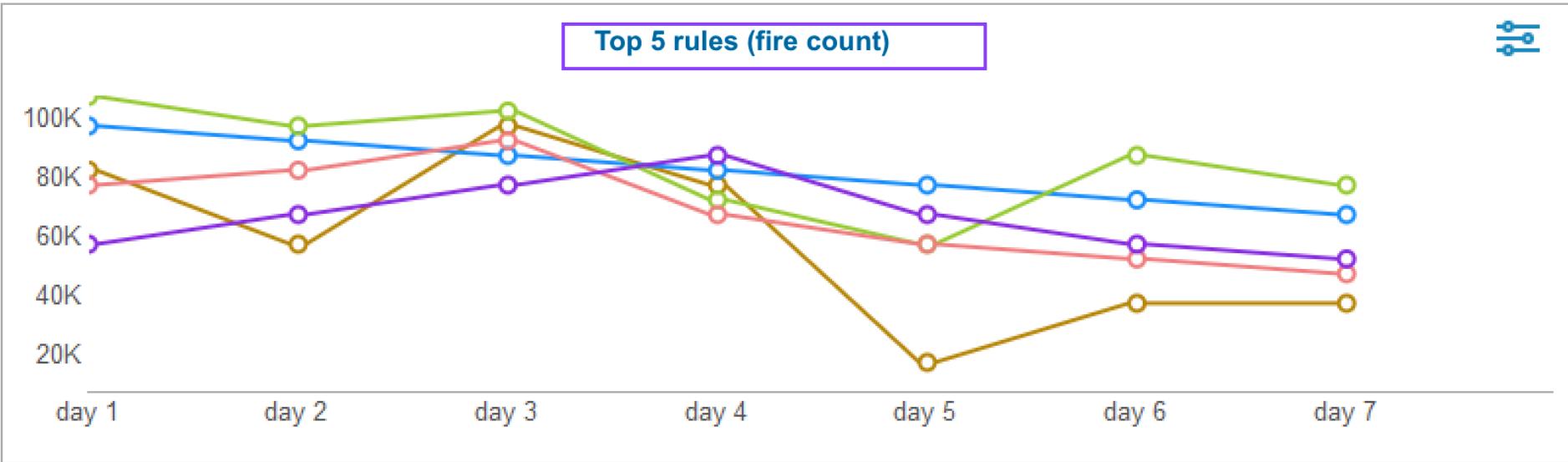


Details for all policy rules

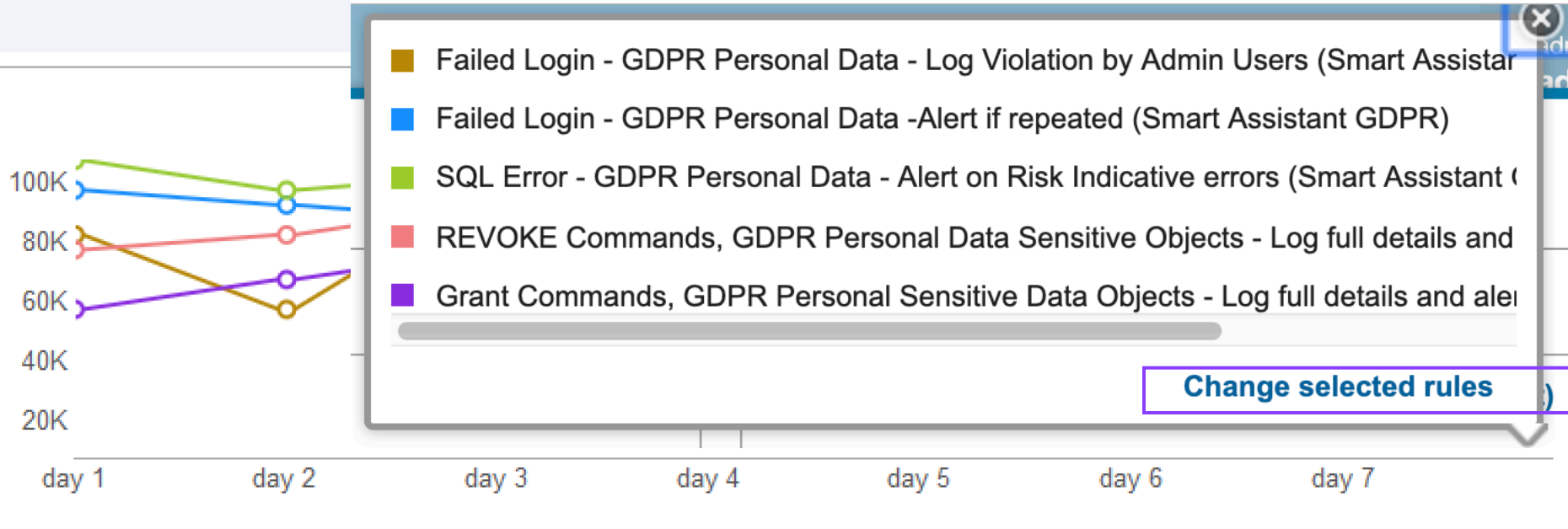
Download as CSV *Filter*

Number	Rule	Action	Fire count	% hit among transactions	% hit among rules	Policy
1	log deletes	LOG FULL DETAILS	0	0	0	Test dbadmin actions
2	select behavior	LOG ONLY	26	1	0	Test dbadmin actions
3	alter command	ALERT ONCE PER SESSION	0	0	0	Test dbadmin actions
4	nonadmin user behavior	LOG ONLY	75684	100	100	Test dbadmin actions

Viewing legend and changing rules shown on graph



Viewing legend

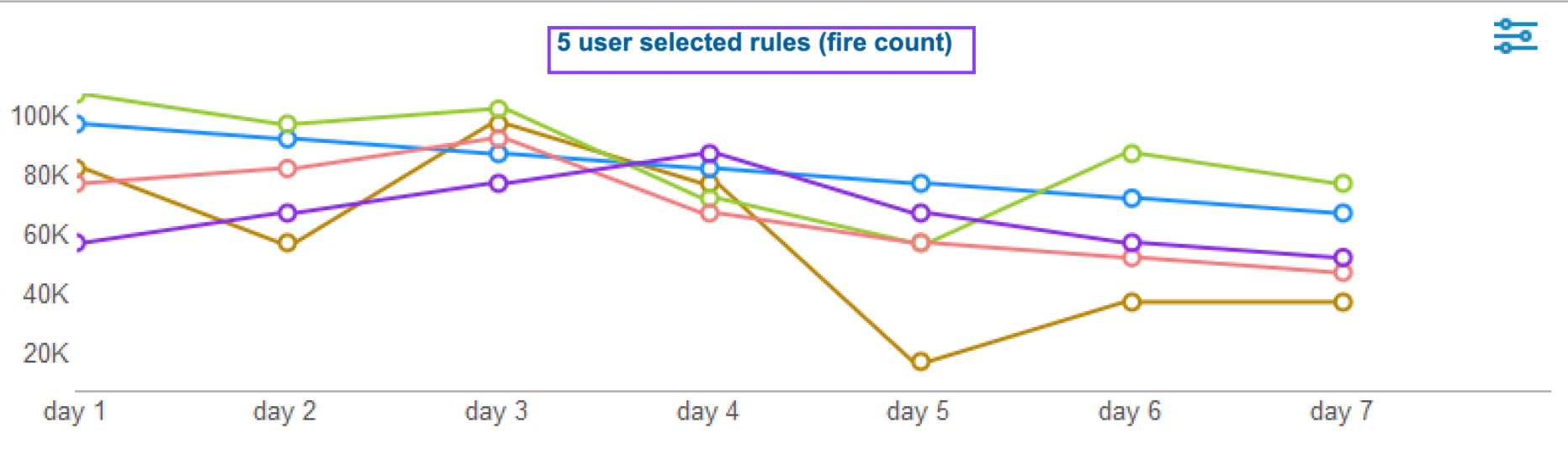


Changing rules

The screenshot displays a security management interface. On the left, a line chart shows data trends for 'day 1' with values ranging from 20K to 100K. The main area features a list of GDPR-related rules, each with a checkbox. Two rules are checked: 'Failed Login - GDPR Personal Data - Log Violation by Admin Users (Smart Assistant (GDPR))' and 'Failed Login - GDPR Personal Data -Alert if repeated (Smart Assistant GDPR)'. A 'Smart Assistant' dialog box is open on the right, and an 'OK' button is highlighted with a red box.

Rule Name	Checked
<input type="checkbox"/> DDL, DML and Select Commands, GDPR Personal Data Sensitive Objects - Log	No
<input checked="" type="checkbox"/> Failed Login - GDPR Personal Data - Log Violation by Admin Users (Smart Assistant (GDPR))	Yes
<input checked="" type="checkbox"/> Failed Login - GDPR Personal Data -Alert if repeated (Smart Assistant GDPR)	Yes
<input type="checkbox"/> GDPR Personal Data Admin User - Alert per match (violation) on DML and Sele	No
<input type="checkbox"/> GDPR Personal Data Authorized User, GDPR Personal Data Sensitive Objects	No
<input type="checkbox"/> GDPR Personal Data Unauthorized User - Alert per match (violation) (Smart As	No

Title is updated to show its been customized



Limitations

- Only support 128 rules max for all policies.
- Only for DAM policies (not FAM or Session level).
- No support for z/os audit.
- No ability to view schedules for ad hoc results
- Installed policy must have rules (ie no data is shown for Allow All default policy)

Trouble Shooting

If no data show up in gui result page:

- No rules in the current policy
- Snif is not running
- Snif restarted during ad-hoc collection (Ad-hoc Mode)
- Policy reinstalled during ad-hoc collection (Ad-hoc Mode)

Check the logs for event sequence to understand policy analyzer behavior.

```
2019-06-05 15:55:29,157 INFO: Snif policy analyzer service start
2019-06-05 15:55:29,160 INFO: Checking ad-hoc schedule
2019-06-05 15:55:29,162 INFO: No new ad-hoc schedule
2019-06-05 15:55:29,163 INFO: Started policy analyzer continuous stats collection with 2 minutes interval
2019-06-05 15:55:47,814 INFO: Changed interval of continuous stats collection to 3
2019-06-05 16:49:16,896 INFO: Checking ad-hoc schedule
2019-06-05 16:49:16,899 INFO: No new ad-hoc schedule
2019-06-05 16:59:43,930 INFO: Checking ad-hoc schedule
2019-06-05 16:59:43,933 INFO: New schedule at 2019-06-05 17:00:00 with duration of 1 scheduled internally.
2019-06-05 17:00:00,067 INFO: Ad-hoc collection starting at 2019-06-05 17:00:00 has started
2019-06-05 17:01:00,289 INFO: Ad-hoc collection starting at 2019-06-05 17:00:00 has ended
2019-06-05 17:01:00,390 INFO: No new ad-hoc schedule
2019-06-05 17:14:39,378 INFO: Checking ad-hoc schedule
2019-06-05 17:14:39,381 INFO: No new ad-hoc schedule
```

Trouble Shooting - Logs

Logs informative events:

- Start policy analyzer continuous collection
- Stop policy analyzer continuous collection
- Change interval of continuous collection
- Ad-hoc collection started
- Ad-hoc collection ended
- No new ad-hoc schedule
- New ad-hoc schedule at <timestamp>
- Policy analyzer service started
- Skipping stats for this interval because sniff restarted
- Skipping stats for this interval because policy reinstalled

Trouble Shooting - Logs

Logs warning events:

- Policy analyzer service shutdown
- Skip stats for this interval because sniff is not running
- Skip stats for this interval because there are no rules installed
- Received command when policy analyzer service is off.
- Number of rules exceeds 128

Log error events:

- sniff_stats_utils can't map to shared memory
- Mysql operation errors.
- Other exceptions.

Location:

- \$GUARD_LOG_DIR/snif_policy_analyzer/snif_policy_analyzer.log

Guardium V11 New Release Training

Smart Assistant

Contents

Overview

Use cases

Demo

Architecture

Implementation considerations

Troubleshooting

Q & A

Reference materials

Overview

Enables new users (or existing users needing to meet a new compliance standard) an end-end flow for quickly setting up compliance policies, groups and reports.

Follows best practices flow

What's New

- No longer need to have S-TAPs installed *before* using the Smart Assistant/Quick Start
- More options for sensitive data identification
- More contextual information: prerequisites, individual step help, how to videos.

Benefits

- Better fit to diversity of customer environments
- Easier to understand full scope of functionality
- Addresses key customer pain points

Known painpoints

- Customers don't know where to start
- Customers are stuck if they didn't already install GIM listeners
- Customers are not aware that we schedule classification for them (and are not able to change the schedule time from the quick start)
- Customers don't know what to do next (ie after the setup is run)

How the Smart Assistant addresses the pain points

- Prereqs (added based on feedback)
- Available databases do NOT have to have S-TAPs on them to appear in the wizard
- Search for sensitive data is a separate step
 - Can use classifier, import from csv or skip
- Summary page
 - Provides more details about what will be created along with links out to more details
- Summary tile
 - Provides information on which dbs need S-TAPs

Use Cases

New customer

A customer new to Guardium wants to set up compliance policies quickly. They have to start from scratch—defining databases, finding sensitive data, and creating and installing policies and reports.

Current customer

A current Guardium customer wants to set up policies to help meet new compliance standards, such as GDPR. They already know where their sensitive data resides

A current customer wants to expand compliance monitoring to new datasources. They will discover sensitive data and set up rules together

CISO

A CISO wants to see her organization's progress towards meeting compliance standards within Guardium.

Admin

Guardium admin wants to understand what still needs to be done to meet a particular compliance standard within Guardium.

Demo

New Welcome Page

Database inventory

- importing databases from a CSV file

New Smart Assistant for Compliance monitoring

New Dashboard for viewing compliance progress and health



12:15



User Interface



User Interface Search



admin

admin admin



Machine Type
Standalone



Get Started on Data Protection with Guardium



Inventory your databases

[Learn more](#)

[See it in action](#)



Discover sensitive data

[Learn more](#)

[See it in action](#)



Set up compliance monitoring

[Learn more](#)

[See it in action](#)



Active threat analytics

[See it in action](#)

[Risk spotter](#)

[See it in action](#)

[Investigation dashboard](#)

[See it in action](#)

[Learn more](#)



Inventory your

Learn more

See it in action

Learn more about what's new
Guardium release notes

DSDfirstdraft_test

Guardium v11 welcome videos

Discover sensitive data

Watch later

Share

IBM

0:02 / 5:16

YouTube



ve threat analytics
it in action
spotter
it in action
stigation dashboard
it in action
n more



12:15



User Interface



User Interface Search



admin

admin admin



Machine Type
Standalone



Get Started on Data Protection with Guardium



Inventory your databases

[Learn more](#)

[See it in action](#)



Discover sensitive data

[Learn more](#)

[See it in action](#)



Set up compliance monitoring

[Learn more](#)

[See it in action](#)



Active threat analytics

[See it in action](#)

[Risk spotter](#)

[See it in action](#)

[Investigation dashboard](#)

[See it in action](#)

[Learn more](#)



12:16



User Interface



User Interface Search

admin
admin adminMachine Type
Standalone

Compliance Monitoring



Known databases

0

Configured databases

0

Unconfigured databases

0

Compliance dashboard

Databases



Configure monitoring

Import from CSV

Datasource actions



Exclude configured databases

Filter



Database properties

Instance name

Database name

Type

Host name

IP address

Datasource

No items to display

Total: 0 Selected: 0



12:16



User Interface



User Interface Search

admin
admin adminMachine Type
Standalone

Compliance Monitoring



Known databases

0

Configured databases

0

Unconfigured databases

0

Compliance dashboard

Databases



Configure monitoring

Instance name

Database

ases

Filter



Datasource

Import from CSV

Select a CSV file that contains information about your databases. After clicking **Load**, you will identify columns from the CSV file to import as database properties.

Select file to upload

Browse

* Field delimiter

,

Load

Cancel

Total: 0 Selected: 0



12:17



User Interface



User Interface Search

admin
admin adminMachine Type
Standalone

Compliance Monitoring

Known database

0

Compliance dashboard

Databases



Configure monitoring

Instance name

Database

Total: 0 Selected: 0

Import from CSV

Select columns from the CSV file to import as database properties. Values imported for the server name, service name, or instance name property are automatically assigned to the correct property based on the associated database type.

* Host name/IP

IP

* Port number

Port

* Database type

OS

User name

None

Password

None

Service name

None

Database name

None

Server name

None

Instance name

None

OK

Cancel

Unconfigured databases

0

Databases

Filter

Datasource



12:18



User Interface



User Interface Search



admin

admin admin

Machine Type
Standalone

Compliance Monitoring



Known databases

2 ↗

Configured databases

0

Unconfigured databases

2 ↗

Compliance dashboard

Databases



Configure monitoring

Import from CSV

Datasource actions



Exclude configured databases

Filter



	Database properties					Datasource	Compliance type	
	Instance name	Database name	Type	Host name	IP address		Unconfigured	
<input type="checkbox"/>		DN0KALP	DB2		9.70.164.81:50000			
<input type="checkbox"/>	in2kalp		INFORMIX		9.70.164.81:1403			

Total: 2 Selected: 0



12:19



User Interface



User Interface Search

admin
admin adminMachine Type
Standalone

Compliance Monitoring



Known databases

2 ↗

Configured databases

0

Unconfigured databases

2 ↗

Compliance dashboard

Databases

Set up compliance monitoring



Help meet compliance standards by quickly installing policies, populating groups, and running reports for monitoring database activity.





12:19



User Interface



User Interface Search

admin
admin adminMachine Type
Standalone

Set up compliance monitoring



Step 1

Before you begin

Collapse ? □

The smart assistant for compliance monitoring automates the following activities through a simple workflow:

- Identify databases to monitor
- Install compliance monitoring policies
- Schedule policy updates
- Populate groups with objects to monitor
- Run activity-monitoring reports
- Scan for database tables containing sensitive data

Configuring scans for database tables containing sensitive data requires database credentials with the correct permissions. Gather the credentials and verify permissions before you begin or optionally configure the scans later. [Get scripts illustrating the required permissions.](#)

After completing the smart assistant workflow, compliance monitoring policies are distributed to all collectors attached to the central manager and you are ready to begin protecting data.

Important: monitoring agents (S-TAPs) can be installed on your database servers after completing the smart assistant workflow, but database traffic is not examined until the agents are installed. Open [Deploy Monitoring Agents](#) to get started.

Next

Step 2

Select compliance type

Expand ? □

Step 3

Select databases to monitor

Expand ? □

Compliance Monitoring



12:19



User Interface



User Interface Search



admin

admin admin

Machine Type
Standalone

Set up compliance monitoring

✔ Step 1 *Before you begin* [Expand](#) ? □

Step 2 *Select compliance type* [Collapse](#) ? □

Which compliance type do you want to configure?

Select compliance type

Next

Step 3 *Select databases to monitor* [Expand](#) ? □

Step 4 *Search for sensitive data* [Expand](#) ? □

Step 5 *Summary* [Expand](#) ? □

Run setup

Cancel

Compliance Monitoring



12:19



User Interface



User Interface Search

admin
admin adminMachine Type
Standalone

Set up compliance monitoring

Step 1 *Before you begin* **Expand** ? □

Step 2 *Select compliance type* **Collapse** ? □

Which compliance type do you want to configure?

Select compliance type

Basel Committee on Banking Supervision (BASEL II)

General Data Protection Regulation (GDPR)

General Data Protection Regulation for Db2 for z/OS (GDPR for Db2 for z/OS)

Health Insurance Portability and Accountability Act (HIPAA)

Payment Card Industry Data Security Standard (PCI)

Personally Identifiable Information (PII)

Sarbanes-Oxley Compliance (SOX)

Expand ? □

Expand ? □

Expand ? □

Run setup

Cancel

Compliance Monitoring



12:20



User Interface



User Interface Search

admin
admin adminMachine Type
Standalone

Set up compliance monitoring

- Step 1 *Before you begin* [Expand](#)
- Step 2 *GDPR type selected* [Expand](#)
- Step 3** *Select databases to monitor* [Collapse](#)



Import from CSV

Filter



Database properties

	Database properties					Compliance type	
	Instance name	Database name	Type	Host name	IP address	Ready for policy	Unconfigured
<input type="checkbox"/>		DN0KALP	DB2		9.70.164.81:50000	Needs agents installed	
<input type="checkbox"/>	in2kalp		INFORMIX		9.70.164.81:1403	Needs agents installed	
<input type="checkbox"/>							



12:20



User Interface



User Interface Search

admin
admin adminMachine Type
Standalone

Set up compliance monitoring

Step 4

Search for sensitive data

Collapse ?

Compliance monitoring policies contain rules for monitoring access to database tables. Effective compliance monitoring depends on identifying tables that contain sensitive data like credit card numbers or personally-identifiable information.

How do you want to identify database tables containing sensitive data?

☐ Scan for tables ☒ Manually define table names ☐ Skip for now

Import the names of tables containing sensitive data from one or more CSV files and manually refine the list using the add and remove actions. The list of tables is added to a sensitive-objects group for monitoring.

Browse

* Field delimiter

,

Column to import

Load



Filter



Table name

No items to display

Total: 0 Selected: 0



12:20



User Interface



User Interface Search

admin
admin adminMachine Type
Standalone

Set up compliance monitoring

Step 4

Search for sensitive data

Collapse ? □

Compliance monitoring policies contain rules for monitoring access to database tables. Effective compliance monitoring depends on identifying tables that contain sensitive data like credit card numbers or personally-identifiable information.

How do you want to identify database tables containing sensitive data?

☐ Scan for tables ☐ Manually define table names ☒ Skip for now

When establishing a Guardium deployment, you may initially want to focus on monitoring and traffic volume. Selecting Skip for now allows you to identify tables containing sensitive data at a later time.

Important: your compliance monitoring strategy is not complete without identifying and monitoring the sensitive data in your databases.



12:21



User Interface



User Interface Search

admin
admin adminMachine Type
Standalone

Set up compliance monitoring

Step 4

Search for sensitive data

Collapse ?

Compliance monitoring policies contain rules for monitoring access to database tables. Effective compliance monitoring depends on identifying tables that contain sensitive data like credit card numbers or personally-identifiable information.

How do you want to identify database tables containing sensitive data?

☒ Scan for tables ☐ Manually define table names ☐ Skip for now

Select databases to scan for sensitive data. Tables containing sensitive data are added to a sensitive-objects group for monitoring, and the scan is scheduled to run once weekly.

Test datasource credentials				Filter	
<input checked="" type="checkbox"/>	Instance name	Database name	Type	Host name	Ready for classification
<input checked="" type="checkbox"/>		DN0KALP	DB2	9.70.164.81:50000	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	in2kalp		INFORMIX	9.70.164.81:1403	<input checked="" type="checkbox"/>
Total: 2 Selected: 2					

Compliance Monitoring



12:21



User Interface



User Interface Search

admin
admin adminMachine Type
Standalone

Set up compliance monitoring

Step 5

Summary

Collapse ? □

Clicking **Run Setup** takes the following actions:

- | | | |
|--|---|------------------------------|
| ✓ Install compliance monitoring policy | Smart Assistant GDPR | View details |
| ✓ Schedule policy reinstallation | Run once every day | Edit |
| ✓ Populate server IP group | GDPR Personal Data Authorized Server IPs | |
| ✓ Install classification policy | Smart Assistant GDPR scenario | View details |
| ✓ Schedule classification | Run once on specific days | Edit |
| ✓ Create audit process | Audit process for Smart Assistant GDPR scenario | |
| ✓ Send results to contacts | admin | Add |

You must complete the following actions:

- | | | |
|--|---|---|
| ⚠ Populate groups | 5 | View details |
| ⚠ Install monitoring agents (S-TAPs) for databases | 2 | Install monitoring agents |
| ⚠ Review classification results and remove false positives | | Learn more |
| ✓ Add to my to-do list | | |



12:21



User Interface



User Interface Search

admin
admin adminMachine Type
Standalone

Set up compliance monitoring

Step 5

Collapse ?

Clicking **Run Setup** takes the following actions:

- ✓ Install compliance monitoring
- ✓ Schedule policy reinstallation
- ✓ Populate server IP groups
- ✓ Install classification policies
- ✓ Schedule classification
- ✓ Create audit process
- ✓ Send results to contacts

You must complete the following actions:

- ⚠ Populate groups
- ⚠ Install monitoring agents
- ⚠ Review classification results and remove false positives

- ☒ Add to my to-do list

Smart Assistant GDPR policy rules

The following rules are installed with the policy.

1. SQL Error - GDPR Personal Data - Alert on Risk Indicative errors
2. DDL, DML and Select Commands, GDPR Personal Data Sensitive Objects - Log Full Details
3. GDPR Personal Data Unauthorized User - Alert per match (violation)
4. Grant Commands, GDPR Personal Sensitive Data Objects - Log full details and alert
5. Unauthorized Clients access to Personal Data Sensitive Objects - Alert Per Match
6. GDPR Personal Data Admin User - Alert per match (violation) on DML and Select Commands
7. GDPR Personal Data Authorized User, GDPR Personal Data Sensitive Objects - Log Full Details
8. REVOKE Commands, GDPR Personal Data Sensitive Objects - Log full details and alert
9. Failed Login - GDPR Personal Data - Log Violation by Admin Users
10. Failed Login - GDPR Personal Data -Alert if repeated

Close

[Learn more](#)



12:21



User Interface



User Interface Search

admin
admin adminMachine Type
Standalone

Set up compliance monitoring

Step 5

Summary

Collapse ? □

Clicking **Run Setup** takes the following actions:

- | | | |
|--|---|------------------------------|
| ✓ Install compliance monitoring policy | Smart Assistant GDPR | View details |
| ✓ Schedule policy reinstallation | Run once every day | Edit |
| ✓ Populate server IP group | GDPR Personal Data Authorized Server IPs | |
| ✓ Install classification policy | Smart Assistant GDPR scenario | View details |
| ✓ Schedule classification | Run once on specific days | Edit |
| ✓ Create audit process | Audit process for Smart Assistant GDPR scenario | |
| ✓ Send results to contacts | admin | Add |

You must complete the following actions:

- | | | |
|--|---|---|
| ⚠ Populate groups | 5 | View details |
| ⚠ Install monitoring agents (S-TAPs) for databases | 2 | Install monitoring agents |
| ⚠ Review classification results and remove false positives | | Learn more |
| ✓ Add to my to-do list | | |



12:21



User Interface



User Interface Search

admin
admin adminMachine Type
Standalone

Set up compliance monitoring

Step 5

Summary

Collapse ?

Clicking **Run Setup** takes

- ✓ Install compliance
- ✓ Schedule policy
- ✓ Populate server
- ✓ Install classification
- ✓ Schedule class
- ✓ Create audit pr
- ✓ Send results to

You must complete the following

- ⚠ Populate group
- ⚠ Install monitoring agents (S-TAPs) for databases 2
- ⚠ Review classification results and remove false positives
- ☒ Add to my to-do list

Schedule policy reinstallation

Schedule by

Day

Select days

Every Day

* Start schedule at

10:30 AM

Begin schedule

6/7/2019

12:27 PM

Save

Close

[Install monitoring agents](#)[Learn more](#)

Compliance Monitoring



Compliance Monitoring

Known databases

2 ↗

Configured databases

2 ↗

GDPR

2

Unconfigured databases

0

Compliance dashboard

Databases

General Data Protection Regulation (GDPR)



Scanning for sensitive data

Last scan: None

Matches found: None

Databases without monitoring agents
installed: 2[Deploy agents](#)

Monitoring enabled

Traffic last captured: 2019-06-07 12:24:46



Sensitive objects

[Populate group](#)

Applications (Client IP)

[Populate group](#)

Users

[Populate group](#)

Updated: 2019-06-07 12:29:12

[View details](#)

Set up compliance monitoring

Help meet compliance standards by quickly installing policies, populating groups, and running reports for monitoring database activity.



How to edit configuration



Compliance Monitoring

Known databases

2 ↗

Configured databases

2 ↗

GDPR

2

Unconfigured databases

0

Compliance dashboard

Databases

General Data Protection Regulation (GDPR)



Scanning for sensitive data

Last scan: None

Matches found: None

Databases without monitoring agents
installed: 2[Deploy agents](#)

Monitoring enabled

Traffic last captured: 2019-06-07 12:24:46



Sensitive objects

[Populate group](#)

Applications (Client IP)

[Populate group](#)

Users

[Populate group](#)

Updated: 2019-06-07 12:29:12

[View details](#)

Set up compliance monitoring

Help meet compliance standards by quickly installing policies, populating groups, and running reports for monitoring database activity.



Viewing details pane



Compliance Monitoring

Known databases

2 ↗

Configured databases

2 ↗

GDPR

2

Unconfigured databases

0

Compliance dashboard

Databases

General Data Protection Regulation (GDPR)



Scanning for sensitive data

Last scan: None

Matches found: None

Databases without monitoring agents
installed: 2[Deploy agents](#)

Monitoring enabled

Traffic last captured: 2019-06-07 12:24:46



Sensitive objects

[Populate group](#)

Applications (Client IP)

[Populate group](#)

Users

[Populate group](#)

Updated: 2019-06-07 12:29:12

[View details](#)

Set up compliance monitoring

Help meet compliance standards by quickly installing policies, populating groups, and running reports for monitoring database activity.



Compliance Monitoring

Known databases

2 ↗

Configured databases

2 ↗

Compliance dashboard

Databases

General Data Protection Regulation (GDPR)

✓ Scanning for sensitive data

Last scan: None

Matches found: None

✗ Databases without monitoring agents installed: 2

[Deploy agents](#)

✓ Monitoring enabled

Traffic last captured: 2019-06-11 11:39:02

✗ Sensitive objects

[Populate group](#)

✗ Applications (Client IP)

[Populate group](#)

✗ Users

[Populate group](#)

Updated: 2019-06-11 11:40:14

[View details](#)

Set up compliance

Help meet compliance
policies, populating
monitoring groups

General Data Protection Regulation (GDPR)

Updated: 2019-06-11 11:39:02

Summary

Databases

Policies

Reports

Databases

2

Policies

2

Reports

16

▼ Groups

Group name	Type	Members
GDPR Personal Data Authorized Client IPs	Client IP	0
Database DML and SELECT Commands	COMMANDS	26
Database DML, DDL, SELECT, DROP, DELETE and MODIFY Commands	COMMANDS	302
GRANT Commands	COMMANDS	3
REVOKE Commands	COMMANDS	3
Risk-indicative Error Messages	DB Error Codes	0
GDPR Personal Data Sensitive Objects	OBJECTS	0
GDPR Personal Data Authorized Server IPs	Server IP	2
GDPR Personal Data Admin Users	USERS	0
GDPR Personal Data Authorized Users	USERS	0

General Data Protection Regulation (GDPR)



Updated: 2019-06-11 11:39:02

Summary

Databases

Policies

Reports

Databases associated with this compliance type: 2

Instance name	Database name	Type	Server	Has S-TAP
on8swan0	DN1KALRH	DB2	9.70.164.92	
		ORACLE	9.70.144.36	

General Data Protection Regulation (GDPR)



Updated: 2019-06-11 11:39:02




Summary

Databases

Policies

Reports

Databases associated with this compliance type: 2

Instance name	Database name	Type	Server	Has S-TAP
on8swan0	DN1KALRH	DB2	9.70.164.92	 
		ORACLE	9.70.144.36	

Compliance Monitoring

Known databases
2 ↗

Configured databases
2 ↗

General Data Protection Regulation (GDPR)

Updated: 2019-06-11 11:39:02

Summary

Databases

Policies

Reports

Compliance dashboard

Databases

General Data Protection Regulation (GDPR)

✓ Scanning for sensitive data

Last scan: None

Matches found: None

✗ Databases without monitoring agents installed: 2

✓ Monitoring enabled

Traffic last captured: 2019-06-11 11:39:02

✗ Sensitive objects

✗ Applications (Client IP)

✗ Users

Updated: 2019-06-11 11:40:14

Confirmation

Verify that monitoring agents (S-TAPs) are installed and the correct database IP addresses are in the Server IP group. Traffic is not monitored if monitoring agents are not installed. Continue?

☐ Do not ask again

Yes

No

Databases associated with this compliance type: 2

Type

DB2

ORACLE

Server

9.70.164.92

9.70.144.36

Has S-TAP

✗

✗

Populate group

Populate group

Populate group

View details

General Data Protection Regulation (GDPR)



Updated: 2019-06-11 11:39:02

Summary

Databases

Policies

Reports

Policies associated with this compliance type:

► Discovery scenario: Smart Assistant GDPR scenario

▼ Security policy: Smart Assistant GDPR

[Reset to default](#)

1. Failed Login - GDPR Personal Data - Log Violation by Admin Users
2. Failed Login - GDPR Personal Data -Alert if repeated
3. SQL Error - GDPR Personal Data - Alert on Risk Indicative errors
4. REVOKE Commands, GDPR Personal Data Sensitive Objects - Log full details and alert
5. Grant Commands, GDPR Personal Sensitive Data Objects - Log full details and alert
6. DDL, DML and Select Commands, GDPR Personal Data Sensitive Objects - Log Full Details
7. GDPR Personal Data Authorized User, GDPR Personal Data Sensitive Objects - Log Full Details
8. GDPR Personal Data Admin User - Alert per match (violation) on DML and Select Commands
9. GDPR Personal Data Unauthorized User - Alert per match (violation)
10. Unauthorized Clients access to Personal Data Sensitive Objects - Alert Per Match

General Data Protection Regulation (GDPR)



Updated: 2019-06-11 11:39:02

Summary

Databases

Policies

Reports

Reports associated with this compliance type: 16

▼ Security of Processing

- GDPR - Higher Risk SQL Errors**
- GDPR - Policy Violations**
- GDPR - Personal Data Objects Audit Trail**
- GDPR - Personal Data Servers Audit Trail**
- GDPR - Access Management GRANT and REVOKE Commands**
- GDPR - Login Failure to Personal Data DBs**
- GDPR - After Hours Access to Personal Data**
- GDPR - Unauthorized Application Access**
- GDPR - Unauthorized Users Access**
- GDPR - Administrative Activity on Personal DBs**
- GDPR - DDL Activity of Personal DBs**

▼ Data Subject Rights

- GDPR - Data Subject Delete Audit Trail**
- GDPR - Data Subject Rectification Audit Trail**
- GDPR - Data Subject Access Audit Trail**

▼ Personal Data Definitions

GDPR and GDPR -/OS - Discarded Personal Data Objects

Compliance Health Dashboard



Setup



Get Started on Data Protection with Guardium

Smart Assistant

Deploy Monitoring Agents

Compliance Health Monitor Dashboard

Compliance Monitoring

Tools and Views

Central Management

Custom Classes

Reports



Discover sensitive data

[Learn more](#)

[See it in action](#)



Set up compliance monitoring

[Learn more](#)

[See it in action](#)



Active threat analytics

[See it in action](#)

Risk spotter

[See it in action](#)

Investigation dashboard

[See it in action](#)

[Learn more](#)

>>

📱

🔧

⚙️

🕶️

🛡️

🔍

🔒

✅

📈

📊

🕒

👤

Known databases

23 ↗

Configured databases

5 ↗

PII

1

HIPAA

2

PCI

1

SOX

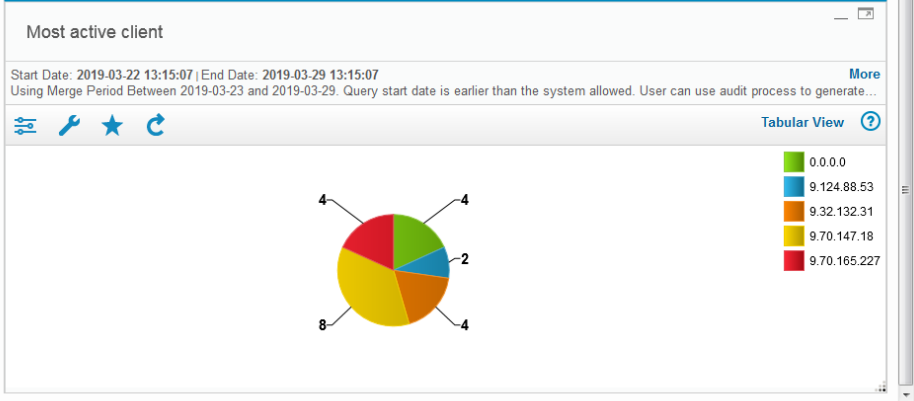
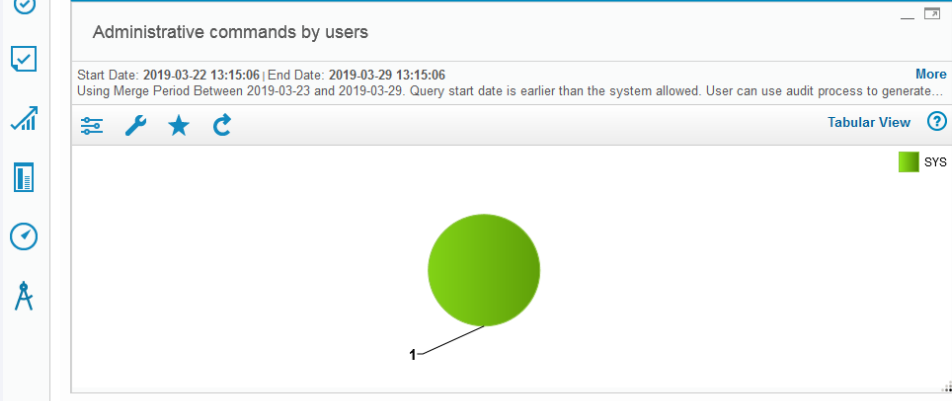
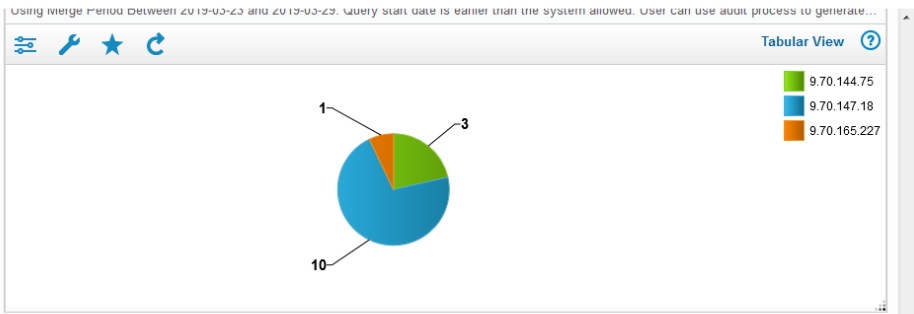
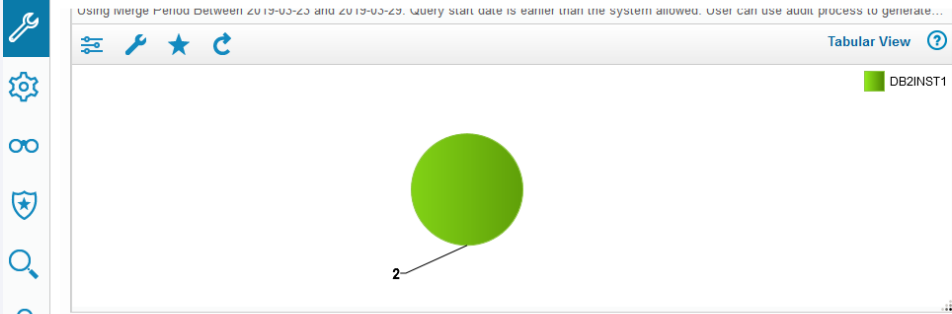
4

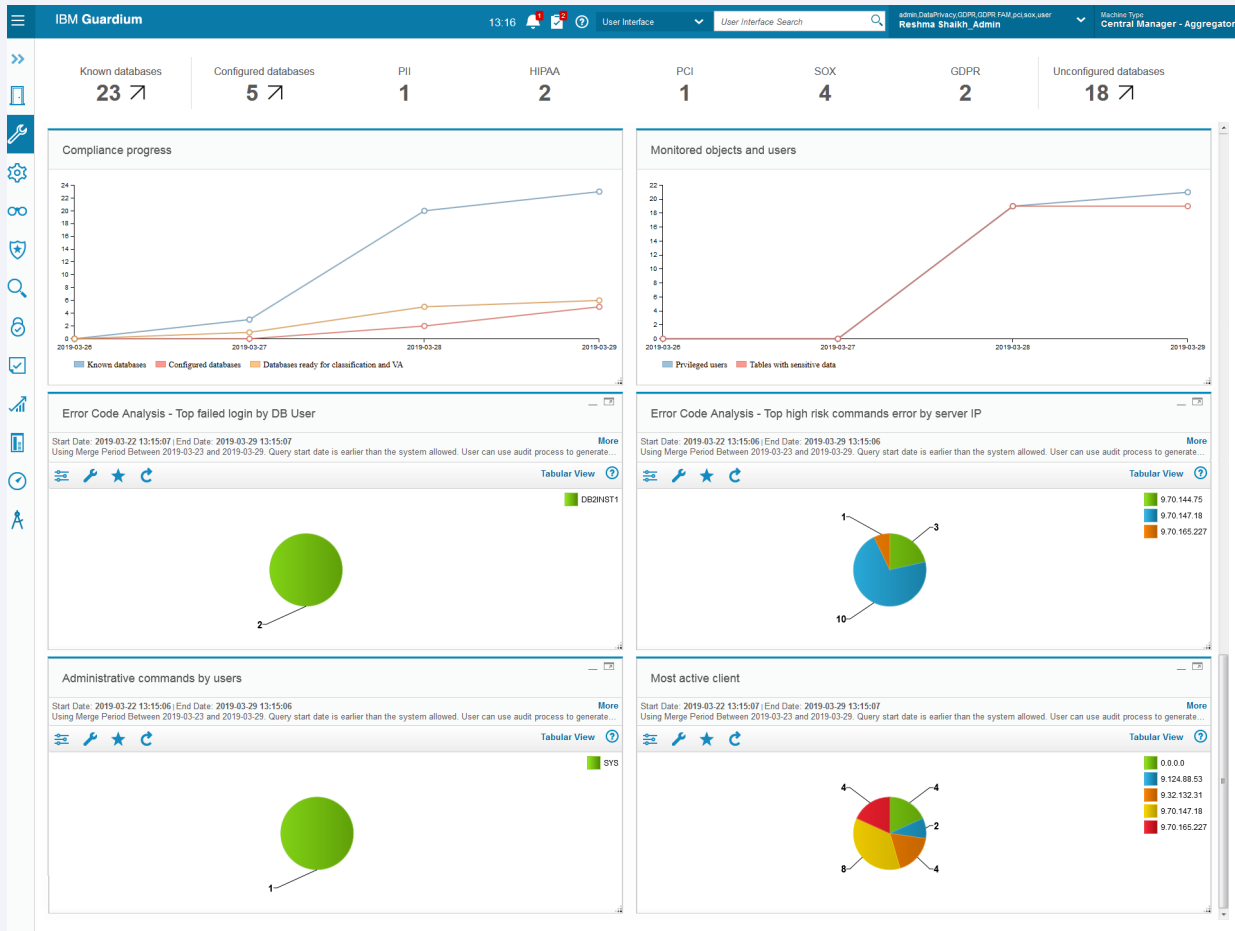
GDPR

2

Unconfigured databases

18 ↗





Implementation considerations: Limitations/Constraints

- Single classification process for each standard
- Users need to change report parameters (ie to specify remote data source) to see data for the compliance reports
- When importing from CSV
 - its CSV not XLS (excel format)
 - the first row defines column names.
 - Each row is complete, meaning that empty fields are accounted for with a delimiter (for example, a comma).
 - Database type is defined using any of the following case-insensitive strings (that can be found in the online help)
 -

Guardium V11 New Release Training

Guardium Integration with CyberArk

Agenda

Overview

Why use CyberArk

CyberArk setup

Guardium integration with CyberArk

Demo

Internal: Troubleshooting

Q & A

Why use CyberArk

- Remove credentials from application or scripts and put them into a secured centralized place (called the Vault).
- Periodical password changes are much easier and can be handled by your company's policy automatically, including saving the Guardium admin and DBA's time.
- All accesses/changes will be tracked for audit.
- Allow access to only trusted applications to enhance application security.
- Adhere to strong password policies.

Why use CyberArk

CyberArk Application Identity Manager (AIM) agent

Why we chose this solution?

- HA-- When the vault is down, datasources are still accessible provided that the password has not changed.
- Performance-- No trip to the vault unless absolutely required.
- Highly recommended by our partner CyberArk as the implementation approach.
- CyberArk agent is required on all Guardium appliances that fetch credentials from CyberArk.
(Reminder: install it on a backup CM server as well!)
- Guardium fetches both username and password from CyberArk.

CyberArk setup

- **Guardium CLI commands for CyberArk setup**
 - show cyberark status
 - store cyberark install
 - store cyberark config_failover
 - store cyberark uninstall
 - store cyberark service start
 - store cyberark service stop

CyberArk setup

CyberArk AIM agent installation

- Check the install status, delete pre-existing host account
- store cyberark install

```
gat-daily-vm04.guard.swg.usma.ibm.com> show cyberark status
CyberArk is not installed
ok
gat-daily-vm04.guard.swg.usma.ibm.com> store cyberark install

Prerequisites to install the CyberArk Application Password Provider:
1. The CyberArk vault system is set up with the required permissions.
2. You have the CyberArk vault host name or IP address, vault user name, and vault password ready,
3. This Guardium system's account Prov_gat-daily-vm04.guard.swg.usma.ibm.com does not exist in the CyberArk vault server. If it exists, delete the account from the vault server before you continue with this installation.

For more information, see the IBM Security Guardium Knowledge Center.

Do you want to continue (yes or no)?
y
Enter the CyberArk Vault host name or IP address: 1.2.3.4
Enter the CyberArk Vault user name: administrator
Enter the CyberArk Vault password: *****
```

Grant permission to the account created by the installation which is in the safe.

Setup High availability

- Store cyberark config_failover

Please refer to the IBM Guardium knowledge center for information on the step by step for setting up CyberArk for Guardium.

Guardium integration with CyberArk

Create New CyberArk Configuration

Setup → Tools and Views — CyberArk configurations

The screenshot displays the CyberArk console interface. On the left is a navigation sidebar with icons and labels for Welcome, Setup (highlighted), Manage, Discover, Harden, Investigate, Protect, and Comply. The main content area shows the 'CyberArk Configurations' table with columns: Name, Application ID, Safe Name, and Folder Name. A single configuration is listed: 'CyberArk_install1' with Application ID 'Guardium', Safe Name 'GuardiumTest', and Folder Name 'root'. An 'Edit CyberArk Configuration' dialog box is open in the foreground, containing four labeled input fields: '* Name' (CyberArk_install1), '* Application ID' (Guardium), '* Safe Name' (GuardiumTest), and '* Folder Name' (root). At the bottom of the dialog are 'Save' and 'Close' buttons. The top of the console shows a header bar with the time '17:22', notification icons, a search bar, and user information 'admin admin' and 'Machine Type: Standalone'.

Name	Application ID	Safe Name	Folder Name
CyberArk_install1	Guardium	GuardiumTest	root

Edit CyberArk Configuration

* Name: CyberArk_install1

* Application ID: Guardium

* Safe Name: GuardiumTest

* Folder Name: root

Save Close

Guardium integration with CyberArk

grdapi commands for managing cyberark configurations.

- create_cyberark_config
- delete_cyberark_config
- list_cyberark_config
- update_cyberark_config
- Ex: **grdapi create_cyberark_config**

name="CyberArk_install1"

applicationId="Guardium"

safeName="GuardiumTest"

folderName=root

Guardium integration with CyberArk

Version of CyberArk Vault supported by Guardium V11: 8.x, 9.x, and 10.x

Database platforms that can be automatically managed by CyberArk:

- ☐ DB2
- ☐ Informix
- ☐ Microsoft SQL Server
- ☐ MySQL Server
- ☐ Oracle
- ☐ SAP HANA
- ☐ SybaseASE

Database platforms of Cloudera, MongoDB, PostgreSQL etc. can still be saved in Vault but could not be automatically managed.

Guardium integration with CyberArk

Activate the database platform in the Vault

Activate a Platform: PVWA → Administration → Platform Management

POLICIESACCOUNTSAPPLICATIONSREPORTSADMINISTRATION

administrator
Last sign in: 6/1/2019

ADMINISTRATION

Administration > Platform Management
Platform Management ?

Import Platform

Platform Preview

Platform Management

Target Account Platforms | Service Account Platforms

Name	Device Type	Status
MySQL Server	Database	Active
Oracle Database	Database	Active
SAP HANA	Database	Active
Sybase ASE	Database	Inactive
IBM Tivoli	Directory	Inactive
MS Active Directory	Directory	Inactive
Novell eDirectory server	Directory	Inactive
Oracle Internet Directory	Directory	Inactive

NAME
Sybase ASE

DESCRIPTION
None

STATUS ?
Inactive

Guardium integration with CyberArk

Add a datasource as an account in CyberArk

CyberArk password vault web access(PVWA)

<https://x.x.x.x/PasswordVault/>

POLICIESACCOUNTSAPPLICATIONSREPORTSADMINISTRATION

Add Account

Store in Safe:GuardiumTest

Device Type:Database

Platform Name:Microsoft SQL Server

Required Properties:

Username:test

Optional Properties:

☐ DSN (ODBC):

☒ Address:MyserverName

☒ Port:1434

☒ Database:Northwind

☐ Windows reconcile account:[Select]

Password Content

Password:••••••••

Confirm Password:

Name:

☐ Auto-generated (Name pattern: Device Type-PolicyID-Address-Username-vty-DSN-ServiceName-TaskName-SystemNumber-Client)
☒ Custom [DatasourceName]

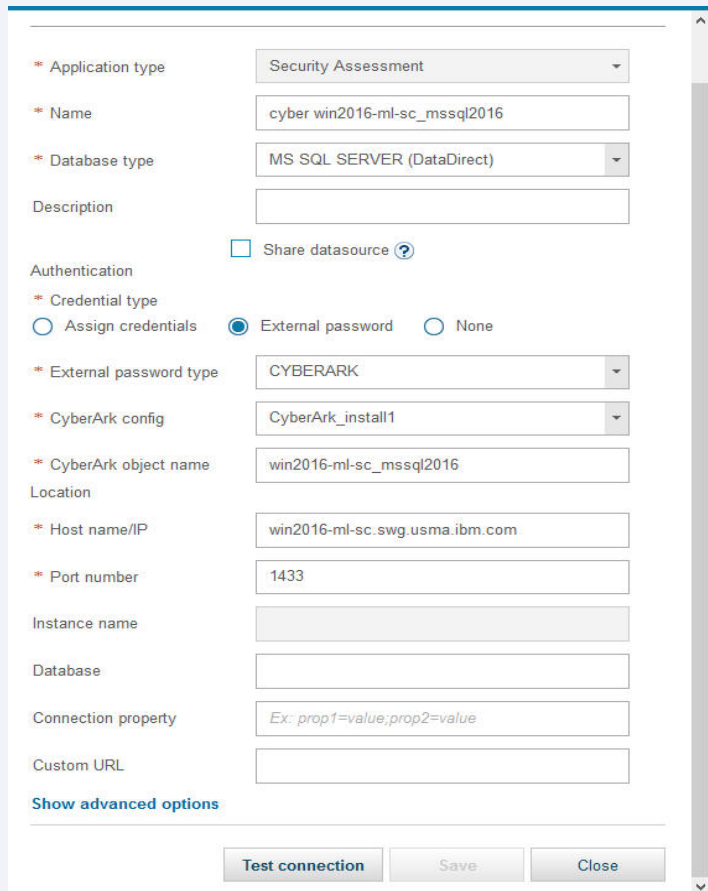
☐ Disable automatic management for this account

Reason:

Save

Cancel

Create a DataSource in the Guardium GUI



The screenshot shows a web-based form for creating a new data source in the Guardium GUI. The form is titled 'Create a DataSource' and contains several sections for configuration. The 'Application type' is set to 'Security Assessment'. The 'Name' field contains 'cyber win2016-ml-sc_mssql2016'. The 'Database type' is set to 'MS SQL SERVER (DataDirect)'. The 'Description' field is empty. There is a checkbox for 'Share datasource' which is unchecked. The 'Authentication' section has three radio buttons: 'Assign credentials' (unchecked), 'External password' (checked), and 'None' (unchecked). The 'External password type' is set to 'CYBERARK'. The 'CyberArk config' is set to 'CyberArk_install1'. The 'CyberArk object name' is set to 'win2016-ml-sc_mssql2016'. The 'Location' section has three fields: 'Host name/IP' (win2016-ml-sc.swg.usma.ibm.com), 'Port number' (1433), and 'Instance name' (empty). The 'Database' field is empty. The 'Connection property' field contains the example text 'Ex: prop1=value;prop2=value'. The 'Custom URL' field is empty. At the bottom, there is a link 'Show advanced options' and three buttons: 'Test connection', 'Save', and 'Close'.

* Application type: Security Assessment

* Name: cyber win2016-ml-sc_mssql2016

* Database type: MS SQL SERVER (DataDirect)

Description:

☐ Share datasource ?

Authentication

* Credential type

☐ Assign credentials ☒ External password ☐ None

* External password type: CYBERARK

* CyberArk config: CyberArk_install1

* CyberArk object name: win2016-ml-sc_mssql2016

Location

* Host name/IP: win2016-ml-sc.swg.usma.ibm.com

* Port number: 1433

Instance name:

Database:

Connection property: Ex: prop1=value;prop2=value

Custom URL:

[Show advanced options](#)

Create a DataSource using Guardium API

grdapi create_datasource

application="Security Assessment"

name=myds

type="MS SQL SERVER (DataDirect)"

useExternalPassword=true

externalPasswordTypeName=CYBERARK

cyberarkConfigName="CyberArk_Config1"

cyberarkObjectName=myds

host=myhost

port=1450

savePassword=false

V11.0 Guardium New Features – Data Protection

Agenda

FDEC new features

- New Schedulers
- Purge Function

FAM

- Demo for FAM for NAS and SharePoint
- Limitations

FAM for Windows and S-TAP split

- What to expect from upgrade

New Features for File Discovery, Entitlement, and Classification Agent

FDEC Configuration Utility: Continued Functionality

The screenshot shows the 'IBM Security Guardium FDEC for NAS Configuration' window. It includes a 'Configured Scans' list on the left and a configuration form on the right. The form contains fields for Scan Name, Guardium Appliance, Scan Host, Scan Paths, Scan Frequency, Scan Options, Directory Level, and buttons for Run Now, New Scan, Save Scan, Purge Scan DB, and Delete Scan. A status section at the bottom shows scan history and current status.

Guardium Appliance hostname or IP address

Frequency of the scan

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

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

Only return records that trigger criteria

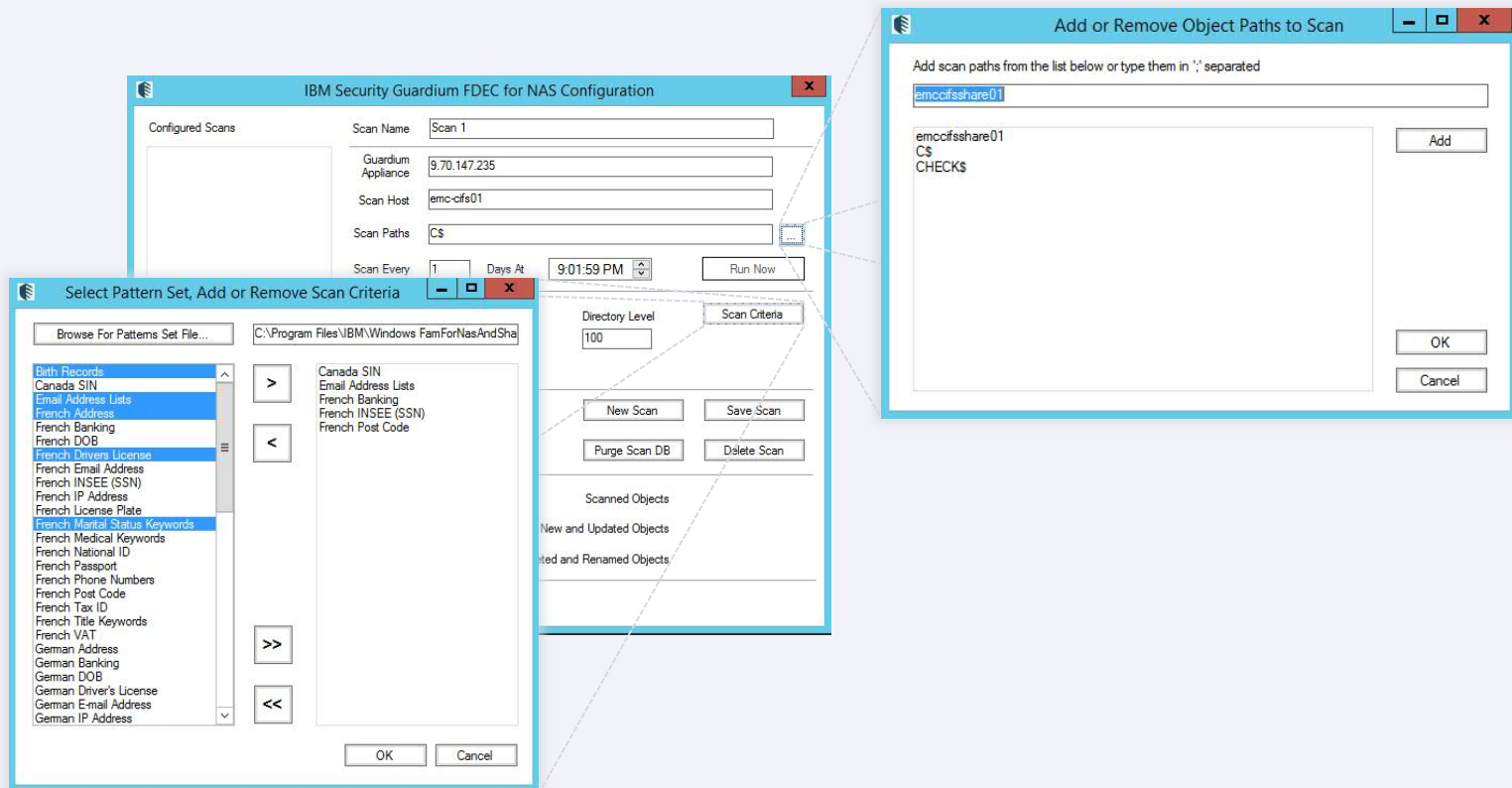
Hostname of IP address of the device to be scanned. Localhost in case of SharePoint

Name of Share

How deep into directory structure should the scan go

Scan Status

FDEC Configuration: Criteria selection and NAS share selection



FDEC Configuration Utility: New Functionality

The New Way

Scan Every Days At

The Old Way

Scan Every ☒ Hours
☐ Days

IBM Security Guardium FDEC for NAS Configuration

Configured Scans

Scan Name

Guardium Appliance

Scan Host

Scan Paths

Scan Every Days At

Scan Options ☐ Containers Only ☒ All Objects ☐ Matches Only

Directory Level

Scan Service Account

Started Last Scan

Finished Last Scan

Next Scan 2019-06-14 21:01:00

Scanned Objects

New and Updated Objects

Deleted and Renamed Objects

Scan Status Idle

Purge Scan DB

Purge Scan DB Every Days At

Last Purge Time -----

Next Purge Time 2019-06-15 12:00:00

New Features for File Activity Monitoring: Policy Builder

File Activity Monitoring: Configuration

The image displays the IBM Security Guardium Activity Monitor Configuration interface, showing multiple overlapping windows for configuring file activity monitoring on the host `emc-cifs01`.

Main Configuration Window (Background):

- Monitored Hosts:** A table showing the host `emc-cifs01` with platform `Unity` and a status of `9/19/2018 9:37:54 AM`.
- Operations Tab:** The `emc-cifs01 properties` window is open, showing the `Operations` tab. It allows selecting file and directory operations to monitor.

File Activity Events Configuration (Middle Window):

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 from EMC CEE. Please refer to the IBM Security Guardium Activity Monitor User Guide for more information.

To reduce number of read events the product can report only the first file read by a user within a 5 minutes interval:

- ☐ Suppress subsequent Read operations in the same folder
- ☐ Suppress Microsoft Office operations on temporary files. This feature may delay reporting of activity.

Account Exclusions Configuration (Right Window):

Activity from the following accounts will be filtered during collection.

- ☒ Add Windows Account
- ☒ Add Unix Account
- ☒ Remove

Account name: Account Type:

Guardium Appliance Configuration (Bottom Right Window):

Please specify Guardium appliance host name or IP to stream activity data from this host. If changed, Guardium service restart is required.

Guardium appliance:

EMC Device Configuration (Bottom Left Window):

Specify an EMC device to be monitored for activity.

NAS Server Name:

File Activity Monitoring: Policy Configuration in Guardium

IBM Guardium

14:57

New Policy

* Type: Network Attached Storage

* Policy Name: NASpolicy

Rule [Show Templates](#)

+ | | - | ↕ | Filter

Name	Rule
------	------

Use the 'New' tool bar icon to create a new rule

File Activity Monitoring: Policy Configuration in Guardium

Create New Rule

Rule name

Rule: rule1

Choose datasources

Datasource victor2k8:emc-cifs01:FAM-NAS

Define rule criteria

Specify the criteria to take action

Include file path

=

abc

Exclude file path

=

xyz

Exclude account

=

me@ibm.com

Exclude extension

=

exe,dll

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

Next

Define rule action

Read | Alert and Audit, SYSLOG

Save

Cancel

File Activity Monitoring: Policy Configuration in Guardium

Create New Rule

✓ Rule name *Rule: rule1*

✓ Choose datasources *Datasource victor2k8:emc-cifs01:FAM-NAS*

✓ Define rule criteria *me@ibm.com, abc*

Define rule action *Specify the action to take*

☒ Specify action for specific operation or group

* Operation

* Rule action

Message Template

Notification Type

Add another action | Remove

Save Cancel

Select operation

- ☐ -- All --
- ☐ Add directory
- ☐ Add file
- ☐ Change directory permission
- ☐ Change file permission
- ☐ Delete directory
- ☐ Delete file
- ☐ Read
- ☐ Rename directory
- ☐ Rename file

At least one item must be selected.

FAM for Windows and STAP: Standalone Agents

Upgrade Standalone Windows FAM and S-TAP

When pre-11.0 FAM and STAP are installed

- FAM will be blocked from installation with a message to uninstall or upgrade STAP first



- STAP will be upgraded but FAM components will be removed. FAM can be installed as a standalone following STAP upgrade or removal.

STAP

GUARDIUM 11.0 NEW RELEASE TRAINING

Agenda

- Pain Points
- New DB/OS support
- Oracle Connection Manager support
- Better Kafka support for Cloudera integration
- External S-TAP changes

Pain Points

- SOFTWARE TAP EVENT severity cleanup (GRD-21970)
 - LOG_NOTICE is overused and includes items that are informational message (e.g. “sqlguard IP is X”) as well as warnings (e.g. “No Kernel Interception methods chosen”)
 - Revised the severity levels to pull the warning messages to LOG_WARNING to make it easier to filter the events

Pain Points






- Ability to control custom kernel compilation (GRD-23132)
 - Not recommended
 - Some customers may want to preferentially use flex-loading when kernel development packages are sporadically installed in their environment
 - Locally built modules are a better fit for the kernel, and a better methodology would be to locally build on test systems and distribute the custom GIM bundles
 - Disabling local build allows validating support for flex loading in test and pushing non-custom GIM bundles to production where kernel development packages may be installed and prevent using a locally built KTAP module that was not used in the test environment

Pain Points

- Ability to control custom kernel compilation (continued)
 - GIM parameter is KTAP_PREVENT_EXACT_MATCH_BUILD
 - Once set and installed, it cannot be changed from this setting in GIM until a new bundle is pushed

Optional parameters

[Nn] - Allow KTAP local build. *[Yy]* - Prevent KTAP local build

KTAP_PREVENT_EXACT_MATCH_BUILD			N			
--------------------------------	---	---	---	---	---	---

Next

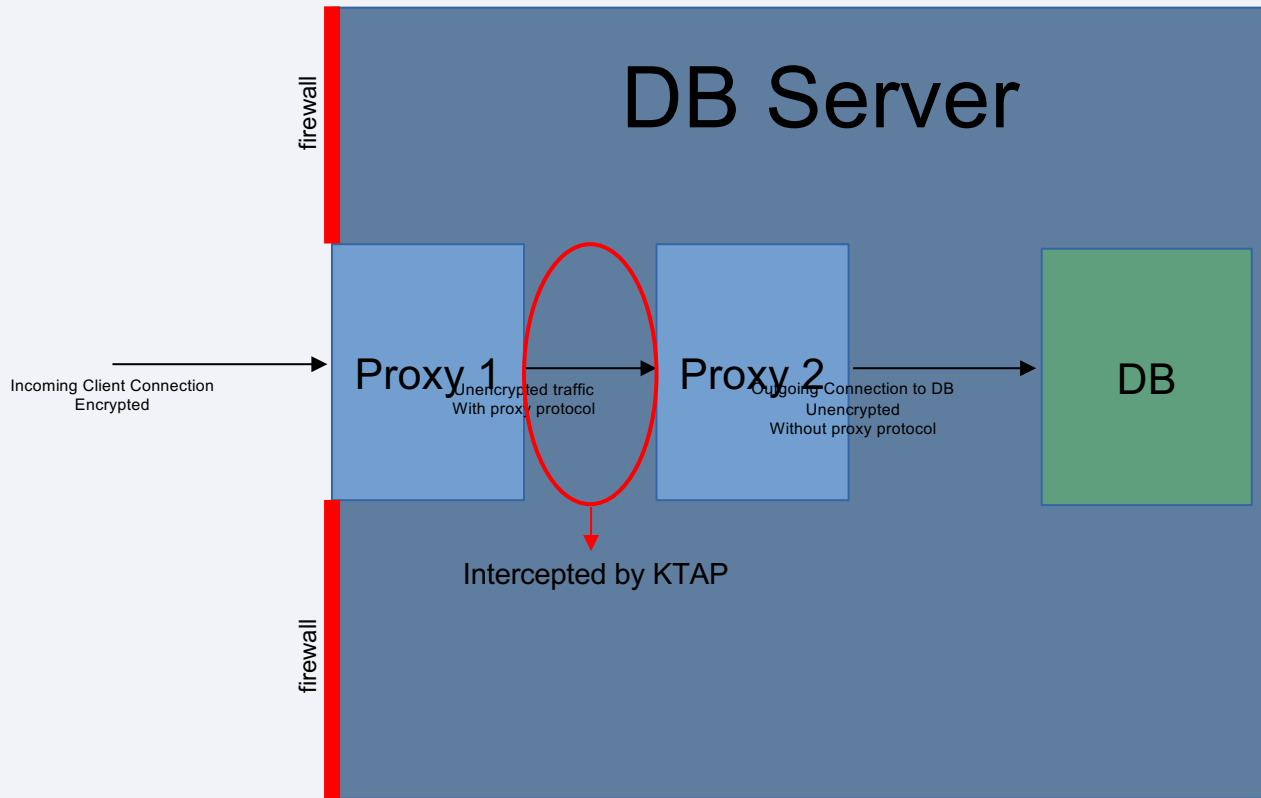
Pain Points

- Ability to control custom kernel compilation (continued)
 - Shell parameter is `--ktap_prevent_exact_match_build`
 - RPM installation does not take parameters and will install allowing local build
 - All installation methods can change the setting after installation with `guard-config-update --set-ktap-prevent-exact-match-build <0, 1>`
 - 0 – allow local build
 - 1 – disallow local build
 - Note that disallowing the local build only takes effect for new modules that would have been built and does not prevent the use of KTAP modules that have already been built

New DB/OS Support

- SLES 15 (x86_64, PPC64LE, s390x)
- Solaris 11.4
- Removed support for Ubuntu 10.04 & 12.04
- New method of supporting encrypted databases by using a double proxy solution
 - Couchbase and Neo4J supported
 - Either HAProxy or NGINX can be used and is installed on the DB host
 - First proxy terminates SSL and adds proxy protocol
 - Proxy protocol injects a packet in the beginning of the TCP stream to identify the real client IP
 - Second proxy removes the proxy protocol packet and sends the unencrypted connection to the DB listener
 - Proxy protocol is not supported by most DB instances, so the second proxy removes the packet
 - KTAP interception is configured to capture traffic between the two proxies
 - DB listeners are reconfigured to accept unencrypted traffic
 - Firewall rules are needed to prevent access to the DB around the proxy entry point

Diagram of a Double Proxy Solution



Using a Double Proxy Solution for Couchbase

- Couchbase configuration is in the `static_config` file
 - To avoid reconfiguring clients, the default ports must be modified so that the clients will connect to the first proxy instance instead
 - For example
 - `{memcached_ssl_port, 11207}`
 - `{ssl_rest_port, 18091}`
 - `{ssl_capi_port, 18092}`
 - `{ssl_query_port, 18093}`
 - `{fts_ssl_port, 18094}`
 - These ports will need to be used in the first proxy instance and Couchbase would need to be configured to expect unencrypted connections and to move these ports to a different number so that they do not duplicate ports being listened on by the proxy instances.

Using a Double Proxy Solution for Couchbase

- Example configuration of unencrypted couchbase ports
 - {memcached_port, 11210}
 - {rest_port, 8091}
 - {capi_port, 8092}
 - {query_port, 8093}
 - {fts_http_port, 8094}
- The first proxy instance would be configured to terminate SSL on and add proxy protocol to ports
 - 11207, 18091, 18092, 18093, 18094
- The second proxy instance would then be configured to listen to intermediate ports and remove proxy protocol
 - 21207, 28091, 28092, 28093, 28094

Using a Double Proxy Solution for Couchbase

- The second proxy instance would then be configured to send the unencrypted traffic to the unencrypted Couchbase ports
- Firewall rules should be used to protect the ports from access externally to the host
- Full documentation will be available in the v11.0 documentation

Using a Double Proxy Solution for Neo4J

- Neo4J configuration is in neo4j.conf
 - Neo4J advertises the ports it uses. Since the ports will need to be changed to avoid conflicting with the proxy ports, Neo4J will need to have its port configuration changed and the proxy entry point ports will need to be configured for advertising (requires version 3.5.0 or newer)
 - For example
 - `dbms.connector.bolt.listen_address=127.0.0.1:27687`
 - `dbms.connector.bolt.advertised_address=rh7u3x64t-ktap:7687`
 - `dbms.connector.http.listen_address=127.0.0.1:7474`
 - `dbms.connector.https.listen_address=127.0.0.1:27473`
 - `dbms.connector.https.advertised_address=rh7u3x64t-ktap:7473`

Using a Double Proxy Solution for Neo4J

- The first proxy instance would be configured to terminate SSL on and add proxy protocol to ports
 - 7687, 7473
- The second proxy instance would then be configured to listen to intermediate ports and remove proxy protocol
 - 17687, 17473
- The second proxy instance would then be configured to send the unencrypted traffic to the unencrypted Neo4J ports
 - 27687, 7474
- Full documentation will be available in the v11.0 documentation

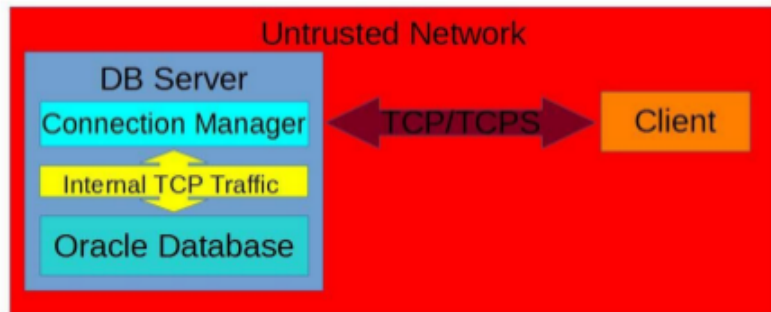
Oracle Connection Manager Support

- Oracle Connection Manager (CMAN) is an Oracle product which acts as a proxy for an Oracle DB
 - It is possible to use CMAN to terminate SSL either for performance reasons, or as an alternative to ATAP
 - Oracle recommends using CMAN 18c since it has performance and security improvements
 - Does not currently support terminating Oracle's native encryption (ASO)
 - Is usable on standalone systems or in RAC and Exadata environments
 - Full documentation will be available in the v11.0 documentation

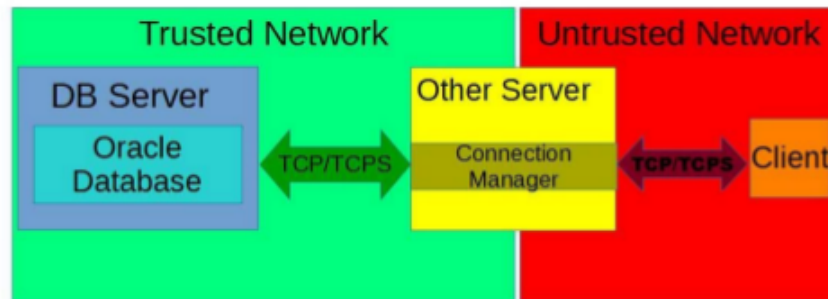
Oracle Connection Manager Support

- CMAN can be installed on the same node as the DB listener, or on a remote node. When on the same node, the decrypted traffic will not leave the host machine.

Connection Manager and Database
located on same system



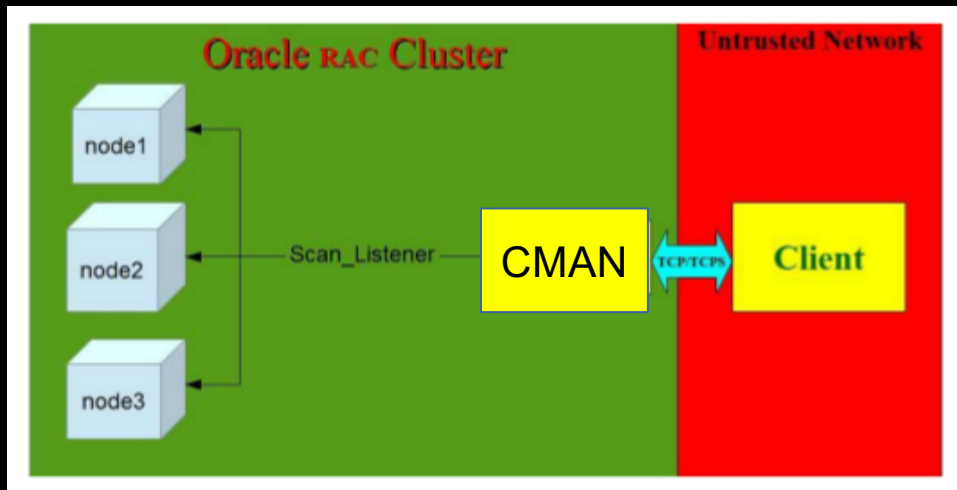
Connection Manager and Database
located on different systems



Oracle Connection Manager Support

- In a RAC or Exadata environment, since the individual nodes will be altered to expect unencrypted traffic, internode communication will be unencrypted. The cluster's network should be private to avoid security concerns.

RAC and Exadata environments use a SCAN listener. CMAN would be installed on each node and is the entry point to the cluster, decrypting traffic internally and routing to the SCAN listener.



Better Kafka Support for Cloudera Integration

- Uses librdkafka
 - Multiple STAPs can be put into the same Kafka consumer group for load balancing and HA
 - A Kafka consumer group is Kafka managed group of consumers with the same group name.
 - Setting the same kafka_group_name for multiple STAPs that are configured for the same Kafka cluster and topic will create the consumer group.
 - Kafka will assign the topic partitions across the consumers in a group.
 - If a consumer leaves or joins the consumer group, the Kafka cluster will rebalance the topic partitions across the consumers.

External S-TAP Changes

- New Databases
 - MySQL and MariaDB
 - PostgreSQL
 - Mongo
 - DB2

External S-TAP Changes

- Certificate Verification Overview
 - Certificate Verification Capability
 - Server Certificate
 - Verify server certificate based on whitelist, blacklist, custom CA certificate, and system built-in CA bundle
 - Client Certificate (Mutual Authentication)
 - Verify client certificate based on custom CA certificates or system built-in CA bundle
 - Actions for invalid certificates
 - Admin can configure to reset connections and/or logging when an invalid certificate is detected

External S-TAP Changes

- Certificate Verification Overview (continued)

- Verification Orders

- If whitelist is set (apply to server cert only)
 - Accept the server certificate immediately when it is in the whitelist
- If blacklist is set (apply to server cert only)
 - Take actions(reset connection or logging) immediately if server certificate is in the blacklist
- If trusted CA certificate is set (apply to both client and server cert)
 - Verify client/server certificate according to the trusted CA certificates
 - Take actions(reset connection or logging) if the verification fails
- If trusted CA not set (apply to both client and server cert)
 - Verify client/server certificate according to the default CA certificate bundle
 - We already included AWS CA certificate for AWS RDS, and some other built-in CA bundles inside on CentOS 7.4

External S-TAP Changes

- Certificate Verification Configuration
 - Trusted CA Certificates can be stored in the collector with a CLI command
 - `store certificate custom_keystore_external_stap`
 - Requires a token from 'create csr external_stap' to associate with an External S-TAP deployment
 - This will allow trusted certificates to route to the correct External S-TAP instance in the case that you have multiple deployments managed by one collector
 - CA certificates will be used to verify client and server certificates by the External S-TAP

External S-TAP Changes

- Certificate Verification Configuration (continued)

- Whitelist

- store certificate whitelist_external_stap
 - Requires a token from 'create csr external_stap' to associate with an External S-TAP deployment
- Only applies to the server certificate when External S-TAP creates an outgoing connection to the DB service
- When disconnect_on_invalid_certificate is set, clients that are not trusted by a Trusted Certificate will not be allowed to connect and server certificates that are neither whitelisted nor trusted by a Trusted Certificate will be allowed to be connected to

- Blacklist

- store certificate_blacklist_external_stap
 - Requires a token from 'create csr external_stap' to associate with an External S-TAP deployment
- Only applies to the server certificate when External S-TAP creates an outgoing connection to the DB service
- Blacklisted certificates are never allowed to be connected to by the External S-TAP

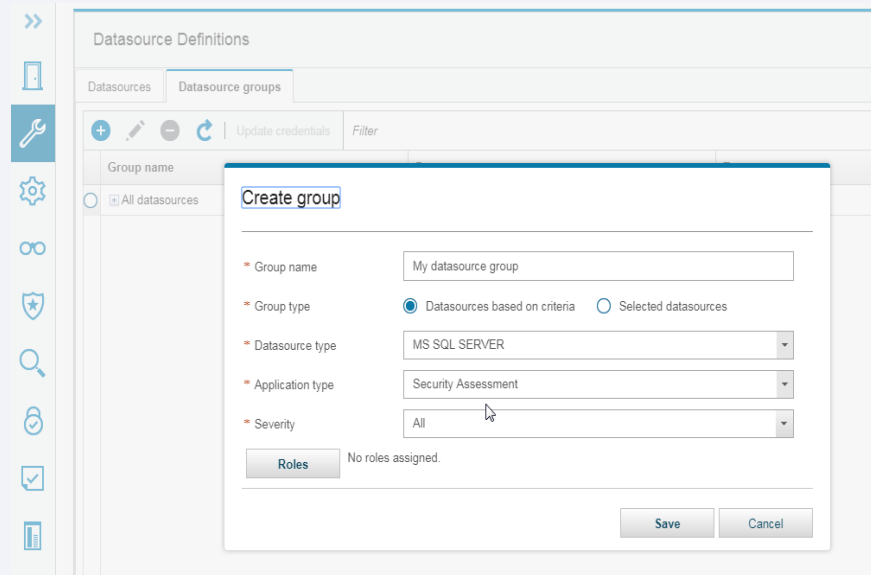
Guardium V11 New Release Training

VA Test Exceptions and Test Detail Exceptions

Contents

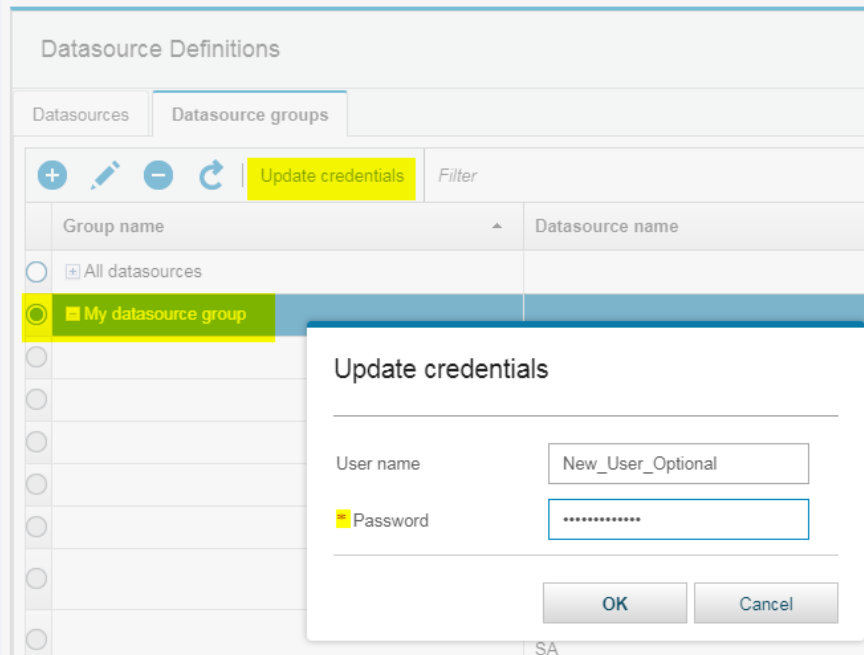
- Changing datasource credentials in bulk using groups
- Running Security Assessments with datasource groups
- Creating VA test exceptions
- Creating VA test detail exceptions
- Reporting for test and test detail exceptions
- Demo
- Q & A
- Reference materials (APIs)

Datasource Group



- You can now create datasource groups based on criteria or selected datasources.
- You can use datasource groups to change usernames and passwords in bulk.
- You can run security assessments using groups of datasources.
- You can create exceptions using datasource groups.
- All of this functionality can be done using grdapi.

Datasource Group Credential update



- When changing the password for a group of datasources, you can update both username (optional) and password.
- This is useful when you have a group of datasources using the same credentials like Windows Active Directory for SQL Server logins.

Creating Security Assessments using Datasource Groups

- You can create security assessments with individual datasources.
- You can create security assessments with datasource groups.
- You can create security assessments using datasource groups and individual datasources.
- Security assessments will execute unique datasources within each assessment.

Security Assessment Builder

Description

(demo) SQL Server using group

Automatically add all future CVE or APAR tests after DPS uploaded☐

Datasources

Name	Type	Host
DPS: MSSQL2014 FAIL on w2k12std-va02 Datadirect_MS SQL SERVER(Security Assessment)	MS SQL SERVER	w2k12std-va02.guard.swg.usma.ibm.com
DPS: MSSQL2014 PASS on w2k12std-va01 OPEN_MS SQL SERVER(Security Assessment)	MS SQL SERVER	w2k12std-va01.guard.swg.usma.ibm.com
My datasource group	Datasource group	

Add Datasource

Add Datasource Group

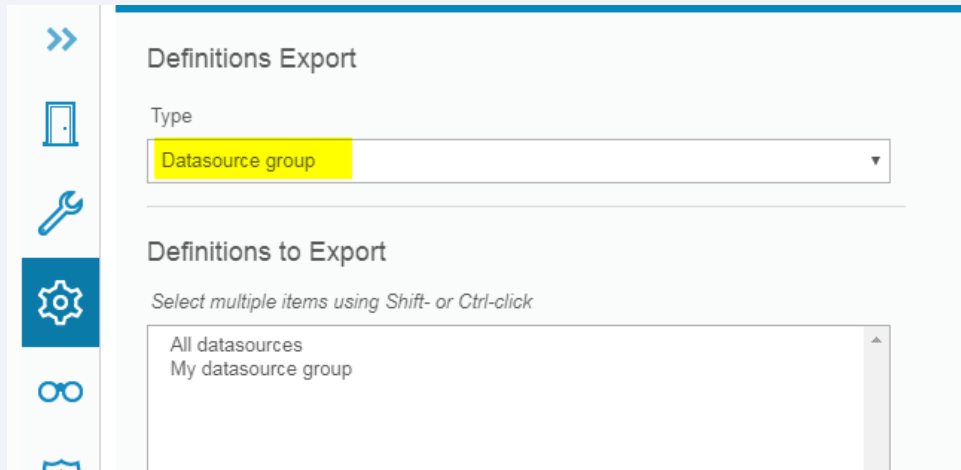
Roles

No Roles have been assigned to this Security Assessment

Roles

Export and Import of Datasource Groups

- You can export and import datasource groups.
- You can export security assessments which also export and import datasource group dependencies.



Test Exceptions Enhancement for VA

- Use test exceptions to overwrite findings for a specific test within a duration.
- Test exceptions can be created for a single assessment or all assessments.
- Test exceptions can be created for a single, group or all datasources.

Create test exception for Unused database components must be disabled

Test name

Assessment scope ☒ Single assessment ☐ All assessments

Assessment

Datasource scope ☒ Single datasource ☐ Group ☐ All datasources

Datasource

Approver

Start date

End date

Justification

Test Detail Exceptions Enhancement for VA

- Use test detail exceptions to whitelist a finding for a specific grantee on a given test.
- Test detail exceptions can be created for a single assessment or all assessments.
- Test detail exceptions can be created for a single, group or all datasources.
- Test detail exceptions can be created using regular expressions or exact text match.

The screenshot displays the IBM Security interface with a test detail exception being added. On the left, a test result for 'No Authorization To AUDIT SYSTEM Privilege' is shown, categorized as 'Priv.' with a 'Critical' severity. The test category is 'Priv.' and the test severity is 'Critical'. The test details include 'DPS: Oracle19 FAIL rh7va-vm02 ON9PRH7V PDB' and 'Datasource type: ORACLE'. The test result is 'Fail'. A recommendation is provided: 'We recommend you revoke the AUDIT SYSTEM privilege from'. A table of test details is shown with columns for ID, Detail value, and Example. The first row is selected, showing 'Grantee = GUARDIUM_ROLE : Privilege = AUDIT SYSTEM'. A red arrow points to the 'Add exception' button in the 'Add to test details exception list' dialog. The dialog is titled 'Add exception for selected test details' and contains fields for Test name, Assessment scope (Single assessment, All assessments), Datasource scope (Single datasource, Group, All datasources), Datasource (DPS: Oracle19 FAIL rh7va-vm02 ON9PRH7V PDB), Start date (6/3/2019), End date (8:37 PM), and a Justification field. The 'All assessments' and 'Single datasource' options are selected. The 'Justification' field is empty and has a red 'X' icon. The 'Save' and 'Close' buttons are at the bottom right.

No Authorization To AUDIT SYSTEM Privilege
Test category: Priv. Test severity: Critical
DPS: Oracle19 FAIL rh7va-vm02 ON9PRH7V PDB
Datasource type: ORACLE Datasource severity: High
Fail
AUDIT SYSTEM privilege has been granted to unauthorized grantees. Including 0
Short Description: This test checks for grants of system privilege 'AUDIT SYSTEM' excludes privileges granted to these system predefined grantees (DBA, DATAPUMP)
External Reference: CIS Oracle 11gR2 v1.0.0 Item #4.3.3
Recommendation: We recommend you revoke the AUDIT SYSTEM privilege from
Details
Add Selected Members To Exception Group
Create Test Details Exception
Grantee = GUARDIUM_ROLE : Privilege = AUDIT SYSTEM
Grantee = GUARDIUM_TEST : Privilege = AUDIT SYSTEM
Close this window

Add to test details exception list

Review the list of test details below and create an exception to add elements that are not already covered, select the rows
Elements found by vulnerability scan

ID	Detail value	Example
<input checked="" type="checkbox"/>	Grantee = GUARDIUM_ROLE : Privilege = AUDIT SYSTEM	
<input type="checkbox"/>	Grantee = GUARDIUM_TEST : Privilege = AUDIT SYSTEM	

Total: 2 Selected: 1

* Datasource group

Add exception for selected test details

Test name: No Authorization To AUDIT SYSTEM Privilege

Assessment scope: ☐ Single assessment ☒ All assessments

Datasource scope: ☒ Single datasource ☐ Group ☐ All datasources

* Datasource: DPS: Oracle19 FAIL rh7va-vm02 ON9PRH7V PDB

Start date: 6/3/2019 8:37 PM

End date:

* Justification:

Save Close

Test Detail Exceptions Enhancement for VA

- Creating a test detail exception using the regular expression screen.
- Regular expressions for test detail exceptions do not need to be prefixed with (R).
- Regular expressions for group exceptions do require the (R) prefix.
- Both test detail exceptions and exception groups use JAVA's regular expression.

Create test details exception

Enter details for the new exception. If you specify a regular expression, the regex and any test details that match it will be added to the list once you click on the Save button.

Element type: ☒ Regular expression ☐ Text

* Regular expression: Grantee = GUARDIUM_ROLE

Test name: No Authorization To AUDIT SYSTEM Privilege

Assessment scope: ☐ Single assessment ☒ All assessments

Datasource scope: ☒ Single datasource ☐ Group ☐ All datasources

* Datasource: DPS: Oracle19 FAIL rh7va-vm02 ONSPRHTV PDB

Start date: 6/3/2019 8:41 PM

End date:

* Justification: This is required by the application.

Save Close

Test Detail Exceptions Enhancement for VA

- The Test detail exception editor allows you to modify existing exceptions.
- The button can be launched from within the security assessment finder, test configuration and tuning screens.

The screenshot shows the 'Test Detail Exceptions' editor. On the left, there's a sidebar with 'Tests available' and a list of database types including ORACLE, SYBASE, and TERADATA. The main area is titled 'Test Detail Exceptions' and contains a 'Search test detail exceptions' section. This section has a dropdown for 'Assessment' (set to 'Any assessment'), a radio button group for 'Datasource scope' (with 'Single datasource' selected), a dropdown for 'Datasource' (set to 'Any datasource'), a checkbox for 'Included in datasource group', a dropdown for 'Datasource type' (set to 'ORACLE'), a dropdown for 'Test' (set to 'No Authorization To AUDIT SYSTEM Privilege'), and a 'Text' input field. A 'Search' button is at the bottom of this section. Below the search section, it says 'Test detail exceptions found'.

The screenshot shows the 'Test Detail Exceptions' table view. It has a search bar at the top right with an 'Expand' button. Below the search bar, it says 'Test detail exceptions found' with a 'Collapse' button. A message states: 'Review the list of test details below and create an exception for those of interest. The match column shows if any of the test details are already covered by an existing exception. To set new criteria and add elements that are not already covered, select the rows of interest and click on Add exception.' Below this is a table with columns: ID, Exception value, Datasource, Assessment, Valid from, Valid to, Approver, and Justification. The table contains one row with ID 1. At the bottom, there's a 'Total: 1 Selected: 0' and a pagination bar showing '10 | 25 | 50 | 100'. A 'Close' button is at the bottom right.

ID	Exception value	Datasource	Assessment	Valid from	Valid to	Approver	Justification
1	Grantee = GUARDIUM_ROLE; Privilege = AUDIT SYSTEM	DPS Oracle19 vm02 ONPRHIV.PDB	All assessments	6/3/2019, 8:37:00 PM	12/31/9999, 7:00:00 AM	admin	Guardium_role need this privileges per application requirements.

Exception Groups Enhancement

- You can now add start date, end date and justification for exception groups at the group level.
- APIs for exception groups from older Guardium releases will continue to work in Guardium 11.0. You can also choose to update your APIs to use the new optional parameters.

The screenshot displays the 'Exception Group' configuration window. At the top, a yellow header bar contains the text 'Exception Group'. Below this, the 'Exception Group' label is positioned to the left of a dropdown menu showing 'Oracle: No Authorization to ALTER SYSTEM Privilege'. The main configuration area is a light gray box containing the following fields:

- Approver:** A text field with the value 'admin'.
- Start Date:** A date input field followed by a blue icon with the number '2' and the text '(optional future time)'.
- End Date:** A date input field followed by a blue icon with the number '2' and the text '(optional future time)'.
- Justification:** A large text area for entering details.

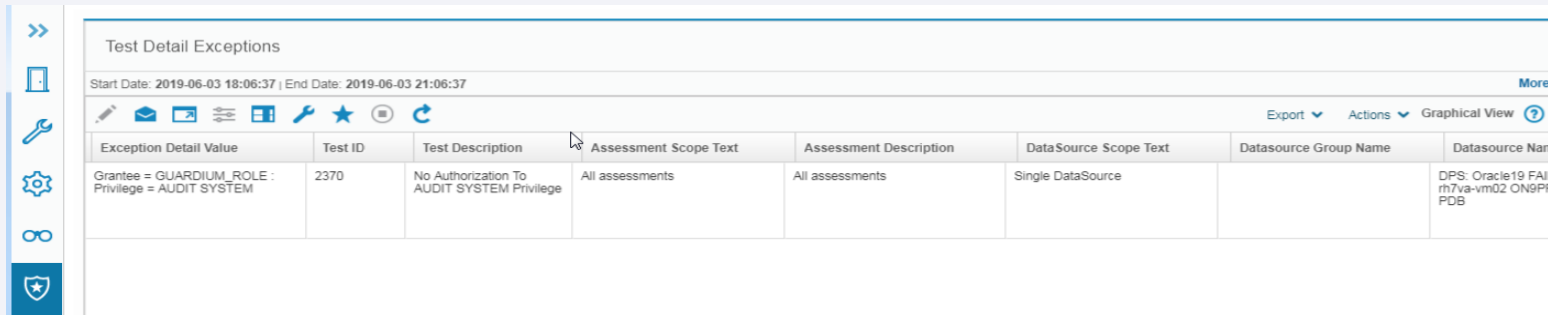
At the bottom of the window, there is a horizontal bar with five buttons: 'Cancel', 'Add Comments', 'Test Detail Exceptions', 'Restore Default', and 'Save'.

Exception execution order

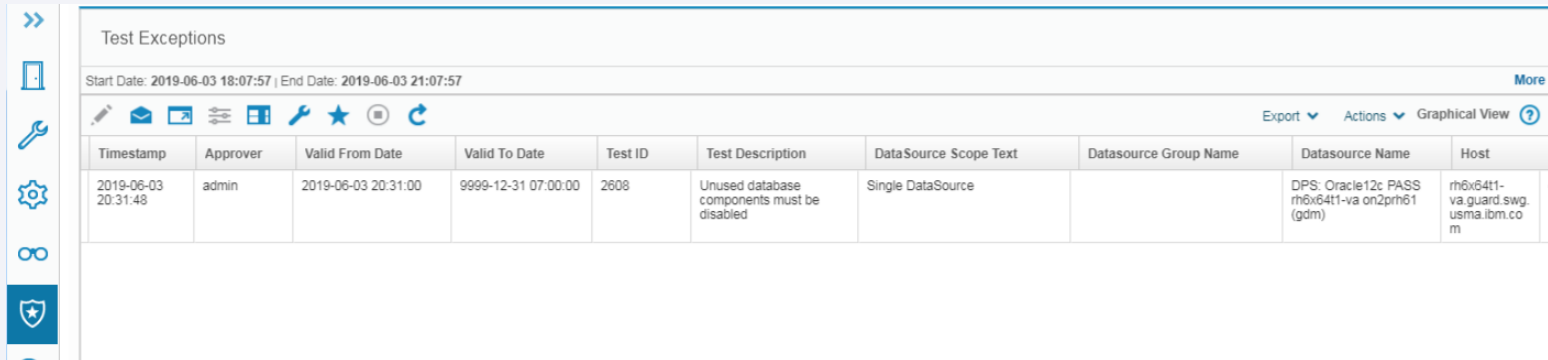
- The security assessment runner will apply exceptions in this order
 - Test exceptions, if exist
 - Group exceptions, if exist
 - Test detail exceptions, if exist

Reporting For Test and Detail Exceptions

- Use pre-defined reports to see exceptions you've created for auditing purposes.



Start Date: 2019-06-03 18:06:37 End Date: 2019-06-03 21:06:37							
Export Actions Graphical View ?							
Exception Detail Value	Test ID	Test Description	Assessment Scope Text	Assessment Description	DataSource Scope Text	Datasource Group Name	Datasource Name
Grantee = GUARDIUM_ROLE : Privilege = AUDIT SYSTEM	2370	No Authorization To AUDIT SYSTEM Privilege	All assessments	All assessments	Single DataSource		DPS: Oracle19 FAIL rh7va-vm02 ON9PR PDB



Start Date: 2019-06-03 18:07:57 End Date: 2019-06-03 21:07:57									
Export Actions Graphical View ?									
Timestamp	Approver	Valid From Date	Valid To Date	Test ID	Test Description	DataSource Scope Text	Datasource Group Name	Datasource Name	Host
2019-06-03 20:31:48	admin	2019-06-03 20:31:00	9999-12-31 07:00:00	2608	Unused database components must be disabled	Single DataSource		DPS: Oracle12c PASS rh6x64t1-va on2prh61 (gdm)	rh6x64t1-va.guard.usma.ibm.com

Q & A

For more information or follow-up questions, please contact:
IBM Security Guardium Support.

APIs References

Exception Group API References

- API that references exception group:
 - add_assessment_test
 - delete_assessment_test
 - list_assessment_tests
 - update_assessment_test

Example:

- » `grdapi add_assessment_test assessmentDescription="Oracle Security Assessment Demo" datasourceType="oracle" testDescription="No Authorization To ALTER SYSTEM Privilege" exceptionsGroup="Oracle: No Authorization to ALTER SYSTEM Privilege" fromDate="now +1 DAY" explanation="Demo purpose"`
- » `grdapi delete_assessment_test assessmentDescription="Oracle Security Assessment Demo" datasourceType="oracle" testDescription="Version: Oracle"`
- » `grdapi list_assessment_tests assessmentDescription="Oracle Security Assessment Demo"`
- » `grdapi update_assessment_test testDescription="Weak Passwords Are Screened" exceptionsGroup="Oracle Weak Passwords Are Screened" assessmentDescription="Oracle Security Assessment Demo" fromDate="now +1 DAY" explanation="Demo purpose"`

Test Exceptions API Reference

- API that references test exceptions:
 - `create_test_exception`
 - `delete_test_exception`
 - `delete_test_exception_by_id`
 - `list_test_exception`
 - `list_test_exception_by_id`
 - `update_test_exception`

Example:

- » `grdapi create_test_exception assessmentDesc="Oracle Security Assessment Demo" datasourceName="DPS: Oracle19 FAIL rh7va-vm02 ON9PRH7V PDB" explanation="demo test exception" fromDate="now " toDate="now +1 day" testDescription="No authorization To ANY TABLE Privileges"`
- » `grdapi delete_test_exception allowMultiDelete=0 testDescription="No authorization To ANY TABLE Privileges" assessmentDesc="Oracle Security Assessment Demo" datasourceName="DPS: Oracle19 FAIL rh7va-vm02 ON9PRH7V PDB" datasourceType="oracle"`
- » `grdapi delete_test_exception_by_id testExceptionId=20`

Test Exceptions API Reference - Continued

Example:

- » `grdapi delete_test_exception_by_id testExceptionId="20,21" allowMultiDelete=1`
- » `grdapi list_test_exception assessmentDesc="Oracle Security Assessment Demo" testDescription="No authorization To ANY TABLE Privileges" datasourceName="DPS: Oracle19 FAIL rh7va-vm02 ON9PRH7V PDB"`
- » `grdapi list_test_exception_by_id testExceptionId=2`
- » `grdapi update_test_exception testExceptionId=2 toDate="now +10 day"`

Test Detail Exceptions API Reference

- API that references test detail exceptions:
 - `create_test_detail_exception`
 - `delete_test_detail_exception`
 - `delete_test_detail_exception_by_id`
 - `list_test_detail_exception`
 - `update_test_detail_exception`

Example:

- » `grdapi create_test_detail_exception exceptionType=1 detailExceptionValue="sp_oa" datasourceName="DPS: MSSQL2014 FAIL on w2k12std-va02 Datadirect" testDescription="Procedures granted to users" toDate="now +1 day" explanation="test add api" assessmentScope=0 datasourceScope=0 assessmentDesc="MSSQL exception test" fromDate="now"`
- » `grdapi delete_test_detail_exception allowMultiDelete=1 detailExceptionValue="sp_ob" assessmentDesc="MSSQL exception test"`
- » `grdapi delete_test_detail_exception_by_id detailExceptionId=3542`

Test Detail Exception API Reference - Continued

Example:

- » `grdapi list_test_detail_exception approver="admin" datasourceType="MS SQL SERVER" assessmentScope=0 datasourceScope=0 datasourceName="DPS: MSSQL2014 FAIL on w2k12std-va02 Datadirect"`
- » `grdapi update_test_detail_exception testDetailExceptionsId=3600 fromDate="now"`

Guardium V11 New Release Training

Oracle 18c Patches, CVE and PostgreSQL v11

Content

- Oracle 18c patches and CVE test enhancements
- PostgreSQL v10, 11 support.
- Q & A

Oracle Patches and Release Review

Overview of New Release and Update Model for Database

- **Annual Releases**

- Oracle will deliver releases **yearly** instead of on a multi-year cycle
- Customers can get bug fix support for up to eight years on selected releases

- **Quarterly Release Updates (RUs)** - replace bundle patches

- RUs are **proactive**, highly tested bundles of critical fixes which enable customers to avoid known issues
- RUs greatly reduce the need to apply risky backports of individual fixes

- I • **Quarterly Release Update Revisions (RURs)** - replace PSUs

- RURs contain security and regression fixes to a RU that extend the RU's lifetime up to two quarters
- RURs allow customers to stay current on security content, while applying other bug fixes at a more conservative pace

- RUs and RURs ship on the same Jan, April, July, Oct dates as PSUs and BPs

Oracle Patches and Release Review

	Jan 18	Apr	Jul	Oct	Jan 19	Apr	Jul	Oct
RU	18.1.0	18.2.0	18.3.0	18.4.0	18.5.0	18.6.0	18.7.0	18.8.0
RUR #1	÷		18.2.1	18.3.1	18.4.1	18.5.1	18.6.1	18.7.1
RUR #2				18.2.2	18.3.2	18.4.2	18.5.2	18.6.2
RU					19.1.0	19.2.0	19.3.0	19.4.0
RUR#1							19.2.1	19.3.1
RUR #2								19.2.2

Figure 1-2 Example of an Oracle Database Release Number



Oracle Patches Metadata

- Guardium v11.0 supports the detection of Oracle18c quarterly and security patches for Patch and CVE tests.
- Guardium v11.0 also supports the detection of Oracle 18c OJVM CVE tests.

Edit group

Description

Oracle Database Version+Patches

General

Members

+ | - | Import

Filter

Member	Alias
<input type="checkbox"/> 12.1.0.2+12.1.0.2.190416DBBP	
<input type="checkbox"/> 12.1.0.2+PSU 12.1.0.2.190416	
<input type="checkbox"/> 12.1.0.2+WinBundle 12.1.0.2.190416	
<input type="checkbox"/> 12.2.0.1+DBRU 12.2.0.1.190416	
<input type="checkbox"/> 12.2.0.1+WinBundle 12.2.0.1.190416	
<input checked="" type="checkbox"/> 18+RU 18.6.0.0.190416	
<input checked="" type="checkbox"/> 18+RUR 18.4.2.0.190416	
<input checked="" type="checkbox"/> 18+RUR 18.5.1.0.190416	
<input type="checkbox"/> 19+RU 19.3.0.0.0	

Total: 13 Selected: 0 < 1 >

Reset to predefined

Save

Close

PostgreSQL v11 support

- In PostgreSQL v10 and higher. Password encryption supports both md5 and scram-sha-256.
- To support the stronger password encryption which VA recommends, Guardium v11.0 uses latest postgresql-42.2.5.jar driver. This driver supports PostgreSQL 8.2 or higher.
- Customers who upgrade to the scram-sha-256 password encryption will have to alter all database users to use this type of password encryption.

PostgreSQL New Test

- Test ID = 2689, Test Desc = Password Encryption Strength

IBM Guardium®

Results for Security Assessment:  PostgreSQL Password Encryption

Assessment executed: 2019-06-04 19:19:13



Password Encryption Strength

Test category: Priv. Test severity: Critical

DPS: PostgreSQL 11 FAIL on rh7va-vm02

Datasource type: POSTGRESQL Datasource severity: None

Fail

Password_encryption is not set to "scram-sha-256". Including 0 items present in exceptions group.

Short Description: This test checks if the password stored in the database is encrypted using scram-sha-256. SCRAM is preferred because it is an Internet standard and is more secure than the PostgreSQL-specific MD5 authentication protocol. It is a challenge-response scheme that prevents password sniffing on untrusted connections and supports storing passwords on the server in a cryptographically hashed form that is thought to be secure.

External Reference: PostgreSQL.org

Recommendation: We recommend that you change the password_encryption configuration to "scram-sha-256" in the postgresql.conf immediately.

Details

[Add Selected Members To Exception Group](#)

[Create Test Details Exception](#)

Password_encryption setting:

password_encryption setting is md5

[Close this window](#)



PostgreSQL Tests Enhancements

- Enhancements were done for these tests to ensure they are working correctly in the latest release of PostgreSQL.

Test_desc = No object privileges granted to users or roles on postgres system database

Test_desc = Password Encryption Storage

Test_desc = PostgreSQL_DATA environment variable defined

Test_desc = PostgreSQL_BIN environment variable defined.

Test_desc = Password authentication is encrypted

Guardium V11 New Release Training

VA for DataStax Cassandra

Content

- Guardium VA
- DataStax Cassandra Support
- DataStax Cassandra VA Tests
- Gdmmonitor script
- DataStax Cassandra DataSource
- Demo
- Troubleshooting
- Q & A
- Reference materials

IBM Guardium VA Solution

- IBM Guardium Vulnerability Assessment scans data infrastructures (databases, data warehouses and big data environments) to detect vulnerabilities, and suggests remedial actions.
- The solution identifies exposures such as missing patches, weak passwords, unauthorized changes and misconfigured privileges.
- Full reports are provided as well as suggestions to address all vulnerabilities.
- It identifies threats and security gaps in databases that could be exploited by hackers.



Supporting DataStax Cassandra - Phase 1



DataStax is the enterprise platform built on the open source Apache Cassandra database, which is one of the most popular NOSQL , open source distributed DBMS which provides you high availability with no single point of failure.


IBM Guardium VA Customers will now be able to scan multiple DataStax versions to detect and remediate vulnerabilities, such as;

- Excessive User & Group Privilege
- Mis-configurations and Default settings
- Privilege Escalation
- Un-patched Databases
- Old Versions, not supported by product

What's New

- Supporting DSE v5.1, v6.0 & v6.7
- Supporting JDBC connection using DataDirect JDBC driver
- Supporting native and LDAP authentication with SSL
- Providing latest version and patches from quarterly DPS
- Our VA solution for DSE Clusters can be run on all nodes.
- Introducing 16 new VA tests

DataStax Cassandra VA Tests

test_id	Test_DESC	
573	Version: Datastax Cassandra DSE	
574	Datastax Cassandra DSE Patch Level	
575	Default Port Not used	
2695	No Individual User Privileges - Functions Resources	
2696	No Individual User Privileges - Data Resources	
2697	No Individual User Privileges - Search Indexes	
2698	Review User-Defined Roles	
2699	No Individual User Privileges - Remote Procedure Calls	
2700	No Individual User Privileges - Proxy Login and Execute	
2701	No Individual User Privileges - MBeans	
2702	Superuser privilege granted to users	
2703	Remove the Superuser Role from the Cassandra Account	
2704	Nested Grants on Roles	
2705	Disable Login for the Default Superuser - Cassandra	
2706	User Roles with the Grantable Permission	
2707	User Roles with the Authorize Permission	

VA Scan Credential Requirements

- Guardium VA supplies scripts for each supported DBMS to help setup appropriate privileges to successfully execute VA. This is done outside of the Guardium appliance usually using a native database client.
- The gdmmonitor-DSE-Cassandra.sql script is located in /var/log/guard/gdmmonitor_scripts

```
[root@gva07 gdmmonitor_scripts]# cat gdmmonitor-DSE-Cassandra.sql
-----
-- Description
-----
-- Database Type: DataStax Cassandra
--
-- This script grant privilege to the 'GDMMONITOR' role (requirement for database assessment tests).
--
-----
-- before running this script
-----
--
-- CREATE A USER ROLE CALL 'SQLGUARD' or name of your choice.
--
-- For example:
--     CREATE ROLE SQLGUARD WITH PASSWORD = 'V3ryC0mPlex' AND LOGIN = true;
--
-----
-- after running this script
-----
--
-- GRANT GDMMONITOR TO SQLGUARD;
--
-- 20190501: created the initail gdmmonitor-DSE-Cassandra.sql script
-----
--
-- create 'GDMMONITOR' role
CREATE ROLE GDMMONITOR;
--
-- Grant select permission for keyspaces to GDMMONITOR role for read-only access.
GRANT SELECT ON KEYSPACE system_auth TO GDMMONITOR;
GRANT SELECT ON KEYSPACE system TO GDMMONITOR;
```

DataStax Cassandra DataSource

- Use the gdmmonitor-DSE-Cassandra.sql script to create required roles to access the database
- Supporting native and LDAP authentication with SSL
- Require to upload a SSL client certificate in .pem format for Cassandra database that setup with mutual authentication.

Update datasource

* Application type

Security Assessment

* Name

DPS: DSE 6.0.2 FAIL on dba-datastax-sa01 SSL

* Database type

DATASTAX CASSANDRA (DataDirect)

Description

☒ Share datasource ?

☒ Use SSL

Add certificate

☒ Import server ssl certificate

☐ Use LDAP

Authentication

* Credential type

☒ Assign credentials ☐ External password ☐ None

* User name

sqlguard

* Password

Location

* Host name/IP

9.98.176.188

* Port number

9042

Database

system

Connection property

Ex: prop1=value;prop2=value

Custom URL

Show advanced options

☒ Connection successful

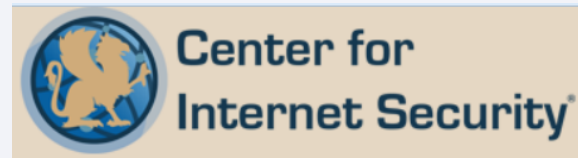
Test connection

Save

Close

DataStax Cassandra Reference

- DSE Admin Guide – https://docs.datastax.com/en/dse/6.7/dse-admin/datastax_enterprise/security/securityTOC.html
- DataStax Security Assurance- <https://www.datastax.com/products/datastax-security-assurance>
- Apache Cassandra - <http://cassandra.apache.org/>
- CIS unpublished benchmark - <https://workbench.cisecurity.org/>
- Cassandra Security google community - <https://docs.google.com/document/d/13-yu-1a0MMkBiJFPNkYoTd1Hzed9tgKltWi6hFLZbsk/e/dit#heading=h.xq6exsjcda8>
- CVE - <https://cve.mitre.org/index.html>



Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Names

DataStax Cassandra VA Tests

Version: Datastax Cassandra DSE



Results for Security Assessment: (wl) DSE fail dba-cloudera-sa02
Assessment executed: 2019-06-05 03:28:02



Version: Datastax Cassandra DSE
Test category: Ver. Test severity: Major

dba-cloudera-sa02 DSE 5.1.10 port 9044
Datasource type: DATASTAX CASSANDRA Datasource severity: None

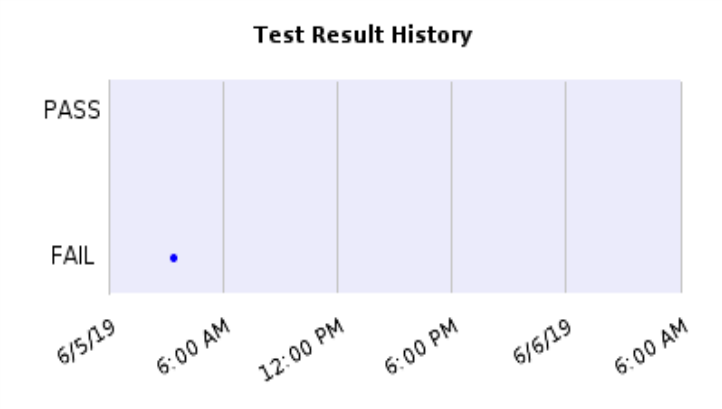
Fail

Version: DATASTAX CASSANDRA '5.1'.
Short Description: This test checks whether your current Datastax cassandra DSE version is a vendor-supported version. Datastax does not provide security fixes or software updates to unsupported software versions.
External Reference: Guardium, Test ID 573

Recommendation: The Datastax cassandra DSE installed is not one of the standard Datastax versions; it is recommended that you upgrade this Datastax cassandra instance to an acceptable version defined in the "Datastax cassandra DSE Version+Patches" group.

Details
N/A

[Close this window](#)



Datastax Cassandra DSE Patch Level



Results for Security Assessment: (wl) DSE fail

Assessment executed: 2019-06-05 00:54:39



Datastax Cassandra DSE Patch Level

Test category: Ver. Test severity: Major

DPS: DSE 6.7.0 FAIL on dba-datastax-sa02 LDAP

Datasource type: DATASTAX CASSANDRA Datasource severity: None

Fail

Current database patch: DATASTAX CASSANDRA 6.7 '0'. Recommended patch >= : DATASTAX CASSANDRA 6.7 '3'.

Short Description: This test checks the patch level of your Datastax Cassandra DSE database. Good security practice requires that you upgrade Datastax cassandra DSE to the latest patch level available for your version to ensure that you have all available security fixes and software upgrades.

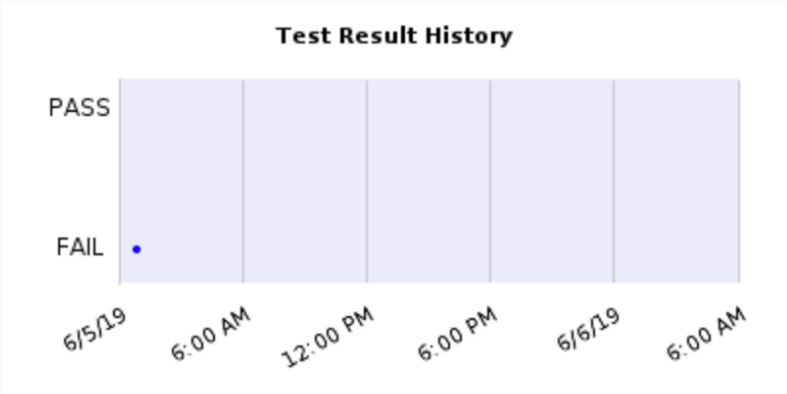
External Reference: Guardium, Test ID 574

Recommendation: The Datastax cassandra system is not patched to your standard level for this version. We recommend that you upgrade this database to an accepted patch level. Please note, if you are required to meet certain corporate version and/or patch requirements or if you have applied a recent version and/or patch, you can modify or add the entries to our existing "Datastax cassandra DSE Version+Patches" group and will help you pass this test.

Details

N/A

Close this window



Default Port Not used



Results for Security Assessment: (wl) DSE fail



Assessment executed: 2019-06-05 00:54:39

Default Port Not used

Test category: Conf. Test severity: Major

DPS: DSE 6.7.0 FAIL on dba-datastax-sa02 LDAP

Datasource type: DATASTAX CASSANDRA Datasource severity: None

Fail

The DataStax cassandra database is using default port.

Short Description: This test checks that Datastax Cassandra database is not using default port 9042. The default port is widely known and is an easy target for attackers.

External Reference: DSE Administrator Guide

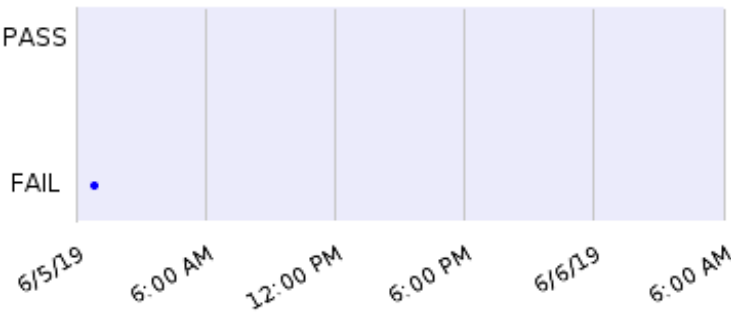
Recommendation: The default port is in use for the DataStax cassandra database. The default port is widely known and is an easy target for attackers. We recommend that you use a different port other than 9042. Please make the recommended change(s) to the cassandra.yaml configuration file by setting the native_transport_port parameter to a non default port.

Details

N/A


Close this window

Test Result History



Nested Grants on Roles

IBM Guardium®

Results for Security Assessment:  (wl) DSE fail
Assessment executed: 2019-06-05 00:54:39



Nested Grants on Roles

Test category: Auth. Test severity: Major

DPS: DSE 6.7.0 FAIL on dba-datastax-sa02 LDAP

Datasource type: DATASTAX CASSANDRA Datasource severity: None

Fail

Nested role grants were found. Including 0 items present in exceptions group.

Short Description: This test checks for a non-login role granted to another non-login role instead of a login user role. When granting a role to a role, you can easily grant the role that may not be intended for the individual grantee. It may also be less obvious when performing auditing on privileges by an auditor. It is recommended to grant the non-login role directly to individual users/login roles as required rather than to other non-login roles.

External Reference: DSE Administrator Guide

Recommendation: We recommend users avoid granting non-login roles to other non-login roles. Best practice mandates that you should grant the non-login role directly to individual users/login roles as required rather than to other non-login roles. Please review the output to make sure role nesting is avoided.

Details

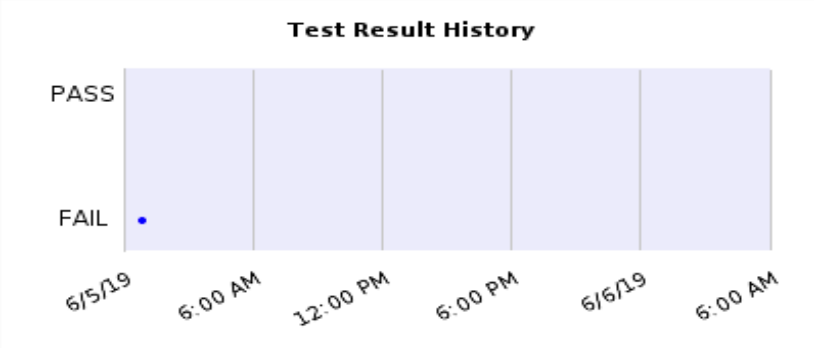
Add Selected Members To Exception Group

Create Test Details Exception

Following role and member are both non-login roles:

role = guardium_role2 : member = guardium_role

Close this window



No Individual User Privileges - Data Resources

IBM Guardium®

Results for Security Assessment: **(wl) DSE fail**

Assessment executed: 2019-06-05 00:54:39

No Individual User Privileges - Data Resources

Test category: Priv. Test severity: Major

DPS: DSE 6.7.0 FAIL on dba-datastax-sa02 LDAP

Datasource type: DATASTAX CASSANDRA Datasource severity: None

Fail

One or more can_login roles granted with privileges on data resources were found. Including 0 items present in exceptions group.

Short Description: This test checks for the can_login user roles granted with privileges on data resources. Data resources are keyspaces, types, tables, and rows. Access is controlled using a modeled hierarchy. Granting and revoking a privilege on a top level object automatically allows the same permission on all ancestors. Privileges granted to a login role are difficult to maintain and create a risk of misuse. Best practice mandates that you should grant object privileges only to non-login roles, and then grant those roles to individual can_login user roles as required.

External Reference: DSE Administrator Guide

Recommendation: We recommend that you grant privileges on data resources only to non-login roles and then grant those roles to individual can_login user roles as required. To revoke privileges, issue the following SQL statement: `REVOKE <permission> ON <resource_name> FROM <role_name>;`

Details

Add Selected Members To Exception Group

Create Test Details Exception

Following roles granted with privileges on data resources:

Role = mdemeesh : Resource = data : Permissions = AUTHORIZE
Role = mdemeesh : Resource = data : Permissions = SELECT
Role = vateam : Resource = data/myks : Permissions = ALTER
Role = vateam : Resource = data/myks : Permissions = AUTHORIZE
Role = vateam : Resource = data/myks : Permissions = CREATE
Role = vateam : Resource = data/myks : Permissions = DESCRIBE
Role = vateam : Resource = data/myks : Permissions = DROP
Role = vateam : Resource = data/myks : Permissions = MODIFY
Role = vateam : Resource = data/myks : Permissions = SELECT
Role = vateam : Resource = data/myks/user : Permissions = ALTER
Role = vateam : Resource = data/myks/user : Permissions = AUTHORIZE
Role = vateam : Resource = data/myks/user : Permissions = DROP
Role = vateam : Resource = data/myks/user : Permissions = MODIFY
Role = vateam : Resource = data/myks/user : Permissions = SELECT
Role = va_user : Resource = data : Permissions = SELECT

Close this window



Test Result History



No Individual User Privileges - Functions Resources

IBM Guardium®

Results for Security Assessment: (wl) DSE fail

Assessment executed: 2019-06-05 00:54:39

No Individual User Privileges - Functions Resources

Test category: Priv. Test severity: Major

DPS: DSE 6.7.0 FAIL on dba-datastax-sa02 LDAP

Datasource type: DATASTAX CASSANDRA Datasource severity: None

Fail

One or more can_login user roles granted with privileges on functions and aggregate resources were found. Including 0 items present in exceptions group.

Short Description: This test checks for the can_login roles granted with privileges on functions and aggregate resources. Although user defined functions and aggregates are located in a keyspace, function permissions are distinct and must be applied separately. Access is controlled using modeled hierarchy. Granting and revoking a privilege on a top level object automatically allows the same permission on all ancestors. User defined functions are only available in environments that have enable_user_defined_functions set to true in the cassandra.yaml file.

External Reference: DSE Administrator Guide

Recommendation: We recommend grant privileges on functions and aggregate resources only to non-login roles and then grant those roles to individual can_login user roles as required. To revoke privileges, issue the following SQL statement: `REVOKE <permission> ON <resource_name> FROM <role_name>;`

Details

Add Selected Members To Exception Group

Create Test Details Exception

Following roles granted with privileges on functions and aggregate resources:

Role = vateam : Resource = functions/myks : Permissions = ALTER

Role = vateam : Resource = functions/myks : Permissions = AUTHORIZE

Role = vateam : Resource = functions/myks : Permissions = CREATE

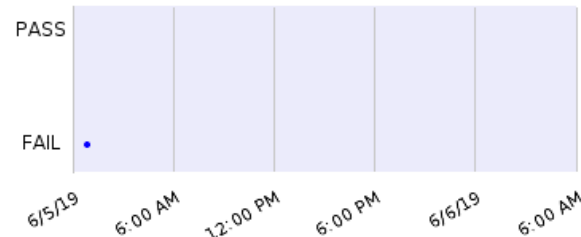
Role = vateam : Resource = functions/myks : Permissions = DROP

Role = vateam : Resource = functions/myks : Permissions = EXECUTE

Close this window



Test Result History



No Individual User Privileges - Proxy Login and Execute

IBM Guardium®

Results for Security Assessment: **(wl) DSE fail**

Assessment executed: 2019-06-05 00:54:39



No Individual User Privileges - Proxy Login and Execute

Test category: Priv. Test severity: Major

DPS: DSE 6.7.0 FAIL on dba-datastax-sa02 LDAP

Datasource type: DATASTAX CASSANDRA Datasource severity: None

Fail

One or more login roles granted with privileges on proxy login and execute were found. Including 0 items present in exceptions group.

Short Description: This test checks for the can_login user roles granted with privileges on proxy login and execute. Proxy login and execute allow a role to execute individual commands or all commands as another role. Typically used when users are interacting with the database through an application that authenticates the users before sending the request to the DataStax Enterprise database. Privileges granted to login roles are difficult to maintain and create a risk of misuse. Best practice mandates that you should grant object privileges only to non-login roles and then grant those roles to individual can_login user roles as required.

External Reference: DSE Administrator Guide

Recommendation: We recommend you grant privileges on proxy login and execute only to non-login roles and then grant those roles to individual can_login user roles as required. To revoke privileges, issue the following SQL statement: `REVOKE <permission_name> ON ROLE <role_name> FROM <application_role>;`

Details

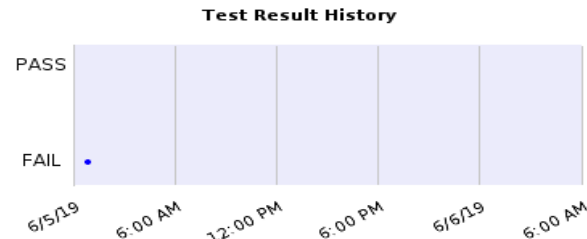
Add Selected Members To Exception Group

Create Test Details Exception

Following roles granted with privileges on proxy login and execute:

Role = vateam : Resource = roles/gdmmonitor : Permissions = PROXY.EXECUTE
Role = vateam : Resource = roles/gdmmonitor : Permissions = PROXY.LOGIN
Role = vateam : Resource = roles/guardium_role : Permissions = PROXY.EXECUTE
Role = vateam : Resource = roles/guardium_role : Permissions = PROXY.LOGIN
Role = vateam : Resource = roles/guardium_role2 : Permissions = PROXY.EXECUTE
Role = vateam : Resource = roles/guardium_role2 : Permissions = PROXY.LOGIN
Role = vateam : Resource = roles/sqlguard : Permissions = PROXY.EXECUTE
Role = vateam : Resource = roles/sqlguard : Permissions = PROXY.LOGIN
Role = vateam : Resource = roles/va_user : Permissions = PROXY.EXECUTE
Role = vateam : Resource = roles/va_user : Permissions = PROXY.LOGIN

Close this window



No Individual User Privileges - MBeans

IBM Guardium®

Results for Security Assessment: [\(wl\) DSE fail dba-cloudera-sa02](#)

Assessment executed: 2019-06-05 03:28:02

No Individual User Privileges - MBeans

Test category: Priv. Test severity: Major

dba-cloudera-sa02 DSE 5.1.10 port 9044

Datasource type: DATASTAX CASSANDRA Datasource severity: None

Fail

One or more login roles granted with privileges on MBeans were found. Including 0 items present in exceptions group.

Short Description: This test checks for the can_login roles granted with privileges on MBeans. After enabling JMX authentication, DataStax Enterprise (DSE) utilities and other third-party tools require MBean access to execute commands. The tools use JMX MBeans to remotely gather information and execute requests. Access is controlled using a modeled hierarchy. Granting and revoking a privilege on a top level object automatically allows the same permission on all ancestors. Privileges granted to a login role are difficult to maintain and create a risk of misuse. Best practice mandates that you should grant object privileges only to non-login roles and then grant those roles to individual can_login user roles as required.

External Reference: DSE Administrator Guide

Recommendation: We recommend you grant privileges on MBeans only to non-login roles and then grant those roles to individual can_login user roles as required. To revoke privileges, issue the following SQL statement: `REVOKE <permission> ON <resource_name> FROM <role_name>;`

Details

[Add Selected Members To Exception Group](#)

[Create Test Details Exception](#)

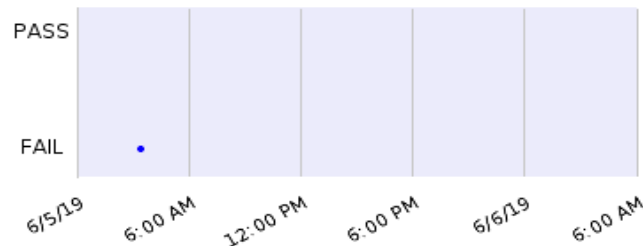
Following roles granted with privileges on MBeans:

Role = va_user : Resource = mbean : Permissions = DESCRIBE

[Close this window](#)



Test Result History



No Individual User Privileges - Remote Procedure Calls

IBM Guardium®

Results for Security Assessment: [\(wl\) DSE fail dba-cloudera-sa02](#)

Assessment executed: 2019-06-05 03:28:02

No Individual User Privileges - Remote Procedure Calls

Test category: Priv. Test severity: Major

dba-cloudera-sa02 DSE 5.1.10 port 9044

Datasource type: DATASTAX CASSANDRA Datasource severity: None

Fail

One or more can_login user roles granted with privileges on remote procedure calls were found. Including 0 items present in exceptions group.

Short Description: This test checks for the can_login user roles granted with privileges on remote procedure calls. Remote Procedure Call (RPC) is a protocol that one program can use to request a service from a program located in another computer on a network without having to understand the network's details. Privileges granted to login roles are difficult to maintain and create a risk of misuse. Best practice mandates that you should grant object privileges only to non-login roles and then grant those roles to individual users/login roles as required.

External Reference: DSE Administrator Guide

Recommendation: We recommend you grant privileges on remote procedure calls only to non-login roles and then grant those roles to individual can_login user roles as required. To revoke privileges, issue the following SQL statement: `REVOKE <permission> ON <ALL REMOTE CALLS | REMOTE METHOD name | REMOTE OBJECT name> FROM <role_name>;`

Details

Add Selected Members To Exception Group

Create Test Details Exception

Following roles granted with privileges on remote procedure calls:

Role = va_user : Resource = rpc : Permissions = AUTHORIZE

Role = va_user : Resource = rpc : Permissions = EXECUTE

Role = va_user : Resource = rpc : Permissions = MODIFY

Role = va_user : Resource = rpc : Permissions = SELECT

[Close this window](#)



Test Result History



No Individual User Privileges - Search Indexes

IBM Guardium®

Results for Security Assessment: (wl) DSE fail dba-cloudera-sa02

Assessment executed: 2019-06-05 03:28:02

No Individual User Privileges - Search Indexes

Test category: Priv. Test severity: Major

dba-cloudera-sa02 DSE 5.1.10 port 9044

Datasource type: DATASTAX CASSANDRA Datasource severity: None

Fail

One or more can_login roles granted with privileges on search indexes were found. Including 0 items present in exceptions group.

Short Description: This test checks for the can_login user roles granted with privileges on search indexes. DataStax Enterprise Search Indexes permissions can only be managed on a Search enabled node. Apply search index permissions in addition to keyspace and table permissions. Access is controlled using a modeled hierarchy. Granting and revoking a privilege on a top level object automatically allows the same permission on all ancestors. Privileges granted to login roles are difficult to maintain and create a risk of misuse. Best practice mandates that you should grant object privileges only to non-login roles and then grant those roles to individual can_login user roles as required.

External Reference: DSE Administrator Guide

Recommendation: We recommend you grant privileges on search indexes only to non-login roles and then grant those roles to individual users/login roles as required. To revoke privileges, issue the following SQL statement: `REVOKE <permission> ON <resource_name> FROM <role_name>;`

Details

Add Selected Members To Exception Group

Create Test Details Exception

Following roles granted with privileges on search indexes:

Role = va_user : Resource = search : Permissions = AUTHORIZE
Role = va_user : Resource = search : Permissions = SEARCH.ALTER
Role = va_user : Resource = search : Permissions = SEARCH.COMMIT
Role = va_user : Resource = search : Permissions = SEARCH.CREATE
Role = va_user : Resource = search : Permissions = SEARCH.DROP
Role = va_user : Resource = search : Permissions = SEARCH.REBUILD
Role = va_user : Resource = search : Permissions = SEARCH.RELOAD

Close this window




Test Result History



Review User-Defined Roles

IBM Guardium®

Results for Security Assessment:  (wl) DSE fail
Assessment executed: 2019-06-05 00:54:39

Review User-Defined Roles

Test category: Priv. Test severity: Caution

DPS: DSE 6.7.0 FAIL on dba-datastax-sa02 LDAP

Datasource type: DATASTAX CASSANDRA Datasource severity: None

Fail

One or more unauthorized roles granted to another role were found. Including 0 items present in exceptions group.

Short Description: This test checks for roles granted to another role. Nesting roles gives all the permissions of the role to the member role. Depending on the role and the privileges, grants to the role should be limited. Limiting the accounts that have the certain roles reduces the chances that an attacker can exploit these capabilities.

External Reference: DSE Administrator Guide

Recommendation: We recommend you review the list of roles and its members, decide if that member truly needs that role, and if not, for each member, issue the following SQL statement: `revoke <member> from <role>;`

Details

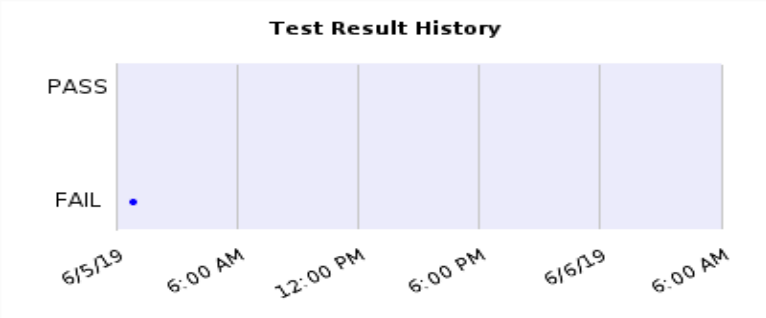
Add Selected Members To Exception Group

Create Test Details Exception

Following roles were found:



- role = gdmmonitor : member = sqlguard
- role = guardium_role2 : member = guardium_role
- role = mdemeesh : member = guardium_role
- role = mdemeesh : member = guardium_role2
- role = vateam : member = guardium_role

Close this window



Superuser privilege granted to users

IBM Guardium®

Results for Security Assessment:  (wl) DSE fail 
Assessment executed: 2019-06-05 00:54:39

Superuser privilege granted to users

Test category: Auth. Test severity: Critical

DPS: DSE 6.7.0 FAIL on dba-datastax-sa02 LDAP

Datasource type: DATASTAX CASSANDRA Datasource severity: None

Fail

Superusers were found. Including 0 items present in exceptions group.

Short Description: This test checks for users that are granted with superuser privilege. The superuser privilege allows you to do anything to the data and have full administrator rights to the database, including changing passwords, creating, dropping roles. Limiting the users that have the superuser role reduces the chances that an attacker can exploit these capabilities. This test checks for superusers that are not cassandra.

External Reference: DSE Administrator Guide

Recommendation: Superusers were found. We recommend to review the list of superusers. For each user, carefully evaluate if that user truly needs the superuser role. If not, for each user, issue the following SQL statement: alter role <role> with superuser=false;

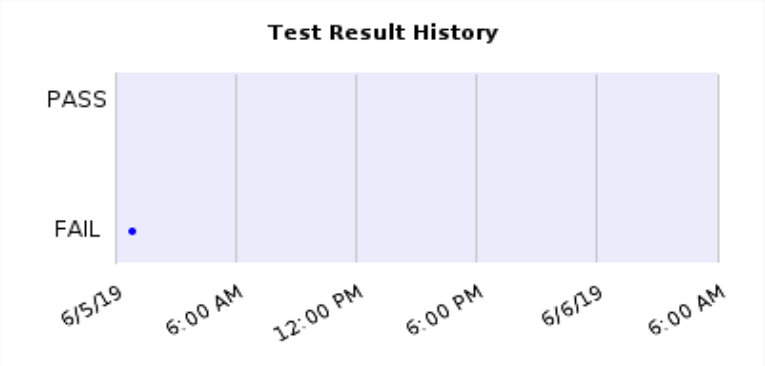
Details

[Add Selected Members To Exception Group](#)

[Create Test Details Exception](#)

vateam

[Close this window](#)



User Roles with the Authorize Permission

IBM Guardium®

Results for Security Assessment: (wl) DSE fail

Assessment executed: 2019-06-05 00:54:39

User Roles with the Authorize Permission

Test category: Priv. Test severity: Critical

DPS: DSE 6.7.0 FAIL on dba-datastax-sa02 LDAP

Datasource type: DATASTAX CASSANDRA Datasource severity: None

Fail

One or more can_login user roles with the authorize permission were found. Including 0 items present in exceptions group.

Short Description: This test checks for the can_login user roles with the Authorize permission. User roles with Authorize permission allows grant or revoke of the permission that has been granted on the resource. This test exclude the role cassandra.

External Reference: DSE Administrator Guide

Recommendation: We recommend that you review the list of the can_login user roles with the authorize permission. Revoke all can_login user roles granted with the authorize permission and instead grant object privileges only to non-login roles, then grant those roles to individual users/login roles as required. To revoke user roles with the authorize permissions, you can use the following command: `REVOKE AUTHORIZE ON <resource_name> FROM <role_name>;`

Details

Add Selected Members To Exception Group

Create Test Details Exception

Following can_login user roles are granted with the authorize permission

Role = mdemeesh : Resource = data

Role = vateam : Resource = data/myks

Role = vateam : Resource = data/myks/user

Role = vateam : Resource = functions/myks

Role = vateam : Resource = roles/gdmmonitor

Role = vateam : Resource = roles/guardium_role

Role = vateam : Resource = roles/guardium_role2

Role = vateam : Resource = roles/sqlguard

Role = vateam : Resource = roles/va_user

Close this window




Test Result History



User Roles with the Grantable Permission

IBM Guardium®

Results for Security Assessment:  (wl) DSE fail
Assessment executed: 2019-06-05 00:54:39



User Roles with the Grantable Permission

Test category: Priv. Test severity: Critical

DPS: DSE 6.7.0 FAIL on dba-datastax-sa02 LDAP

Datasource type: DATASTAX CASSANDRA Datasource severity: None

Fail

User roles with the grantable permission were found. Including 0 items present in exceptions group.

Short Description: This test checks for the can_login user roles with the grantable permission. User roles with the grantable permission allows grant or revoke of the permission on the resource to another role, other than any of their own roles.

External Reference: DSE Administrator Guide

Recommendation: We recommend that you review the list of the can_login user roles with the grantable permission. For each login user role, carefully evaluate if that user truly needs the grantable permission. To revoke user roles with the grantable permission, you can use the following command: `REVOKE AUTHORIZE FOR <permission_list> ON <resource_name> FROM <role_name>;`

Details

Add Selected Members To Exception Group

Create Test Details Exception

Following user roles with the grantable permissions were found:

Role = mdemeesh : Resource = data : Grantable_Permission = ALTER
Role = mdemeesh : Resource = data : Grantable_Permission = CREATE
Role = mdemeesh : Resource = data : Grantable_Permission = DESCRIBE
Role = mdemeesh : Resource = data : Grantable_Permission = DROP
Role = mdemeesh : Resource = data : Grantable_Permission = MODIFY
Role = mdemeesh : Resource = data : Grantable_Permission = SELECT

[Close this window](#)

Test Result History



Disable Login for the Default Superuser - Cassandra

IBM Guardium®

Results for Security Assessment: (wl) DSE fail

Assessment executed: 2019-06-05 01:42:40



Disable Login for the Default Superuser - Cassandra

Test category: Auth. Test severity: Critical

DPS: DSE 6.0.2 FAIL on dba-datastax-sa01 SSL/LDAP

Datasource type: DATASTAX CASSANDRA Datasource severity: None

Fail

The login for the default superuser is not disabled.

Short Description: The default installation of Cassandra includes a superuser role named cassandra. Superuser permissions allow for the creation, deletion, and permission management of other users. Considering the cassandra role is well known, it should not be a superuser or one which is used for any administrative tasks. We recommend you create your own superuser account and disable the login for the default cassandra account.

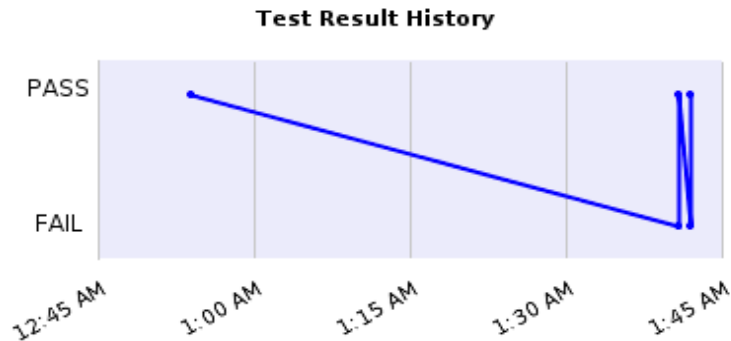
External Reference: DSE Administrator Guide

Recommendation: The login for the default superuser cassandra is not disabled in your database. We recommend disabling the cassandra user. You can disable the cassandra user by executing the following statement, for example, in the cqlsh console: `UPDATE system_auth.roles SET can_login=FALSE WHERE role='cassandra'`

Details

N/A

[Close this window](#)



Remove the Superuser Role from the Cassandra Account

IBM Guardium®

Results for Security Assessment: (wl) DSE fail

Assessment executed: 2019-06-05 01:42:40



Remove the Superuser Role from the Cassandra Account

Test category: Auth. Test severity: Critical

DPS: DSE 6.0.2 FAIL on dba-datastax-sa01 SSL/LDAP

Datasource type: DATASTAX CASSANDRA Datasource severity: None

Fail

The superuser role for the cassandra account exists.

Short Description: The default installation of Cassandra includes a superuser role named Cassandra. Superuser permissions allow for the creation, deletion, and permission management of other users. Considering the Cassandra role is well known, it should not be a superuser or one which is used for any administrative tasks. We recommend you create your own superuser account and remove the superuser role from the default Cassandra account.

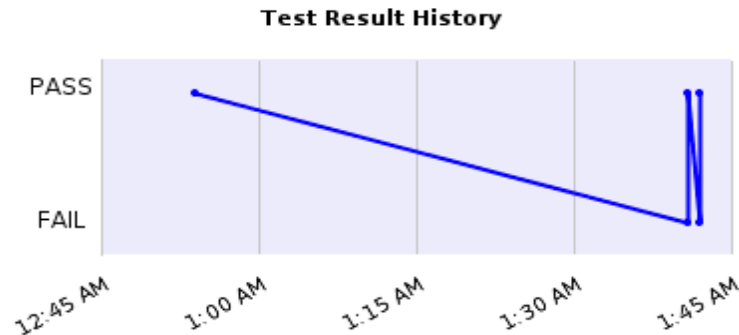
External Reference: DSE Administrator Guide

Recommendation: The Cassandra account has the superuser role in your database. We recommend you remove the superuser role from the default Cassandra account. You can remove the superuser role from the Cassandra account by executing the following statement, for example, in the cqlsh console: `UPDATE system_auth.roles SET is_superuser=false WHERE role='cassandra'`

Details

N/A

[Close this window](#)



Guardium V11 New Release Training

GUI - space optimization and data density

Group Builder enhancements

Unable to Modify or Delete Datasources

Allow the upload of a certificate-key pair to Guardium for the web UI

Contents

Overview

Use cases

Demo

Architecture

Implementation considerations

Troubleshooting

Q & A

Reference materials

Overview (GRD-21114)

Dashboard reports can now be arbitrarily resized to allow better optimization of available space.

New functionality was added to allow users to refresh the entire dashboard simultaneously instead of refreshing each report individually.

What's New

- Arbitrarily resize dashboard reports
- Refresh entire dashboard at once

Benefits

- Better use of available space
- Make it easier to refresh dashboard data

Overview (GRD-21114) – Cont'd

My Dashboard [2019-06-04-13:25:40]

Number of columns ☐ 1 ☒ 2 ☐ 3 [?](#)

Add Report

Delete dashboard

View mode

Refresh

Full dashboard refresh

Failed User Login Attempts - Distributed

Start Date: 2019-06-04 10:27:06 | End Date: 2019-06-04 13:27:06
Using Merge Period Between 2019-05-29 and 2019-06-04.

More

[Edit](#) [Email](#) [Print](#) [Filter](#) [Star](#) [Share](#) [Refresh](#) Status

Export Actions Graphical View ?

Date	User Name	Source Address	Destination Address	Database Protocol	Exception Timestamp	Count of Exceptions	Source Host
2019-06-04 11:00:00	?	9.70.165.111	9.70.165.111	ORACLE	2019-06-04 11:00:59	14	sys-vm27.guard.swg.usma.ibm.com
2019-06-04 11:00:00	?	9.70.165.111	9.70.165.111	ORACLE	2019-06-04 11:01:00	32	sys-vm27.guard.swg.usma.ibm.com

Total: 643 Selected: 0

< 1 2 3 ... 33 >

Resize handle

Administrative Commands By User Dashboard-Distributed

Start Date: 2019-06-04 10:26:55 | End Date: 2019-06-04 13:26:55
Using Merge Period Between 2019-05-29 and 2019-06-04.

More

[Edit](#) [Email](#) [Print](#) [Filter](#) [Star](#) [Share](#) [Refresh](#) Status

Export Actions Graphical View ?

Date	Source	TZ	DB User Name	Total access
2019-06-04 11:00:00	sys-vm93.guard.swg.usma.ibm.com	-04:00	DB2_F272	181
2019-06-04 11:00:00	sys-vm93.guard.swg.usma.ibm.com	-04:00	DB2_E8SM	181
2019-06-04 11:00:00	sys-vm93.guard.swg.usma.ibm.com	-04:00	DB2_RRB9	181

Total: 71 Selected: 0

< 1 2 3 4 >

20 | 50 | 100

Exception Count

Start Date: 2019-06-04 10:26:17 | End Date: 2019-06-04 13:26:17
Using Merge Period Between 2019-05-29 and 2019-06-04.

More

[Edit](#) [Star](#) [Share](#) ?

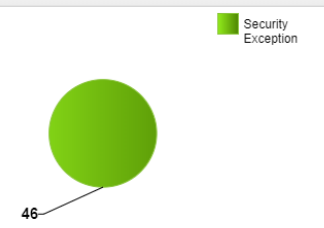
46

Exceptions Distribution

Start Date: 2019-06-04 10:26:11 | End Date: 2019-06-04 13:26:11
Using Merge Period Between 2019-05-29 and 2019-06-04.

More

[Filter](#) [Star](#) [Share](#) [Refresh](#) Tabular View ?



Overview (GRD-21111)

In group builder, for hierarchical groups, show flattened group member count in addition to hierarchical group member count.

What's New

- Show flattened member count for hierarchical groups

Benefits

- Help users see which hierarchical groups are actually empty when flattened.

Overview (GRD-21111) – Cont'd

Group Builder								
<div><div><div></div><div></div><div></div><div></div><div></div><div></div></div><div>Download as CSV</div><div>Actions</div><div>All group types</div><div>Filter</div></div>								
Name	Type	Application	Members	Populated by	Hierarchical	Used in discovery scenario	Used in policy	Used in query
Test H Group	OBJECTS	Public	2 / 0		✓			
AA Classifier ALL Values 1559576642563	OBJECTS							
AA Exclude Schemas1559576642561	SCHEMA							

Format: X / Y where X is the member count and Y is the flattened member count.
Run "Flatten hierarchical groups" to update the flattened member count.

After performing the flatten groups action:

Group Builder								
<div><div><div></div><div></div><div></div><div></div><div></div><div></div></div><div>Download as CSV</div><div>Actions</div><div>All group types</div><div>Filter</div></div>								
Name	Type	Application	Members	Populated by	Hierarchical	Used in discovery scenario	Used in policy	Used in query
Test H Group	OBJECTS	Public	2 / 4		✓			

Overview (GRD-23303)

Previously granting access for a datasource to a role only allowed read-only access for that role. In v11 that restriction can be lifted to allow users to grant full control over owned datasource to specific groups.

What's New

- Allow granting full control over datasource to a role

Benefits

- Help users better manage datasources

Overview (GRD-23303) – Cont'd

1. Create datasource and grant permission to user role

Application type: Classifier

Name: swan

datasource
Grant other users access to the item you are defining by assigning security roles.

☐ All roles Grant access to everyone

☐ cli

☐ DataPrivacy

☐ datasec-exempt

☐ dba

☐ diag

☐ fam

☐ GDPR

☐ GDPR FAM

☐ infosec

☐ inv

☐ netadm

☐ pci

☐ review-only

☐ sox

☒ **user**

☐ vulnerability-assess

OK Cancel

Roles 1 role assigned.

CAS database instance

Account Enter owner account

2. By default, as a user try to update the datasource an error will occur

Update datasource

Application type: Classifier

Name: swan1

Database type: Oracle (DataDirect - Service Name)

Description:

☒ Share datasource ?

☐ Use SSL Add certificate

Authentication

☒ Assign

User name:

Password:

Location:

Host name:

Port number: 1521

Service name: on8swan0

Schema:

Connection property: Ex: prop1=value;prop2=value

Custom URL:

Show advanced options

You must save the datasource before testing the connection

Test connection Save Close

Failed to save datasource "swan1".
Only the owner or admin can modify this datasource.
Close

Overview (GRD-23303) – Cont'd

3. Enable the full control feature by executing GrdAPI command

```
gat-daily-vm10.guard.swg.usma.ibm.com> grdapi modify_guard_param paramName=ALLOW_DATASOURCE_FULL_CONTROL_BY_ROLE paramValue=true  
ID=0  
ok  
gat-daily-vm10.guard.swg.usma.ibm.com> █
```

The screenshot shows the 'Update datasource' dialog box. The 'Name' field is highlighted with a red rectangle and contains the text 'swan1'. The 'Database type' is set to 'Oracle (DataDirect - Service Name)'. The 'User name' is 'scott' and the 'Password' is masked with dots. The 'Host name/IP' is 'swan', 'Port number' is '1521', and 'Service name' is 'on8swan0'. The 'Authentication' section has 'Assign credentials' selected. The 'Test connection' button is visible at the bottom.

Update datasource

* Application type: Classifier

* Name: swan1

* Database type: Oracle (DataDirect - Service Name)

Description:

☒ Share datasource ?

☐ Use SSL [Add certificate](#)

Authentication

* Credential type: ☒ Assign credentials ☐ External password ☐ None

* User name: scott

* Password:

Location

* Host name/IP: swan

* Port number: 1521

* Service name: on8swan0

Schema:

Connection property: Ex: prop1=value;prop2=value

Custom URL:

[Show advanced options](#)

[Test connection](#) [Save](#) [Close](#)

4. Datasource can now be successfully saved by the user role.

Overview (GRD-25809)

In order to increase awareness of Guardium Ecosystem functionality among users modifications were made to the Guardium UI to make Ecosystem related functionality more prominent even when ecosystem is disabled.

What's New

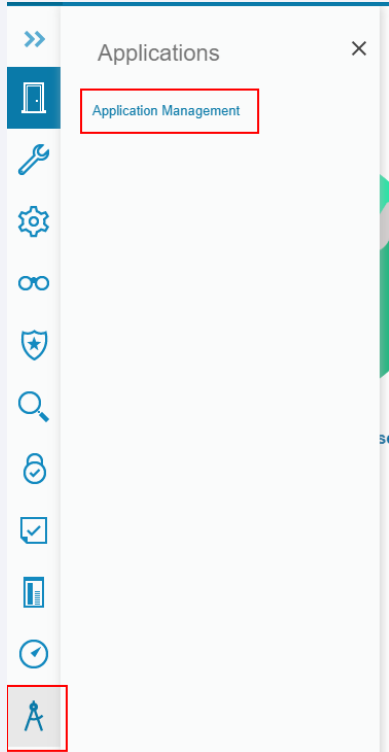
- Ecosystem related UI is visible even when functionality is not disabled
- Link to app exchange was added to the UI to allow for easier

Benefits

- Increases awareness of ecosystem functionality

Overview (GRD-25809) – Cont'd

1. “Application Management” navigation link moved under “Applications” category and is visible even if ecosystem feature is off.



Application Management

Application Lifecycle is not enabled. Enable the application lifecycle using the following CLI command:
store system ecosystem on

2. “Guardium App Exchange” link is shown when working with ecosystem UI

Application Management

Discover applications on the [Guardium App Exchange](#).



Download as CSV

Start

Stop

Update

Assign roles

Action log

Update credentials

Name	Description	Status

Overview (GRD-13822)

Allow users to set custom security certificate for communication between guardium appliance and client machine when operating guardium web ui.

What's New

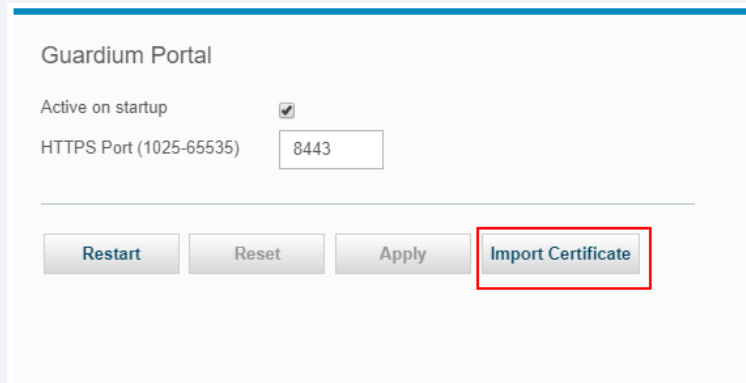
- Allow users to customize web ui certificate

Benefits

- Users can use a stronger more secure certificate to operate guardium web ui

Overview (GRD-13822) – Cont'd

1.



Guardium Portal

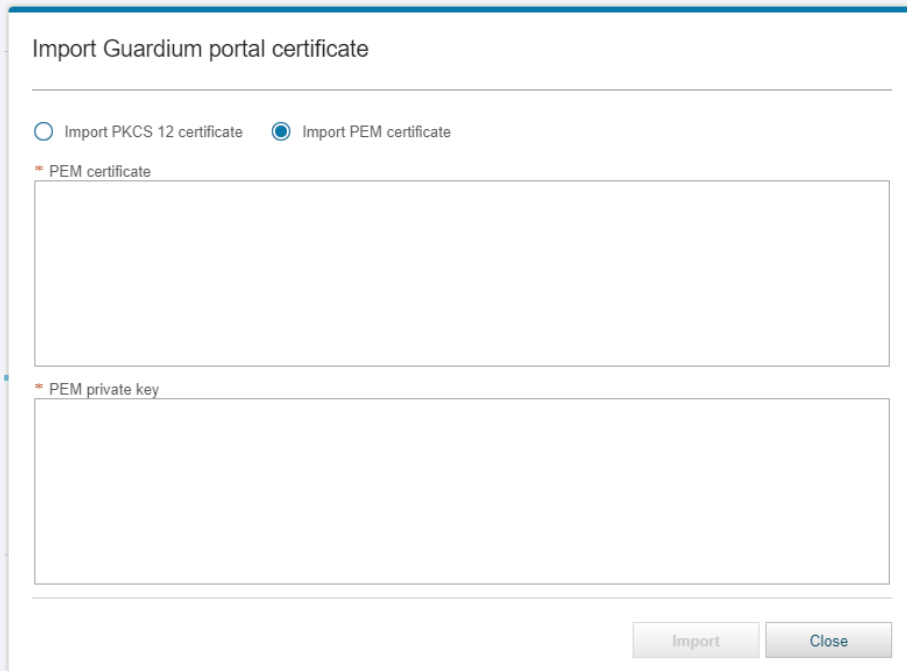
Active on startup ☒

HTTPS Port (1025-65535)

Restart **Reset** **Apply** **Import Certificate**

Can import in either PKCS 12 or PEM format

2.2



Import Guardium portal certificate

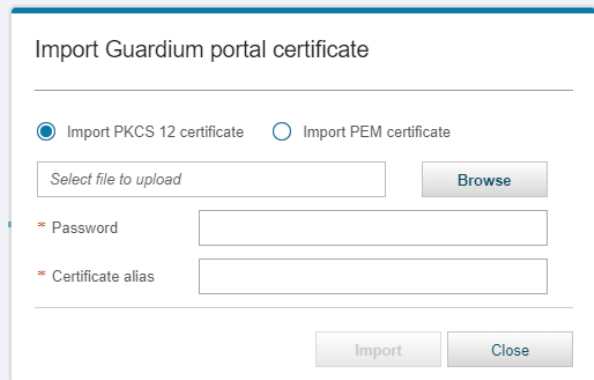
☐ Import PKCS 12 certificate ☒ Import PEM certificate

* PEM certificate

* PEM private key

Import **Close**

2.1



Import Guardium portal certificate

☒ Import PKCS 12 certificate ☐ Import PEM certificate

Select file to upload **Browse**

* Password

* Certificate alias

Import **Close**

Overview (GRD-13822) – Cont'd

3.1

Import Guardium portal certificate

☒ Import PKCS 12 certificate ☐ Import PEM certificate

testkeystore.p12

* Password

* Certificate alias

3.2

Import Guardium portal certificate

☐ Import PKCS 12 certificate ☒ Import PEM certificate

* PEM certificate


```
-----BEGIN CERTIFICATE-----
MIID5TCCAs2gAwIBAgIJAInNlw9LyhjTMA0GCSqGSIb3DQEBBCwUAMIGIMQswCQYD
VQQGEwJDQTEQMA4GA1UECAwHT250YXJpbzEQA4GA1UEBwwHVGV9yb250bzEMMAoG
A1UECgwDSUJNMREwDwYDVQQLDAhTZWN1cm0eTERMA8GA1UEAwwiR3VhcmRpdW0x
ITAFBgkqhkiG9w0BCQEWEmF2Y2WlUyZ2hAY2EuaWJlLnNvbTAeFw0xOTA2MDQyMjUz
MDIaFw0yMDA2MDMyMjUzMDIaMIGIMQswCQYDVQQGEwJDQTEQMA4GA1UECAwHT250
YXJpbzEQA4GA1UEBwwHVGV9yb250bzEMMAoGA1UECgwDSUJNMREwDwYDVQQLDAhT
ZWN1cm0eTERMA8GA1UEAwwiR3VhcmRpdW0xITAFBgkqhkiG9w0BCQEWEmF2Y2WlU
Y2hAY2EuaWJlLnNvbTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALab
lqgFKwBxkLUAOvjNVX6+c2OXnvZEXxOOILuDtYk7JVK63mpP8WVieYRHmUZI1h7j3B
-----
```

* PEM private key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAwqggSkAgEAAoIBAQCwG5aoBSsAcZC1
ADr4zVV+vnNjI572RMTipS7q7cpOyVSut5qI/FonmER5IGZdye49wWhtagImqY27
hXY3/GOKTU5AEEnJcsjeyvM/n5qaneU21f2ir8sBsYhV+j+1OYqtl12qW+/nZRdzd
unaC90rluUdQlBqM5nm8xW1SWCPnRvOu0RFLWGS55hrE1lulolnwQNGdsJSmKF88
aMKfov7WqUgScI7dIYS5XJm8w3Keou3QHIO2ERYPIMer/rxM8SLt/lqLunl6dR1Q
dWcDQUznaMq9p77Pac5khHWCc/IDbatKYPIDE+FNf+mMW4sViqoeGaLwDTVexviX
70W/63tPaqMBAAECggEAMcFZq1bac1GipMDP6IN66Dg+uaCY1NNRHVAKEpacUe4n
8sUE81KU1iL7Fa6LzU5h1SiTrD0BAe8QcC6g2+h+7mi49vk/PILLyz/1LXvJEf/
qlu6svn+y6BamktnrHMC71s7AN875oBcNPBr/bWPlk+h5YMikaDkoXIASL1N4qV9
-----
```

4

Confirmation

 Confirmation

Certificate imported. Restart the UI for the changes to take effect.

If you experience problems, restore the keystore to its previous state using the following CLI command: *restore certificate keystore*

Restart the UI now?

Implementation considerations: Limitations/Constraints

GRD-23303 – Unable to Modify or Delete datasource

- Feature is off by default to enable backward compatibility. To enable GrdAPI command needs to be run via CLI or REST to update `GUARD_PARAMETER ALLOW_DATASOURCE_FULL_CONTROL_BY_ROLE` to true

`modify_guard_param paramName=ALLOW_DATASOURCE_FULL_CONTROL_BY_ROLE paramValue=true`

GRD-13822 – Allow upload of certificate-key pair

When specifying PEM formatted strings certificate string must start with `-----BEGIN CERTIFICATE-----` and end with `-----END CERTIFICATE-----`. Key string must start with `-----BEGIN RSA PRIVATE KEY-----` and end with `-----END RSA PRIVATE KEY-----`.

Troubleshooting – Diagnostic procedures

Standard UI troubleshooting applies to all aforementioned deliverables:

- Examine browser javascript console for errors
- Check catalina.out for errors
- Enable debug logging to get more information if necessary

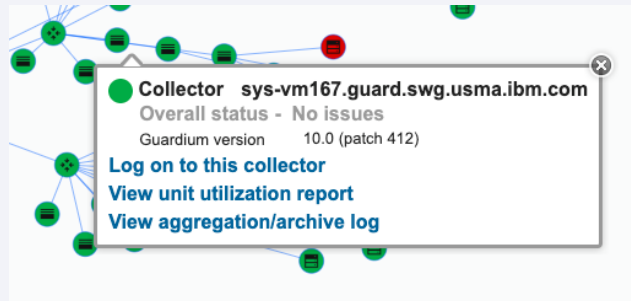
IBM Security Guardium

V 11.0 New Release Training

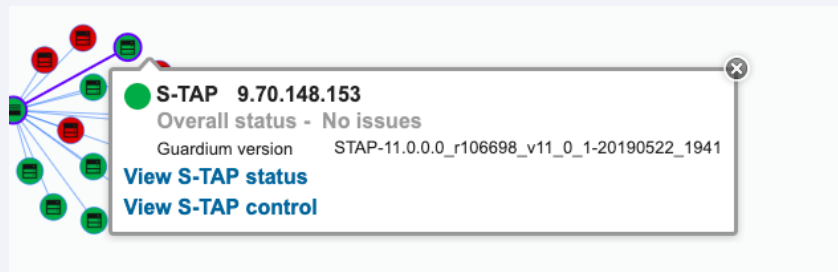
DEPLOYMENT HEALTH ENHANCEMENT

Version Information

Version information for appliance



Version information for STAP



Patch Information & Stale data

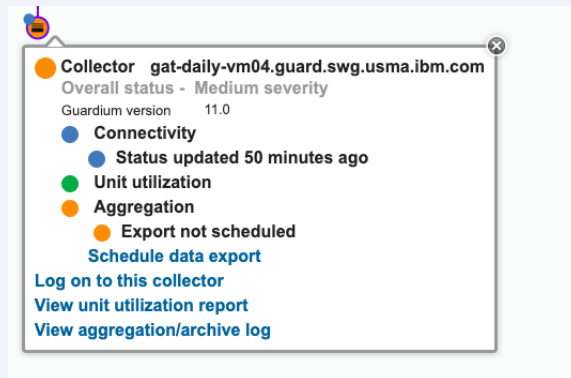
Display patch information for appliance

- The latest patch that has been installed



- New unknown state for stale data

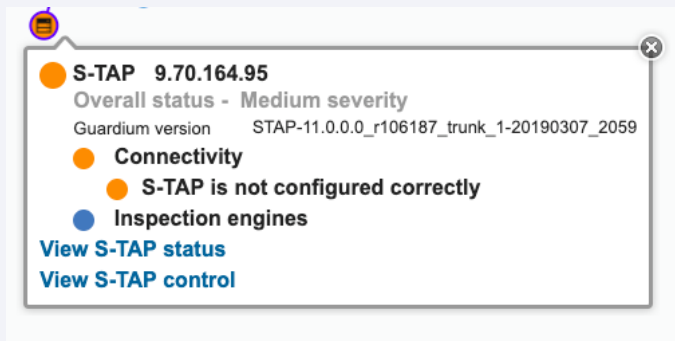
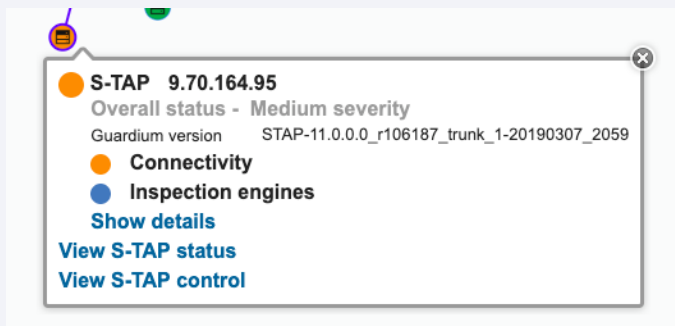
- If data is older than duration set by the change tracker then it is marked as stale
- Will display in format of 'Status update x [minutes|hours|days] ago' depending on how long the data has been stale



Misconfigured STAP

Added STAP new yellow status

- Indicates that there is misconfiguration in STAP configuration.
- Added 'View S-TAP control' to allow user to jump to stap configuration of specified collector



Guardium V11 New Release Training

Mapping Guardium Values to CEF Format in z/OS for IMS and DB2

Overview

What's New

Guardium provides the ability to select the values to display in Alert Messages. For z/OS mainframe, Guardium has added the ability to map several new common event format (CEF) values to the alert message for DB2 and IMS databases.

Those new CEF values are used to real time monitoring of the IMS and DB2 database for z/OS.

Use Cases

- Use Case 1

When a user wants to monitor DB user/ OS user/ client hostname/ DB name/ last error/ SQL no value for mainframe IMS database by real time alert, the user can add relative new fields into the alert template. When alert is triggered, the more detailed information would be saved to syslog or included in email notification or the option selected in rule action.

- Use Case 2

When a user wants to monitor DB protocol version/ client hostname/ DB name/ End user for mainframe DB2 database by real time alert, the user can add relative new fields into the alert template. When alert is triggered, the more detailed information would be saved to syslog or included in email notification or the option selected in rule action.

Demo

Use Case 1 - Monitor DB user/ OS user/ client hostname/ DB name/ last error/ SQL no value for mainframe IMS database by real time alert

Step 1 – Add new fields in alert template

Modify Named Template

Template Name	<input type="text" value="ArcSight_IMS"/>
Template type	<input type="text" value="RT_ALERT"/>
Default message template	<div>CEF:0 IBM Guardium 11.0 %%ruleID %%ruleDescription 5 rt=%%receiptTimeMills cs1=%%severity cs1Label=Severity cs2=%%serverType cs2Label=Server Type cs3=%%classification cs3Label=Classification cat=%%category app=%%DBProtocol cs4=%%DBProtocolVersion cs4Label=DB Protocol Version suser=%%AppUserName sproc=%%SourceProgram act=%%requestType start=%%sessionStartMills externalId=%%violationID duser=%%DBUser dst=%%serverIP dpt=%%serverPort src=%%clientIP spt=%%clientPort proto=%%netProtocol msq=%%SQL String DBUser=%%DBUser OSUser=%%OSUser ClientHostName=%%clientHostname LastError=%%lastError SQLNoValue=%%SQLNoValue</div>

Step 2 – Create a rule action, then choose that alert template

Add New Action

* Rule action	<input type="text" value="ALERT ONCE PER SESSION"/>
* Message Template	<input type="text" value="ArcSight_IMS"/>
* Notification Type	<input type="text" value="SYSLOG"/>

OK

Cancel

Demo

Use Case 1 - Monitor DB user/ OS user/ client hostname/ DB name/ last error/ SQL no value for mainframe IMS database by real time alert

Step 3 – After the alert rule action triggered, check the alert message in syslog

```
Jun  7 11:56:47 ming-vm01 guard_sender[1873]: CEF:0|IBM|Guardium|10.0|20001|Alert IMS|5|rt=1552096313662 cs1=INFO cs1Label=Severity cs2=IMS cs2Label=Server Type cs3= cs3Label=Classification cat= app=IMS cs
4=6 cs4Label=DB Protocol Version user=psb_name=PROGDE2C sproc=MPP act=CONSTRUCT start=1552096313662 externalId=6058000000004353 duser=DSX10041 dst=9.70.144.27 dpt=0 src=9.70.144.27 spt=16390 proto=DLI ms
g=; uid=\DSX10041; prog=\PROGDE2C; job=\MPR10108; step=\REGION; tran=\DE2C; job#\=J0B08264; term=\DSX10041; pcb=\DATAEND; pcb#\=5; dli sts=\bb; desc=\DB Level INSERT; dbd=\DATAENDC; seg=\ORD00001; DBUser=
%%DBUser OSUser=DSX10041 ClientHostName= LastError=bb SQLNoValue=prog=\PROGDE2C; job=\MPR10108; step=\REGION; tran=\DE2C; job#\=J0B08264; desc=\DB Level INSERT; dbd=\DATAENDC; seg=\ORD00001
Jun  7 11:56:47 ming-vm01 guard_sender[1873]: CEF:0|IBM|Guardium|10.0|20001|Alert IMS|5|rt=1552095393331 cs1=INFO cs1Label=Severity cs2=IMS cs2Label=Server Type cs3= cs3Label=Classification cat= app=IMS cs
4=6 cs4Label=DB Protocol Version user=psb_name=PROGHRAA sproc=MPP act=CONSTRUCT start=1552095393331 externalId=6058000000004604 duser=DSX10003 dst=9.70.144.27 dpt=0 src=9.70.144.27 spt=16387 proto=DLI ms
g=; uid=\DSX10003; prog=\PROGHRAA; job=\MPR1GETB; step=\REGION; tran=\HRAA; job#\=J0B08281; term=\DSX10003; pcb=\CLHOTEL; pcb#\=6; dli sts=\bb; p/a=\HOTELA1; desc=\DB Level INSERT; dbd=\PDHOTELA; seg=\RESR
V003; DBUser=%%DBUser OSUser=DSX10003 ClientHostName= LastError=bb SQLNoValue=prog=\PROGHRAA; job=\MPR1GETB; step=\REGION; tran=\HRAA; job#\=J0B08281; desc=\DB Level INSERT; dbd=\PDHOTELA; seg=\RESRV003
Jun  7 11:56:47 ming-vm01 guard_sender[1873]: CEF:0|IBM|Guardium|10.0|20001|Alert IMS|5|rt=1552095724185 cs1=INFO cs1Label=Severity cs2=IMS cs2Label=Server Type cs3= cs3Label=Classification cat= app=IMS cs
4=6 cs4Label=DB Protocol Version user=psb_name=PROGIT2A sproc=MPP act=CONSTRUCT start=1552095724185 externalId=6058000000004862 duser=DSX10009 dst=9.70.144.27 dpt=0 src=9.70.144.27 spt=16387 proto=DLI ms
g=; uid=\DSX10009; prog=\PROGIT2A; job=\MPR10110; step=\REGION; tran=\IT2A; job#\=J0B08266; term=\DSX10009; pcb=\ITEMACT; pcb#\=4; dli sts=\bb; desc=\DB Level GET; dbd=\ITEMACTA; seg=\IA060LOC; DBUser=%%D
Buser OSUser=DSX10009 ClientHostName= LastError=bb SQLNoValue=prog=\PROGIT2A; job=\MPR10110; step=\REGION; tran=\IT2A; job#\=J0B08266; desc=\DB Level GET; dbd=\ITEMACTA; seg=\IA060LOC
Jun  7 11:56:47 ming-vm01 guard_sender[1873]: CEF:0|IBM|Guardium|10.0|20001|Alert IMS|5|rt=1552096603654 cs1=INFO cs1Label=Severity cs2=IMS cs2Label=Server Type cs3= cs3Label=Classification cat= app=IMS cs
4=6 cs4Label=DB Protocol Version user=psb_name=PROGSC4C sproc=MPP act=CONSTRUCT start=1552096603654 externalId=6058000000005118 duser=DSX10014 dst=9.70.144.27 dpt=0 src=9.70.144.27 spt=16389 proto=DLI ms
g=; uid=\DSX10014; prog=\PROGSC4C; job=\MPR10157; step=\REGION; tran=\SC4C; job#\=J0B08263; term=\DSX10014; pcb=\CLINLOG; pcb#\=6; dli sts=\bb; p/a=\INVNTC3; desc=\DB Level INSERT; dbd=\PDINLOGC; seg=\IN03
0ENG; DBUser=%%DBUser OSUser=DSX10014 ClientHostName= LastError=bb SQLNoValue=prog=\PROGSC4C; job=\MPR10157; step=\REGION; tran=\SC4C; job#\=J0B08263; desc=\DB Level INSERT; dbd=\PDINLOGC; seg=\IN030ENG
Jun  7 11:56:47 ming-vm01 guard_sender[1873]: CEF:0|IBM|Guardium|10.0|20001|Alert IMS|5|rt=1552097903344 cs1=INFO cs1Label=Severity cs2=IMS cs2Label=Server Type cs3= cs3Label=Classification cat= app=IMS cs
4=6 cs4Label=DB Protocol Version user=psb_name=PROGIT2D sproc=MPP act=CONSTRUCT start=1552097903344 externalId=6058000000005375 duser=DSX10010 dst=9.70.144.27 dpt=0 src=9.70.144.27 spt=16385 proto=DLI ms
g=; uid=\DSX10010; prog=\PROGIT2D; job=\MPR10169; step=\REGION; tran=\IT2D; job#\=J0B08275; term=\DSX10010; pcb=\ITEMACT; pcb#\=4; dli sts=\bb; desc=\DB Level GET; dbd=\ITEMACTD; seg=\IA060LOC; DBUser=%%D
Buser OSUser=DSX10010 ClientHostName= LastError=bb SQLNoValue=prog=\PROGIT2D; job=\MPR10169; step=\REGION; tran=\IT2D; job#\=J0B08275; desc=\DB Level GET; dbd=\ITEMACTD; seg=\IA060LOC
```

Demo

Use Case 2 - Monitor DB protocol version/ client hostname/ DB name/ End user for DB2 z/OS database by real time alert

Step 1 – Add new fields in alert template

Modify Named Template

Template Name

ArcSight_db2z

Template type

RT_ALERT

Default message template

CEF:0|IBM|Guardium|10.0|%%ruleID|%%ruleDescription|5|rt=%%receiptTimeMills
cs1=%%severity cs1Label=Severity cs2=%%serverType cs2Label=Server Type
cs3=%%classification cs3Label=Classification cat=%%category app=%%DBProtocol
cs4=%%DBProtocolVersion cs4Label=DB Protocol Version suser=%%AppUserName
sproc=%%SourceProgram act=%%requestType start=%%sessionStartMills
externalId=%%violationID duser=%%DBUser dst=%%serverIP dpt=%%serverPort
src=%%clientIP spt=%%clientPort proto=%%netProtocol msg=%%SQLString
DBProtocolVersion= %%DBProtocolVersion ClientHostName= %%clientHostname
DBName= %%DBName EndUser=%%EndUser

Step 2 – Create a rule action, then choose the alert template

Add New Action

* Rule action

ALERT PER MATCH

* Message Template

ArcSight_db2z

* Notification Type

SYSLOG

OK

Cancel

Demo

Use Case 2 - Monitor DB protocol version/ client hostname/ DB name/ End user for DB2 z/OS database by real time alert

Step 3 – After the alert rule action triggered, check the alert message in syslog

```
Jun 6 00:51:09 gat-daily-vm09 GuardiumSniffer[14912]: subject "SQLGUARD ALERT", "CEF:0|IBM|Guardium|10.0|20000|Alert only|5|rt=1552061995927 cs1=INFO cs1Label=Severity cs2=DB2 cs2Label=Server Type cs3= cs3Label=Classification cat= app=D
B2/Z cs4= cs4Label=DB Protocol Version suser=PLAN=DISTSERV ; SQLID=SUSHMIT ; PROG=SYSLH200 ; DB_NAME=DSN00326 sproc=GHP04.GUARD.SWG.:DB2JCC_APPLI act=SQL_GPB start=1552061995927 externalId=0 duser=SUSHMIT dst=9.70.144.27 dpt=8050 src=9.70
.148.161 spt=14643 proto=DRDA:SERVER msg=UPDATE GDMC_STLAB3E_DB1B set CurrentTime \= '/03/08/19 12:16:11.020', ReconnectCount \= 1, SentCount \= SentCount +1 where Connection_ \= 1 and TestID \= 'ghp04 -count -update -server nulld3e11dbc
-test_duration 900 -delay 799 -concurrent_connections 2' DBProtocolVersion= ClientHostName= 9.70.148.161 DBName= DSN00326 EndUser=SUSHMIT"
Jun 6 00:51:09 gat-daily-vm09 GuardiumSniffer[14912]: subject "SQLGUARD ALERT", "CEF:0|IBM|Guardium|10.0|20000|Alert only|5|rt=1552061997005 cs1=INFO cs1Label=Severity cs2=DB2 cs2Label=Server Type cs3= cs3Label=Classification cat= app=D
B2/Z cs4= cs4Label=DB Protocol Version suser=PLAN=DISTSERV ; SQLID=SUSHMIT ; PROG=SYSLH200 ; DB_NAME=DSN00326 sproc=GHP04.GUARD.SWG.:DB2JCC_APPLI act=SQL_GPB start=1552061997005 externalId=0 duser=SUSHMIT dst=9.70.144.27 dpt=8050 src=9.70
.148.161 spt=14643 proto=DRDA:SERVER msg=UPDATE GDMC_STLAB3E_DB1B set CurrentTime \= '/03/08/19 12:16:12.107', ReconnectCount \= 1, SentCount \= SentCount +1 where Connection_ \= 1 and TestID \= 'ghp04 -count -update -server nulld3e11dbc
-test_duration 900 -delay 799 -concurrent_connections 2' DBProtocolVersion= ClientHostName= 9.70.148.161 DBName= DSN00326 EndUser=SUSHMIT"
Jun 6 00:51:09 gat-daily-vm09 GuardiumSniffer[14912]: subject "SQLGUARD ALERT", "CEF:0|IBM|Guardium|10.0|20000|Alert only|5|rt=1552061998086 cs1=INFO cs1Label=Severity cs2=DB2 cs2Label=Server Type cs3= cs3Label=Classification cat= app=D
B2/Z cs4= cs4Label=DB Protocol Version suser=PLAN=DISTSERV ; SQLID=SUSHMIT ; PROG=SYSLH200 ; DB_NAME=DSN00326 sproc=GHP04.GUARD.SWG.:DB2JCC_APPLI act=SQL_GPB start=1552061998086 externalId=0 duser=SUSHMIT dst=9.70.144.27 dpt=8050 src=9.70
.148.161 spt=14643 proto=DRDA:SERVER msg=UPDATE GDMC_STLAB3E_DB1B set CurrentTime \= '/03/08/19 12:16:13.171', ReconnectCount \= 1, SentCount \= SentCount +1 where Connection_ \= 1 and TestID \= 'ghp04 -count -update -server nulld3e11dbc
-test_duration 900 -delay 799 -concurrent_connections 2' DBProtocolVersion= ClientHostName= 9.70.148.161 DBName= DSN00326 EndUser=SUSHMIT"
Jun 6 00:51:09 gat-daily-vm09 GuardiumSniffer[14912]: subject "SQLGUARD ALERT", "CEF:0|IBM|Guardium|10.0|20000|Alert only|5|rt=1552061999352 cs1=INFO cs1Label=Severity cs2=DB2 cs2Label=Server Type cs3= cs3Label=Classification cat= app=D
B2/Z cs4= cs4Label=DB Protocol Version suser=PLAN=DISTSERV ; SQLID=SUSHMIT ; PROG=SYSLH200 ; DB_NAME=DSN00326 sproc=GHP04.GUARD.SWG.:DB2JCC_APPLI act=SQL_GPB start=1552061999352 externalId=0 duser=SUSHMIT dst=9.70.144.27 dpt=8050 src=9.70
.148.161 spt=14643 proto=DRDA:SERVER msg=UPDATE GDMC_STLAB3E_DB1B set CurrentTime \= '/03/08/19 12:16:14.252', ReconnectCount \= 1, SentCount \= SentCount +1 where Connection_ \= 1 and TestID \= 'ghp04 -count -update -server nulld3e11dbc
-test_duration 900 -delay 799 -concurrent_connections 2' DBProtocolVersion= ClientHostName= 9.70.148.161 DBName= DSN00326 EndUser=SUSHMIT"
```


Implementation considerations: Mapping values for IMS

For IMS users on z/OS, the following new variables are populated in the Alert Message template:

%%DBUser

%%OSUser

%%DBName

%%lastError

%%SQLNoValue: The following values are new availables

- prog=;
- job=;
- step=;
- tran=;
- job#=

Implementation considerations: Mapping values for DB2 z/OS

For DB2 users on z/OS, the following new values are populated in the Alert Message template:

%%DBProtocolVersion

%%clientHostName

%%DBName

%%EndUser

Implementation considerations: Configuration

Enabling the client host name variable for alert messages in DB2 z/OS

For DB2 z/OS systems only, cli commands have been added to enable using the client IP address as the host name for alert messages. When enabled, the %%clientHostName variable displays the host IP address.

CLI commands:

```
store sniff_db2z_alert_use_client_ip_for_host_name [on|off]
```

```
show sniff_db2z_alert_use_client_ip_for_host_name
```

Implementation considerations: Limitations/Constraints

For DB2 z/OS system

%%clientHostname -- If the "store snif_db2z_alert_use_client_ip_for_host_name" CLI command is set to *on*, then %%clientHostname stores the client IP address.

%%DBProtocolVersion -- It is populated only if S-TAP version supports the DB Protocol Version parameter.

%%EndUser -- Available for DB2 z/OS systems only. %%EndUser is either: 1.)The DB2 application user.
2.)The CICS user ID, if the z/OS Collector Agent is configured to collect the CICSUserID. For other databases, %%EndUser is blank.

For IMS z/OS system

%%OSUser -- The %%OSUser is the same as the %%DBUser.

%%SQLNoValue -- The following values are available, similar to the %%SQLString values: prog=; job=; step=; tran=; job#=.

Guardium V11 New Release Training

—

Guardium Data Streams

Overview

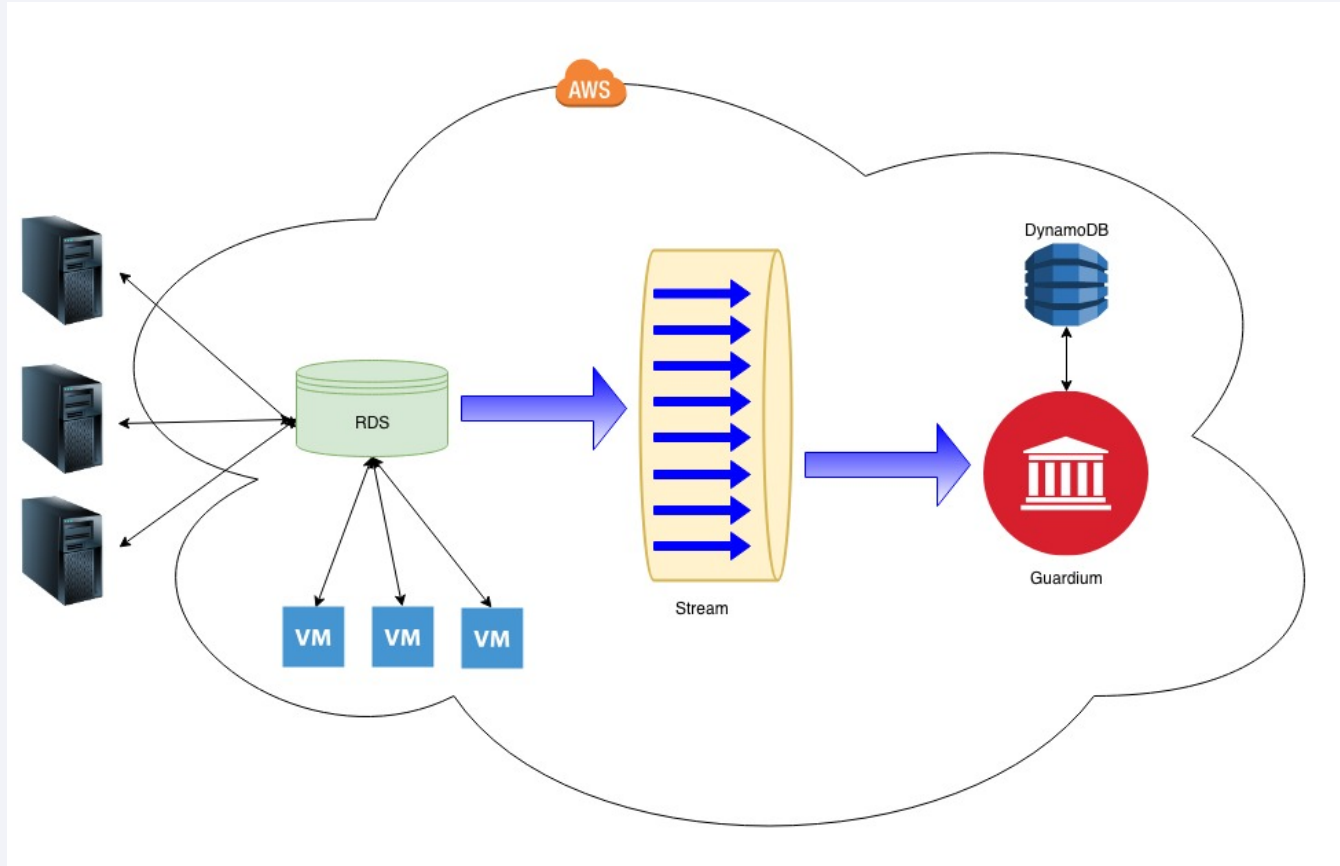
Guardium Data-Streams was created to enable Guardium users to audit cloud databases.

This first release supports RDS on AWS.

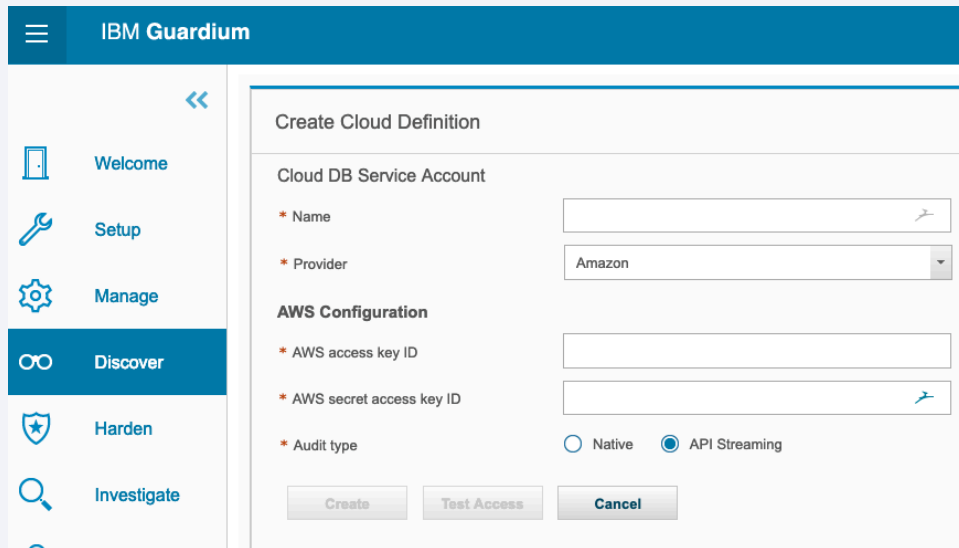
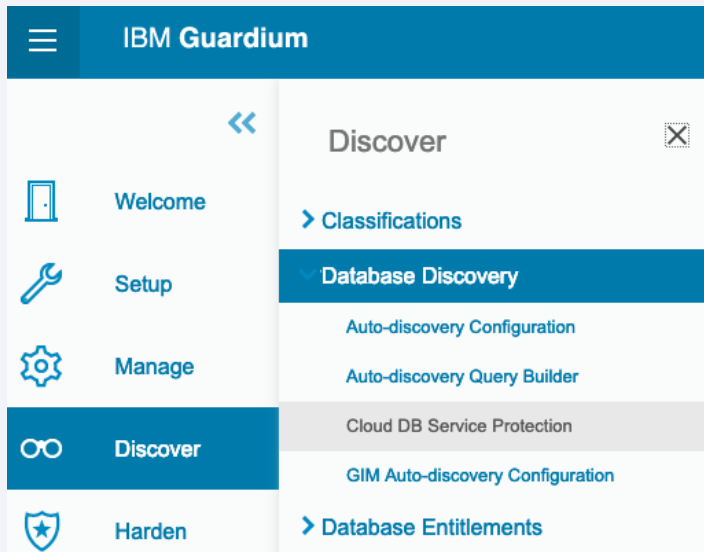
For basic key concepts on what a streaming service is (AWS Kinesis), please use this link:

<https://docs.aws.amazon.com/streams/latest/dev/key-concepts.html>

Architecture



Demo - Create a new Cloud definition.



Demo - After adding a Cloud DB service account, the next step is to discover available streams.


Cloud DB Service Accounts

+

-

Filter



Gils-aws

Cloud DB Service Account 

Name : Gils-aws

Provider : Amazon

Hide Discover Streams

Filter 

<input type="checkbox"/>	Amazon Region	Endpoint
<input type="checkbox"/>	us-gov-west-1	kinesis.us-gov-west-1.amazonaws.com
<input type="checkbox"/>	us-east-1	kinesis.us-east-1.amazonaws.com
<input type="checkbox"/>	us-east-2	kinesis.us-east-2.amazonaws.com
<input type="checkbox"/>	us-west-1	kinesis.us-west-1.amazonaws.com
<input type="checkbox"/>	us-west-2	kinesis.us-west-2.amazonaws.com

Discover

Demo - Next choosing a stream you can enable/assign to collector.

IBM Guardium

16:35

admin admin

Machine Type Standalone

Cloud DB Service Protection

Cloud DB Service Accounts

Gils-aws

Cloud DB Service Account

Name : Gils-aws

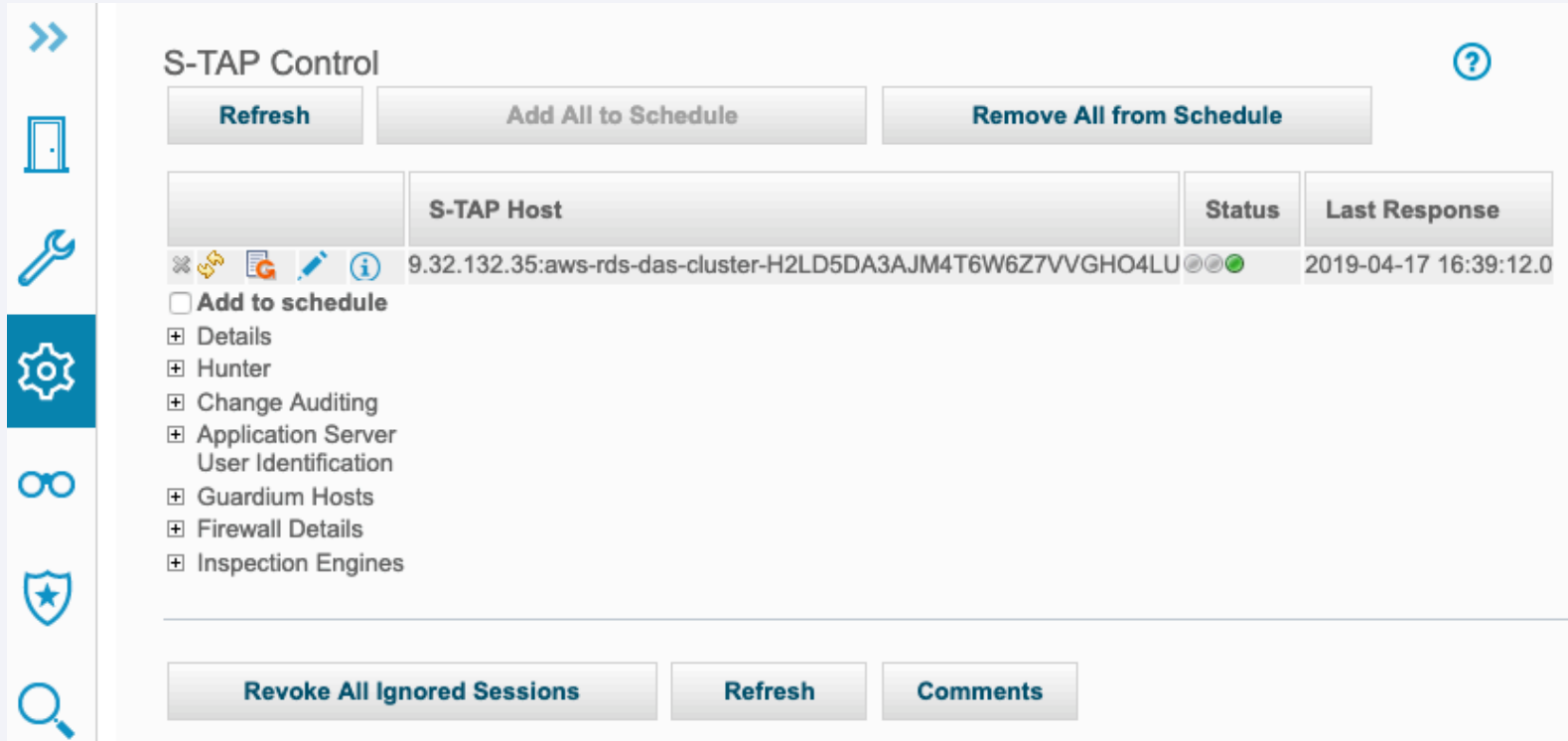
Provider : Amazon

Discover Streams

Streams

Stream	Region	Monitor enabled	Status	Status changed	Comments
aws-rds-das-cluster-3RX4SJSWDYRU75HAFYDM6GFO3Y	us-east-2				
aws-rds-das-cluster-AMKLFDRQWFSIYND7SBXZYSUCRY	us-east-2			2019-03-26 12:35:14	status.comment.stopped
aws-rds-das-cluster-CK23BQD5HHFXRAF43T2NJFHKI	us-east-2				
aws-rds-das-cluster-E3YC7H5JF77JHYZMRQTLYNQNIQ	us-east-2			2019-04-12 18:08:55	status.comment.stopped
aws-rds-das-cluster-H2LD5DA3AJM4T6W6Z7VVGHO4LU	us-east-2			2019-04-17 12:54:43	All Good

Once stream monitoring is enabled an S-TAP host will be created.
Once the stream monitoring is disabled the S-TAP host will be removed.



The screenshot shows the 'S-TAP Control' interface. On the left is a vertical sidebar with icons: a double arrow, a door, a wrench, a gear (selected), glasses, a shield with a star, and a magnifying glass. The main panel has a title 'S-TAP Control' with a help icon. Below the title are three buttons: 'Refresh', 'Add All to Schedule', and 'Remove All from Schedule'. A table follows with columns 'S-TAP Host', 'Status', and 'Last Response'. The table contains one row with the host ID '9.32.132.35:aws-rds-das-cluster-H2LD5DA3AJM4T6W6Z7VVGHO4LU', a status of three green circles, and a timestamp '2019-04-17 16:39:12.0'. To the left of the table is a list of actions: 'Add to schedule' (unchecked), 'Details', 'Hunter', 'Change Auditing', 'Application Server User Identification', 'Guardium Hosts', 'Firewall Details', and 'Inspection Engines'. At the bottom are three buttons: 'Revoke All Ignored Sessions', 'Refresh', and 'Comments'.

S-TAP Control

Refresh **Add All to Schedule** **Remove All from Schedule**

S-TAP Host	Status	Last Response
9.32.132.35:aws-rds-das-cluster-H2LD5DA3AJM4T6W6Z7VVGHO4LU		2019-04-17 16:39:12.0

☐ **Add to schedule**

- ☐ Details
- ☐ Hunter
- ☐ Change Auditing
- ☐ Application Server User Identification
- ☐ Guardium Hosts
- ☐ Firewall Details
- ☐ Inspection Engines

Revoke All Ignored Sessions **Refresh** **Comments**

CLI

Start / stop / restart the datastreams service:

start datastreams

stop datastreams

restart datastreams

To turn on/off log debug messages:

support store datastreams_diag on

support store datastreams_diag off

Datastreams logs are in: /opt/IBM/Guardium/log/datastreams/

Guardium V11 New Release Training

Sniffer Streaming to GBDI

Contents

Overview

Use cases

Architecture

Implementation considerations

Troubleshooting

Q & A

Overview

Sniffer streaming to GBDI

Directly stream audit data from Guardium collector to GBDI.

What's New

- Sniffer streams selected audit data in json document format
- Store audit data in GBDI (Mongo DB) instead of MySQL tables
- Same sniffer binary can be configured to either streaming or traditional logging.
- CLI commands provided for configuration and troubleshooting.

Benefits

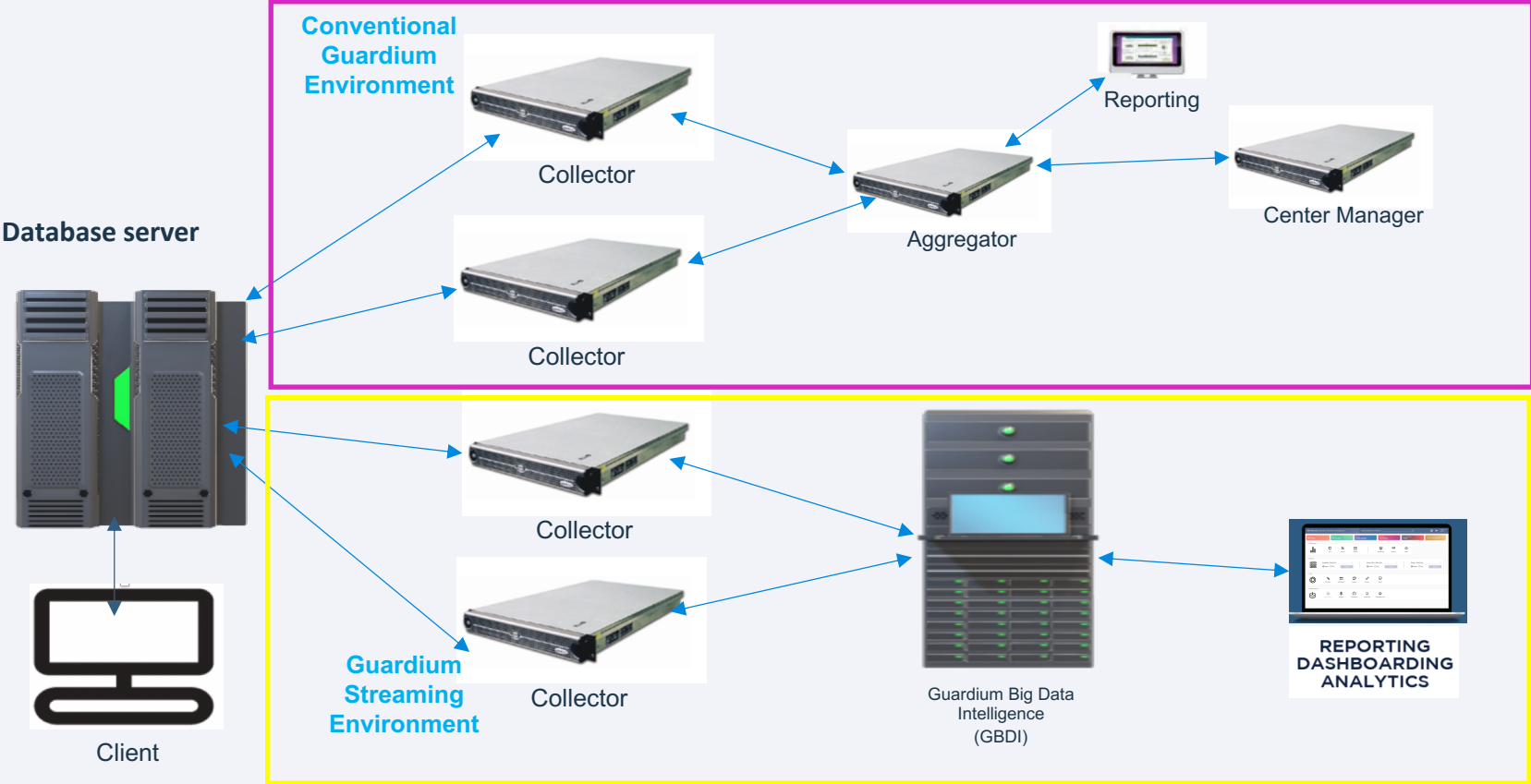
- Stores collected data over longer timeframes in GBDI
- Provides direct, near real-time access to data security and compliance reports and insights.

Use Cases

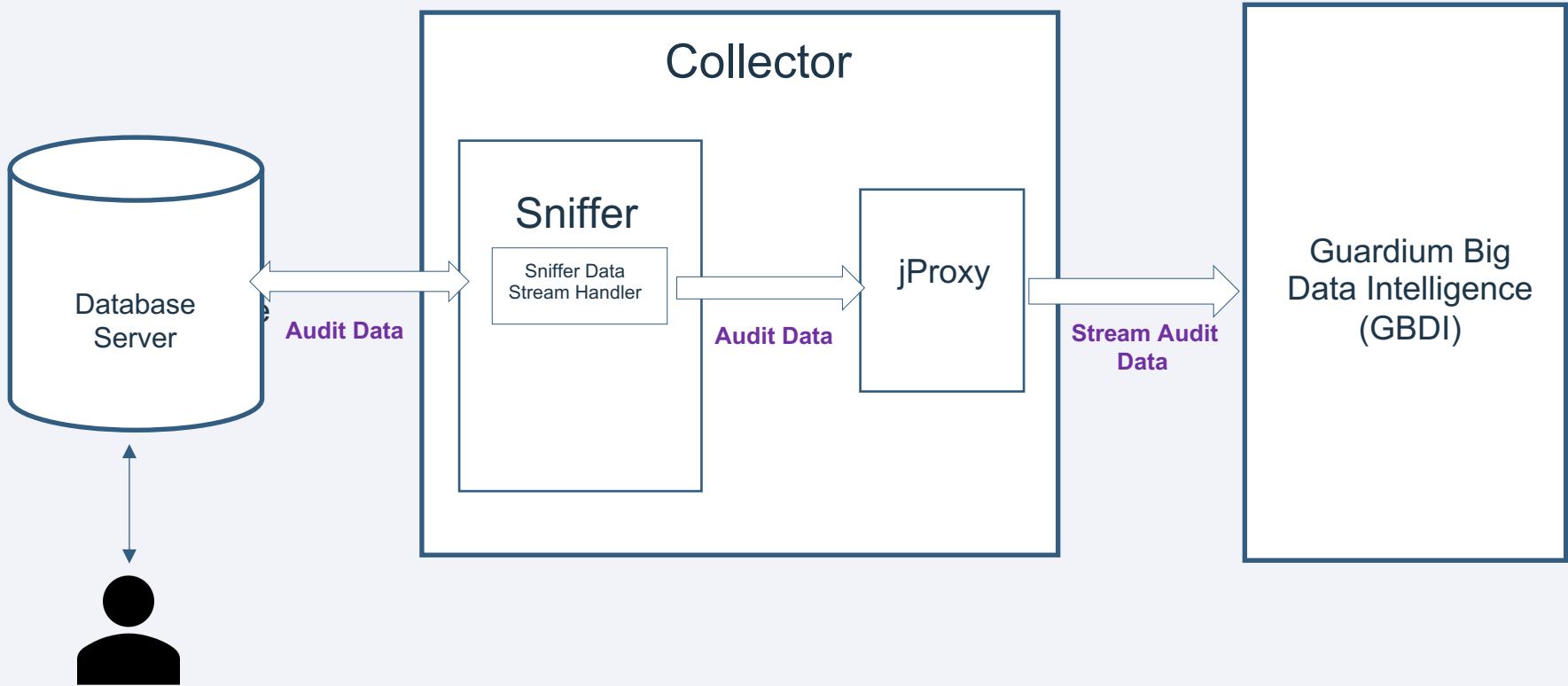
Situations when a user would use the new feature

- Use Case 1: Customers currently using GBDI with DataMart can reconfigure the Guardium collector to directly stream audit data to GBDI
- Use Case 2: Existing Guardium customers can easily convert the appliances to start streaming to GBDI with each configuration.

Architecture



High-Level Architecture with GBDI



Sniffer Data Stream Handler

- Data Stream Handler is a new sub-component in sniffer for data streaming to GBDI
- Handles the specific tasks for streaming:
 - Generate json documents for monitored traffic event
 - Send the json documents to GBDI
 - Update the field values in json documents for session and event responses and statuses.

Jproxy

- jProxy is a connector to GBDI that initiates and maintains connection from Guardium sniffer appliance to GBDI.
- jProxy is a single RPM package installed on Guardium collector
- Provide three system services:
 - **Sonarjproxycd**: Act as a light-weight MongoDB server with some customized functionalities for GBDI.
 - **Jproxyforwarder**: Retrieve the data from local storage and forward to GBDI and clean up forwarded documents from the appliance.
 - **Jproxytimer**: Control jproxyforwarder service timing configuration - start and interval of flushing the data.
- Sniffer communicates with jProxy directly on the local appliance, but jProxy communicates with the remote GBDI.
- jProxy has three configuration files:
 - jproxy.conf - parameters to control the sonarjproxycd service
 - jproxyforwarder.env - parameters to control the jproxyforwarder service
 - logging.conf - settings to control the Log file and log level of jproxy
- The settings in configuration files can be updated by CLI commands.
- jProxy will have its own patch separated from sniffer patching when required.

Data Collections for GBDI

- Session
- Instance
- Full_SQL
- Policy_Violations
- Exception

Session Collection (I)

- Includes the data fields from both GDM_ACCESS and GDM_SESSION table

```
> db.session.findOne()
{
  "_id" : "548995000000000084",
  "Server Type" : "ORACLE",
  "Server OS" : "X86_64/LINUX 2.4.XX",
  "Client OS" : "JAVA_TTC-8.2.0",
  "Server IP" : "9.70.144.184",
  "Analyzed Client IP" : "9.70.144.184",
  "Network Protocol" : "TCP",
  "DB Protocol" : "TNS",
  "DB Protocol Version" : "3.15",
  "DB User Name" : "C##SCOTT",
  "OS User" : "ROOT",
  "Source Program" : "JDBC THIN CLIENT",
  "Client Mac" : null,
  "Client Host Name" : "REDWOOD.GUARD.SWG.USMA.IBM.COM",
  "Server Host Name" : "REDWOOD.GUARD.SWG.USMA.IBM.COM",
  "Server Description" : null,
  "Service Name" : "ON2CREDW",
  "Encryption type" : null,
  "Key Value" : null,
  "IPv6 Flag" : false,
  "Database Name" : "ON2CREDW@ON2CREDW",
  "Client Port" : "16433",
  "Server Port" : "1522",
  "SonarG Source" : "sgss-vc3a-vm03",
  "UTC Offset" : -5,
  "Old Session Id" : "0",
  "Session Start" : ISODate("2019-01-31T21:35:06Z"),
  "Session End" : ISODate("2019-01-31T21:35:06.264Z"),
  "TTL" : NumberLong(0),
  "Session Info" : "0 1 1 178 4 14 4 0",
  "Inactive Flag" : 1,
  "Session Ignored" : "No",
  "Ignored Since" : null,
  "Uid Chain" : null,
  "Uid Chain Compressed" : null,
  "Failover Flag" : false,
  "Failover Timestamp" : null,
  "Mills" : NumberLong("1548970496075"),
  "Required UID Chain from Parent" : false,
  "Login Succeeded" : 0,
  "Sender IP" : "9.70.144.184",
  "Session Key" : NumberLong(2032865344),
  "Caller ID" : 2,
  "Inspection Engine ID" : NumberLong("2256911290"),
  "Char Encoding" : "CP1252",
  "Tap Identifier" : "ORACLE_9.70.144.184(1522,1522,DB_6)",
  "Priority_Queue_Status" : 2
}
```

Session Collection (II)

- Session information is logged both locally in MySQL and streamed to GBDI, for live session lookup and recovery in sniffer
- Session ID generated by the local MySQL on each collector is globally unique since v10
- The same mysql-generated session ID is used as the unique session_id in the session json document for GBDI.

```
mysql> select SESSION_ID,SESSION_KEY from GDM_SESSION where SESSION_ID='973290000000008398';
```

SESSION_ID	SESSION_KEY
973290000000008398	1009610368

```
> db.session.findOne({'_id': '973290000000008398'},{'_id':1, "SonarG Source":1, "Session Key":1})
{
  "id" : "973290000000008398",
  "Session Key" : NumberLong(1009610368),
  "SonarG Source" : "sgss-vc3a-vm03"
}
```

Instance Collection

- Information about the common audit data of the sql instance
- Including the common session data, instance period start/end, construct_id, original_sql, objects and verbs, etc.

```
> db.instance.findOne({"Session Id": "973290000000008398"})
{
  "_id" : "1893956363537213803",
  "Session Id" : "973290000000008398",
  "Server Type" : "ORACLE",
  "Server OS" : "X86_64/LINUX 2.4.XX",
  "Client OS" : "JAVA TTC-8.2.0",
  "Server IP" : "9.70.165.166",
  "Analyzed Client IP" : "9.70.165.166",
  "Network Protocol" : "TCP",
  "DB Protocol" : "TNS",
  "DB Protocol Version" : "3.17",
  "DB User Name" : "C##SCOTT",
  "OS User" : "ROOT",
  "Source Program" : "JDBC THIN CLIENT",
  "Client Mac" : null,
  "Client Host Name" : "SNIF-RH7DB01.GUARD.SWG.USMA.IBM.COM",
  "Server Host Name" : "SNIF-RH7DB01.GUARD.SWG.USMA.IBM.COM",
  "Server Description" : null,
  "Service Name" : "ON8CSNIF",
  "Encryption Type" : null,
  "Key Value" : null,
  "IPV6 Flag" : false,
  "Database Name" : "ON8CSNIF@ON8CSNIF",
  "Client Port" : "45864",
  "Server Port" : "1522",
  "SonarG Source" : "sgss-vc3a-vm03",
  "UTC Offset" : -4,
  "Period Start" : ISODate("2019-03-23T03:00:00Z"),
  "Period End" : ISODate("2019-03-23T03:59:59Z"),
  "Application Event ID" : NumberLong(0),
  "App User Name" : null,
  "Application Event Type" : null,
  "Application Event Value Str" : null,
  "Application Event Value Num" : null,
  "Application Event Date" : null,
  "Construct Id" : "e781ed68d69e4a19de987b95303630f2a426bfb0",
  "Original SQL" : "select * from scrub_luhn_test where card_id=?",
  "Objects and Verbs" : "scrub_luhn_test select",
  "Average Execution Time" : 1
}
```


Full_SQL Collection

- Equivalent to data in GDM_CONSTRUCT_TEXT table.
- A full SQL document may contain:
 - Masked or unmasked SQL based on rule action
 - Prepare statement and bind variable value
 - Return data and return data count for extrusion rule
- Sniffer generates the unique identifier for each full SQL json document
- The unique full_sql identifier is used to update the SQL response data GBDI.

Full_SQL document example

- Example of one full_sql document for extrusion rule, with masked returned data.
- Information about the individual sql event
- Only available when rule actions such as log full sql details are triggered

```
db.full_sql.findOne({"Session Id": "973290000000008398"})
{
  "id" : "17117201512242859794",
  "Session Id" : "973290000000008398",
  "Server Type" : "ORACLE",
  "Server OS" : "X86_64/LINUX 2.4.XX",
  "Client OS" : "JAVA TTC-8.2.0",
  "Server IP" : "9.70.165.166",
  "Analyzed Client IP" : "9.70.165.166",
  "Network Protocol" : "TCP",
  "DB Protocol" : "TNS",
  "DB Protocol Version" : "3.17",
  "DB User Name" : "C##SCOTT",
  "OS User" : "ROOT",
  "Source Program" : "JDBC THIN CLIENT",
  "Client Mac" : null,
  "Client Host Name" : "SNIF-RH7DB01.GUARD.SWG.USMA.IBM.COM",
  "Server Host Name" : "SNIF-RH7DB01.GUARD.SWG.USMA.IBM.COM",
  "Server Description" : null,
  "Service Name" : "ON8CSNIF",
  "Encryption Type" : null,
  "Key Value" : null,
  "IPV6 Flag" : false,
  "Database Name" : "ON8CSNIF@ON8CSNIF",
  "Client Port" : "45864",
  "Server Port" : "1522",
  "SonarG Source" : "sgss-vc3a-vm03",
  "UTC Offset" : -4,
  "Instance ID" : "1893956363537213803",
  "Access Rule Description" : "extrusion_creditcard",
  "Full SQL" : "select * from scrub_luhn_test where card_id=1010",
  "Statement Type" : 0,
  "Bind Variable Values" : null,
  "Prepared statement ID" : -1,
  "Timestamp" : ISODate("2019-03-23T03:16:14.483Z"),
  "Returned Data" : "#####0939",
  "Returned Data Count" : 1,
  "Total Records Affected" : -1,
  "Succeeded" : 1,
  "Status" : 1,
  "Response Time" : 0,
  "ACK Response Time" : 0
}
```

Policy_Violations Collection

- Equivalent to data as in GDM_POLICY_VIOLATIONS_LOG table.
- A policy violation streaming message is sent when a SQL statement is considered as a violation of any installed policy rules
- One policy violation message for each SQL construct violation
- SQL string in policy violation document can be full SQL or masked SQL based on violated policy rules .
- Sniffer generates the unique identifier for each violation message
- This unique policy identifier is cross-referenced in Guardium alerts when the alert template variable %%ViolationID is configured in the alert message template

Policy_Violations document example

```
> db.policy_violations.findOne()
{
  "id" : "8040646097614785938",
  "Session Id" : "58526600000027784",
  "Server Type" : "ORACLE",
  "Server OS" : "X86_64/LINUX 2.4.XX",
  "Client OS" : "JAVA_TTC-8.2.0",
  "Server IP" : "9.70.165.166",
  "Analyzed Client IP" : "9.70.165.166",
  "Network Protocol" : "TCP",
  "DB Protocol" : "TNS",
  "DB Protocol Version" : "3.17",
  "DB User Name" : "C##SCOTT",
  "OS User" : "ROOT",
  "Source Program" : "JDBC THIN CLIENT",
  "Client Mac" : null,
  "Client Host Name" : "SNIF-RH7DB01.GUARD.SWG.USMA.IBM.COM",
  "Server Host Name" : "SNIF-RH7DB01.GUARD.SWG.USMA.IBM.COM",
  "Server Description" : null,
  "Service Name" : "ON8CSNIF",
  "Encryption Type" : null,
  "Key Value" : null,
  "IPv6 Flag" : false,
  "Database Name" : "ON8CSNIF@ON8CSNIF",
  "Client Port" : "54992",
  "Server Port" : "1522",
  "SonarG Source" : "sgss-vc3a-vm04",
  "UTC Offset" : -4,
  "Construct ID" : "c0bde0812381f36400fb0771ece7a02962a5b1dd",
  "Objects and Verbs" : "count, GDMC_on8csnif_rh7db01 select",
  "App User Name" : null,
  "Access Rule ID" : NumberLong(20005),
  "Access Rule Description" : "SQL_ERROR",
  "Verdict" : NumberLong(8),
  "Full SQL" : "select count(*) from GDMC_on8csnif_rh7db01 where XXX298093211_576 = 298.0",
  "Send Message" : NumberLong(0),
  "Current Counter" : NumberLong(1),
  "Key String" : null,
  "Category Name" : null,
  "Classification Name" : null,
  "Severity" : NumberLong(0),
  "Policy Description" : null,
  "Policy String" : null
}
```

Exception Collection

- With GBDI, all sniffer-processed (handled) exceptions and errors are streamed to one exception collection; With MySQL, different types of exceptions may be configured to log into GDM_EXCEPTION or GDM_ERROR tables.
- Other exceptions or errors generated by the internal non-snif processes on collector (e.g. GUI) continue to be logged in GDM_EXCEPTION table.
- SQL strings in the exception document can be full SQL or masked SQL according to policy rules.
- The identifier of the exception streaming document is automatically generated by the Mongo Database for GBDI.

Exception Collection Example

```
> db.exception.findOne()
{
  "_id" : ObjectId("5ca212f43fbc7a24eb549af4"),
  "Exception Type ID" : "SQL_ERROR",
  "Exception Description" : "TDS_SYB-207-16-4",
  "SQL string that caused the Exception" : "select count(*) from GDMC_ssn6snifr_snif_rh7db01 where XXX166093209_715 = 166.0",
  "Error Cause" : null,
  "Count" : 1,
  "Exception Timestamp" : ISODate("2019-04-01T13:32:35.359Z"),
  "Session Id" : "585266000000027777",
  "Server Type" : "SYBASE",
  "Server OS" : "",
  "Client OS" : "",
  "Server IP" : "9.70.165.166",
  "Analyzed Client IP" : "9.70.165.166",
  "Network Protocol" : "TCP",
  "DB Protocol" : "TDS",
  "DB Protocol Version" : "5.0",
  "DB User Name" : "SA",
  "OS User" : "",
  "Source Program" : "JCONNECT 0.6.0.0",
  "Client Mac" : null,
  "Client Host Name" : "SNIF-RH7DB01.GUARD.SWG.USMA.IB",
  "Server Host Name" : "SNIF-RH7DB01.GUARD.SWG.USMA.IB",
  "Server Description" : "ASE 16.0.3.6",
  "Service Name" : "SN6SNIFR",
  "Encryption Type" : null,
  "Key Value" : null,
  "IPV6 Flag" : false,
  "Database Name" : "GUARDIUM_QA",
  "Client Port" : "33302",
  "Server Port" : "4300",
  "SonarG Source" : "sgss-vc3a-vm04",
  "UTC Offset" : -4
}
```

Other Data on Guardium Appliance

- Other non-streaming data remains in MySQL on collector.
- For examples,
 - All configuration related information
 - Alert related information
 - Schedule information
 - STAPs and other connections
 - Access and Session information
 - Other audit data that GBDI does not support currently.

Implementation considerations: Installation and Migration

- Prerequisites, dependencies:
 - v11.0 collector on RHEL 7
 - GBDI environment: SonarG version 4.0
- Installation: as per standard installation procedures for Guardium v11 and SonarG
- jProxy is a separate RPM automatically installed with Guardium v11 appliance installation
- After successful installation, jproxy user and required directories are created automatically.
- Jproxy System service `sonarjproxyd.service`, `jproxytimer.timer`, `jproxyforwarder.service` are automatically enabled when jProxy rpm installation completes.
- Migration: Existing customers with audit data stored in MySQL can use DataMart to migrate the existing data from MySQL into GBDI.

Implementation considerations: Configuration

- Use Guard parameter `SNIF_LOGGER_DESTINATION_TYPE` to control the sniffer logger destination type.
- Default logger destination is MySQL.
- CLI command:
 - > `store sniff_logger_destination_type`
USAGE: store sniff_logger_destination_type <LOCAL|REMOTE>
LOCAL for local MYSQL database, REMOTE for Mongo database GBDI
- Upload the SSH key file (.pem) to Guardium appliance
 - > `import jproxy_files`
- Configure SSH target host for jproxy to communicate with remote GBDI
 - > `store/show jproxy_config ssh_key_file <uploaded key file name>`

Implementation considerations: Configuration

- Configure logger data destination, data collection(s), Mongo client authentication(username, auth, database, mechanism, etc.)
 - > *store/show logger_data_destination_config type <database type>*
 - > *store/show logger_data_destination_config database_name <db name>*
 - > *store/show logger_data_destination_config destination hostname/port <value>*
 - > *store/show logger_data_destination_config authentication*
username/auth_database_name/mechanism <value>
 - > *store/show logger_data_destination_config data <streaming collection name> on/off*
- Configure how often jProxy should flush data collections (by time or accumulated data size or use the default settings)
 - > *store/show jproxy_config flush_timeout_sec <number of seconds>*
 - > *store/show jproxy_config flush_at_size <number of size>*
- CLI commands to start/stop/restart jproxy services:
 - > *start/stop/restart jproxy* - for sonarjproxyd service
 - > *start/stop/restart jproxytimer* - for jproxytimer.timer service
- Port 27118 is reserved for jProxy by default on collector.

Implementation considerations: Limitations/Constraints

- Limitations:
 - Only 5 enabled data collections available on GBDI. All other data are still stored in MySQL
 - When sniff logger destination is configured for GBDI, the disabled data collections will not be streamed to destination. Such data will be ignored.
 - Session UID_CHAIN information is not updated in GBDI as in MySQL
 - Average_Execution_Time field value is not updated in the instance collection (possible in the future release)
 - Statistics report on sniff-streamed data to GBDI is not available

External S-Tap Enhancements

Guardium 11.0 New Release training

Agenda

- Overview
- Architecture
- Demonstration
- Q&A

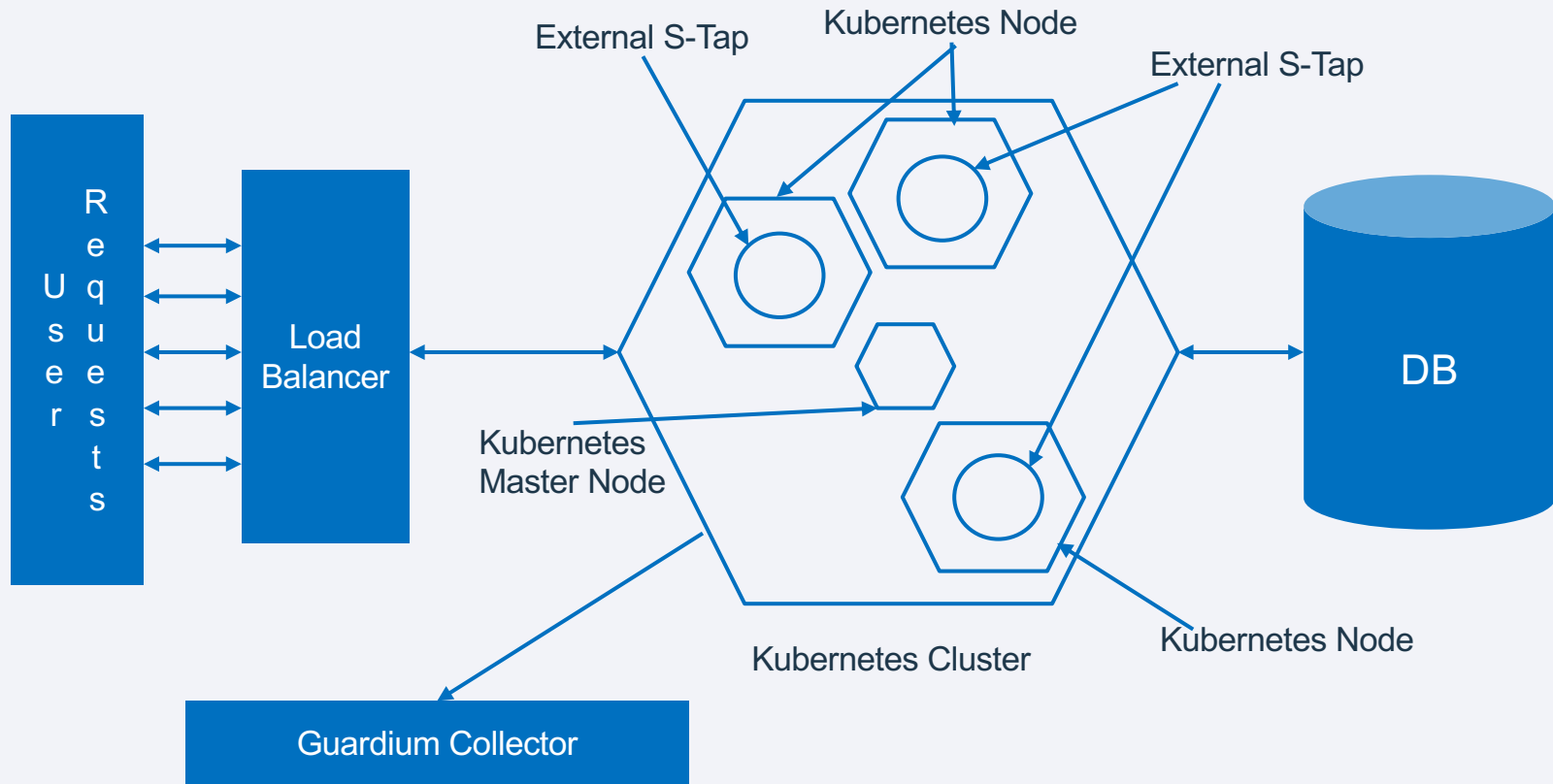
Team Members

- **Architect** – Gali Diamant and Richard Jerrell
- **Developers** – Glenn Weidner and Shraddha Kannav
- **Designer** – Daina Pupons-Wickham
- **Testers** – Jennifer Peng and Ngan Tran
- **ID** – Miriam Lezak
- **Manager** – Krishnaswamy Sundaramurthy

Overview

- **Support for Kubernetes**
 - **AWS**
 - **Azure**
- **UI Driven deployment**

Architecture












Demo

- Deploy External S-TAP using Amazon Elastic Container Service for Kubernetes (Amazon EKS).
- Note similar steps apply if using Microsoft Azure Kubernetes Service (AKS).

Demo


- Click on new  button from External S-TAP Control to deploy with Kubernetes.


External S-TAP instances ?							
    Actions  Export 		Filter 					
External S-TAP group	Group uuid	Host	Database type	Total members	Overall status	Healthy members	Collector
 Oracle_52.36.6.197	eb3d06a5-ea2c-42b5-8d95-66a538f44d22	52.36.6.197	Oracle	2		2	18.236.138.236

Deploy External S-TAP – Kubernetes Tab

	Kubernetes	Docker	Database	Guardium	Advanced
Cloud provider	<i>Select Kubernetes service provider</i>				
* Master URL	<i>Kubernetes cluster master URL</i>				
* Token	<i>Kubernetes cluster access token</i>				
* Deployment name	<i>Kubernetes deployment identifier</i>				

Deploy External S-TAP – Docker Tab

 Kubernetes

 **Docker**

Database

Guardium

Advanced

* Registry key

Kubernetes secret name for credentials

Image

* Location


store/ibmcorp/guardium_external_s-tap


* Tag

Tag for selecting image version

3
0

Deploy External S-TAP – Database Tab

 Kubernetes

 Docker

Database

Guardium

Advanced

Database type

Select type of database

Database port

Database port number


Database host


Database host name or IP address


Demo


External S-TAP instances ?								
<div><div><div>+</div><div></div><div>−</div><div></div></div><div>Actions</div><div>Export</div></div>			Filter					
	External S-TAP group	Group uuid	Host	Database type	Total members	Overall status	Healthy members	Collector
	Oracle_52.36.6.197	eb3d06a5-ea2c-42b5-8d95-66a538f44d22	52.36.6.197	Oracle	2	<div></div>	2	18.236.138.236
	Oracle_34.222.42.193	faf23fd7-0eae-4319-9085-1100c28e5e82	34.222.42.193	Oracle	2	<div></div>	2	18.236.138.236

Demo

 **kubernetes**



 Search

[+ CREATE](#) | 


 [Workloads](#) > [Deployments](#)


Workloads
[Cron Jobs](#)
[Daemon Sets](#)
[Deployments](#)
[Jobs](#)

Deployments


Name	Labels	Pods	Age	Images	
 training-demo	app: training-demo	2 / 2	a day	gweidner/test-private:gproxy-v11.f	

Demo

 **kubernetes**

 Search

+ CREATE





☰

Workloads > Replica Sets > training-demo-789895b966

☰ LOGS

⋮ SCALE

 EDIT

 DELETE

Cron Jobs

Daemon Sets



Deployments

Jobs

Pods

Replica Sets


Pods

Name	Node	Status	Restarts	Age	
 training-demo-789895b966-c24dp	ip-172-20-37-190.us-west-2.compute.internal	Running	0	a day	<div><div></div><div></div></div>
 training-demo-789895b966-fzgv9	ip-172-20-32-99.us-west-2.compute.internal	Running	0	a day	<div><div></div><div></div></div>


3

0

Demo

 **kubernetes**

Search

+ CREATE | 

≡ Shell

Cluster

Namespaces

Nodes

Persistent Volumes


Roles

Storage Classes


Shell in training-demo ▾ in training-demo-789895b966-c24dp

```
[root@training-demo-789895b966-c24dp build]# ps -ef | grep stap
root      16      1  0 19:30 ?        00:00:03 /usr/local/guardium/guard_stap/guard_stap /usr/local/guardium/guard_stap/guard
tap.ini
[root@training-demo-789895b966-c24dp build]#
[root@training-demo-789895b966-c24dp build]# ps -ef | grep proxy
root       7      1  0 19:30 ?        00:00:00 /usr/sbin/gproxyd
root       8      1  0 19:30 ?        00:00:00 /bin/bash /usr/sbin/gproxy_http_live
[root@training-demo-789895b966-c24dp build]#
```

Demo

 **kubernetes**

Search


+ CREATE | 

Discovery and load balancing > **Services**


Workloads


- Cron Jobs
- Daemon Sets
- Deployments
- Jobs


Services


Name	Labels	Cluster IP	Internal endpoints	External endpoints	Age
 training-demo	app: training-demo	100.66.94.201	training-demo:1521 TCP training-demo:32691 TCP	aec7d216c8eda11e9b4d7	a day


Demo

 **kubernetes**

 Search

[+ CREATE](#) | 

 [Discovery and load balancing](#) > [Services](#) > **training-demo**

 [EDIT](#)  [DELETE](#)

Workloads

Cron Jobs


Daemon Sets

Deployments

Connection

Cluster IP: 100.66.94.201

Internal endpoints: training-demo:1521 TCP
training-demo:32691 TCP

External endpoints: [aec7d216c8eda11e9b4d7027c457f5f6-7d0897c7c14e9a39.elb.us-west-2.amazonaws.com:1521](#) 

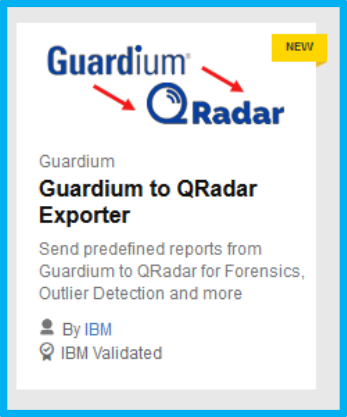
Events

Message	Source	Sub-object	Count	First seen	Last seen
Successfully assigned training-demo-789895b966-c24dp to ip-172-20-37-190.us-west-2.compute.internal	default-scheduler	-	1	2019-06-14T19:30 UTC	2019-06-14T19:30 UTC
MountVolume.SetUp succeeded for volume "dshm"	kubelet ip-172-20-37-190.us-west-2.compute.internal	-	1	2019-06-14T19:30 UTC	2019-06-14T19:30 UTC
MountVolume.SetUp succeeded for volume "default-token-s6qvv"	kubelet ip-172-20-37-190.us-west-2.compute.internal	-	1	2019-06-14T19:30 UTC	2019-06-14T19:30 UTC
pulling image "gweidner/test-private:gpu-v11.0.0.92"	kubelet ip-172-20-37-190.us-west-2.compute.internal	spec.containers(training-demo)	1	2019-06-14T19:30 UTC	2019-06-14T19:30 UTC
Successfully pulled image "gweidner/test-private:gpu-v11.0.0.92"	kubelet ip-172-20-37-190.us-west-2.compute.internal	spec.containers(training-demo)	1	2019-06-14T19:30 UTC	2019-06-14T19:30 UTC
Created container	kubelet ip-172-20-37-190.us-west-2.compute.internal	spec.containers(training-demo)	1	2019-06-14T19:30 UTC	2019-06-14T19:30 UTC
Started container	kubelet ip-172-20-37-190.us-west-2.compute.internal	spec.containers(training-demo)	1	2019-06-14T19:30 UTC	2019-06-14T19:30 UTC

New QRadar app integration in App Exchange

IBM and Business Partner Applications (15)


Items Per Page 8 Sort By Newest



Guardium to QRadar Exporter

Send predefined reports from Guardium to QRadar for Forensics, Outlier Detection and more

By IBM
IBM Validated

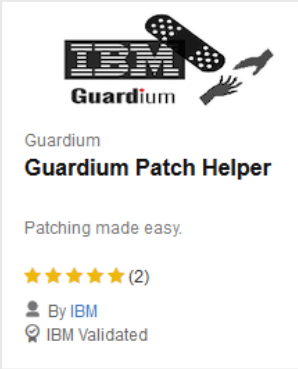


Guardium GN Tools

Toolkit for Guardium Administrators

★★★★★ (2)

By Guardium Notes Blog
IBM Validated

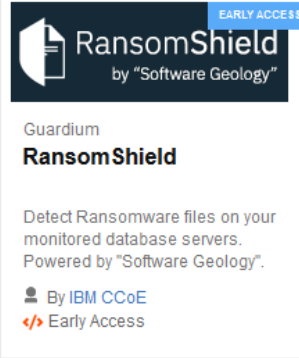


Guardium Patch Helper

Patching made easy.

★★★★★ (2)


By IBM
IBM Validated



RansomShield

Detect Ransomware files on your monitored database servers. Powered by "Software Geology".

By IBM CCoE
Early Access

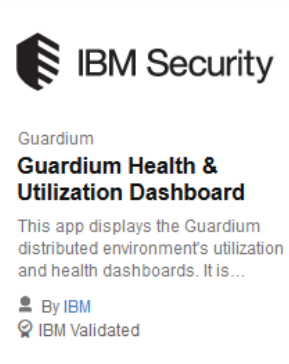


leadcomm
performance and security

Enhanced Report Viewer for Guardium

Experience Guardium reports the "right way" with our exclusive enhanced reporting capabilities.

By LEADCOMM
IBM Validated

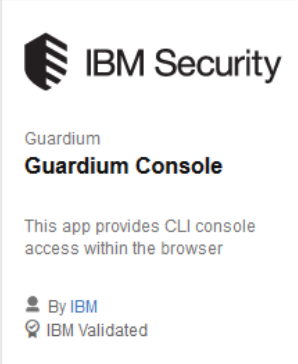


IBM Security

Guardium Health & Utilization Dashboard

This app displays the Guardium distributed environment's utilization and health dashboards. It is...

By IBM
IBM Validated

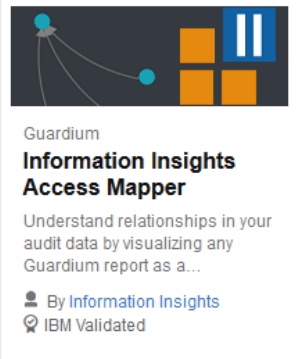


IBM Security

Guardium Console

This app provides CLI console access within the browser

By IBM
IBM Validated



Guardium

Information Insights Access Mapper

Understand relationships in your audit data by visualizing any Guardium report as a...

By Information Insights
IBM Validated

IBM Security / ©

1/2

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

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

IBM Security



