GDP - DB2 Run-through

Thursday, August 7, 2025 7:26 AM

Review and join

Event details

Name	Start time	Duration	Level
IBM Guardium Data Protect and DB2 on AWS event	8/06/2025 10:18 AM	72 hours	200

Description
Test event for content IBM Guardium Data Protect and DB2 on AWS

Terms and Conditions

Read and accept before joining the event:

1. By using AWS Workshop Studio for the relevant event, You agree to the AWS Event Terms and Conditions, the AWS Responsible AI Policy, and the AWS Acceptable Use Policy.
2. If You are under 18 years old, you may participate in the relevant event using AWS Workshop Studio: (a) if You are at least the minimum age below based on the country or region in which You reside, and (b) with the involvement of a parent, guardian, or educator.

Country or region	Minimum age
All countries or regions not listed below (including the United States, Brazil, the United Kingdom, and India)	13
Canada, China, Republic of Korea (South Korea)	14
Australia	15
Japan, Switzerland, Vietnam, and countries in the European Economic Area	16
Azerbaijan, Bolivia, Colombia, Dominican Republic, Indonesia, Lebanon, Malaysia, Mexico, Montenegro, Nepal, Philippines, Thailand, Turkey, and countries in Africa	18

3. You acknowledge and agree that You are using an AWS-owned account that You will only be able to access during the relevant event. You have no ownership rights over this AWS-owned account.
4. During the relevant event, while using this AWS-owned account, You will not use, import, input, or introduce any data, dataset, or other material that contains personal data, financial information, or any other data or materials that may be subject to laws and regulations (such as the General Data Protection Regulation or The Health Insurance Portability and Accountability Act of 1996).
5. If You find residual resources or materials in this AWS-owned account, You will notify your Event Operator immediately.
6. AWS, its affiliates, and any entities or persons acting on AWS's behalf reserves the right to terminate this AWS-owned account and to delete its contents at any time, without any notice to You.
7. During the relevant event, while using this AWS-owned account, You will not process or run any operation on any data other than test datasets or lab materials that have been approved by AWS.
8. You will not copy, import, export or otherwise create derivative works of materials provided by AWS for use outside of the relevant event.
9. AWS, its affiliates, and any entities or persons acting on AWS's behalf have no obligation to enable the transmission of Your materials through AWS Workshop Studio, and may, in their discretion, edit, block, refuse to post, or remove Your materials at any time, without notice to You.
10. If You access and use a service and/or third-party models that have their own terms during the relevant event, while in the AWS-owned account, You agree to review those terms and comply with them during the event.
11. If You are an AWS Partner using AWS Workshop Studio as part of Your participation in the AWS Partner Network Program, Your use of AWS Workshop Studio is governed by these terms, the AWS Partner Network Terms and Conditions, and the AWS Customer Agreement or other agreement with us governing your use of AWS Services.
12. Your use of AWS Workshop Studio will comply with these terms and all applicable laws. If You fail to comply with any of these terms, Your access to AWS Workshop Studio may be immediately terminated, without notice to You.

☐ I agree with the Terms and Conditions

Event dashboard > Guardium Data Protect on AWS

IBM Guardium Data Protect and DB2 on AWS event

Event information

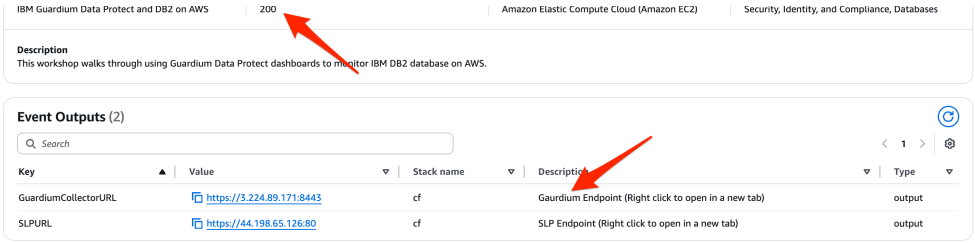
Start time	Duration	Accessible regions
8/06/2025 10:18 AM	72 hours	us-east-1

Description
Test event for content IBM Guardium Data Protect and DB2 on AWS

Workshop

Get started >

Title	Complexity level	AWS services	Topics



1-2 min wrap-up.
Talk about AWS and

1.4. Access Control & Policy Enforcement

Enforce fine-grained access policies, segregate duties, and monitor privileged user activities.

"segregation" or "**separation"** of duties.

1.7. Integration and Automation

Guardium integrates seamlessly with enterprise security infrastructure:

Examples? Or change the ":" to "."
OR should 1.8, 1.9 and 1.10 just be sub items of 1.7?

Getting started

IBM Guardium 12 – Getting started

There are two servers set up in a VPC configuration for this workshop. One server has Guardium Data Protect (GDP) deployed on it. The other server has DB2 community edition installed on it, as well as an opensource tool called Scenario Launch Platform (SLP), that you can read more about here: [https://github.com/IBM/CyberSkill/tree/main/ScenarioLaunchPlatform] should you wish.

The DB2 community edition is pre wired to the GDP instance deployed in the VPC. The SLP tool is used to generate traffic on the DB2 community edition that GDP will report, and has been preset with all the connection and schema information necessary to run the workshop.

You can log into the workshops Guardium Data Protect by accessing this URL [GDP_URL]
You can log into the workshops Scenario Launch Platform by accessing this URL [SLP_URL]

You will use both of these URLs during this workshop. You should not need to log into the servers themselves, however - details of how to do that should you wish are included in the closing section of the workshop.

Step 2

This will bring you to a licence page. The GDP instance has been pre wired to the DB2 server, however the licence needs to be added in order for the two services to speak to each other. Your 90 day trial licence was sent to you when you signed up to the workshop. There are infact two licences that must be added. Start by copying and pasting the first licence key and clicking apply.

Specify they must add the base license key first and then add the append license key. You can't add the append license key first.

Do we want to address or speak to the certificate error and the updates available messages that are shown. Maybe say they can be ignored etc?

Data Discovery and VA

1. Data Discovery & Classification (Discover and Classify)

Core Purpose: Establish visibility into where sensitive or regulated data resides—across structured databases and unstructured data (files, flat files, etc.) in on-prem and cloud environments .

Supported Platforms: Covers major environments such as AWS RDS (MySQL, PostgreSQL, SQL Server, Oracle), MongoDB, IBM Db2 (Linux/UNIX/Windows, z/OS, i), Informix, SAP HANA, Teradata, Netezza, FTP/SMB/HTTP repositories, and more.

Add link to data source page? https://ibm.github.io/guardium-supported-datasources/

1.2 Rule Builder Tools: Use either:

- End-to-end wizard brings a simplified and quicker setup)
- Full Classification Policy Builder gives increased flexibility. Helping to define sources, rules, scheduling, actions.

Format.
Rogue ")"

2. Vulnerability Assessment (Guardium VA)

- Overview: Designed to assess security posture of data environments by identifying infrastructure and configuration vulnerabilities, and guiding remediation efforts
- Deployment Options: Available as part of Guardium Data Protection suite or as a standalone module for purely infrastructure scanning use cases
- Key Capabilities: ** Scans databases, data warehouses and big-data environments. ** Tests for weaknesses such as missing patches, weak credentials, excessive privileges, unauthorized schema changes, and behavioral anomalies (e.g. unusual logins, account sharing) ** Relies on benchmarks such as CIS, STIG, SCAP, and IBM-maintained rule sets ** Supports behavior-based indicators (e.g. after-hours activity, privilege anomalies) ** Broader platform support ** UI and performance improvements, expanded CIS/STIG coverage and improved scalability ** Credentialed, read-only scans (minimal load on systems) ** Produce detailed reports: risk scores, benchmark violations, remediation steps ** Provide dashboards tracking risk posture. ** Automate compliance reporting for standards like PCI DSS, HIPAA, SOX

Can formatting of this be better?

"Broad"

2.1 Synergy Between Discovery & VA

Guardium Discover and Classify equips VA with precise knowledge of where sensitive data resides, allowing prioritized vulnerability scanning on high-risk assets.

Combined, they support risk-based prioritization: vulnerabilities tied to sensitive data surfaced first, guiding effective remediation.

Guardium Discover and Classify is a separate product. I think you are referring to "Guardium's discovery and classification capability"?

2.4 Community Insights

In practice, Guardium VA is widely acknowledged to apply to data-layer infrastructure—it doesn't target broader system assets (like middleware or endpoints) unless integrated with tools like QRadar for extended coverage . Also, keep Guardium's DPS patches updated to ensure your tests reflect the latest CVEs and benchmarks .

What is DPS?

3. Workshop activities

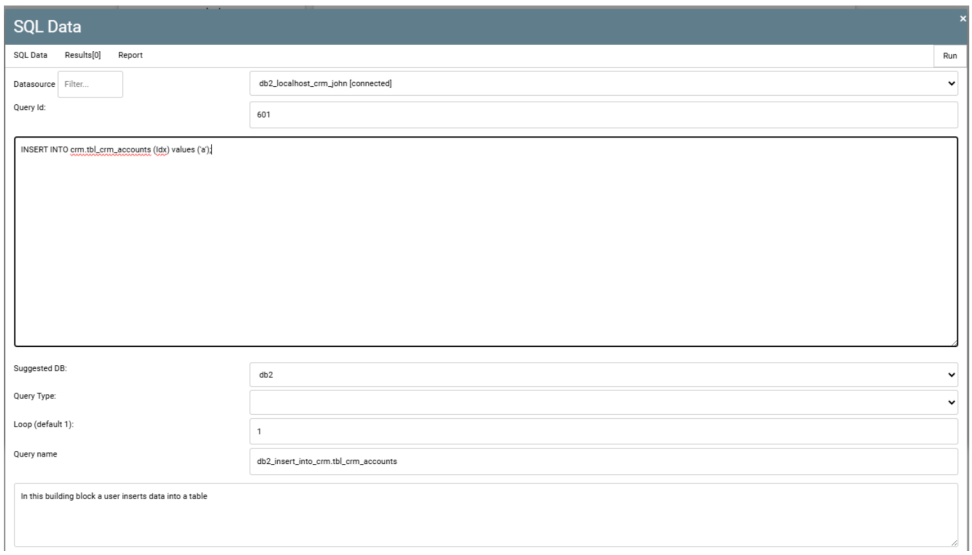
- Guardium Discover & Classify: Automates sensitive data discovery across structured and unstructured sources, enabling accurate classification with high ML-backed accuracy.
- Guardium Vulnerability Assessment: Scans databases/data warehouses for infrastructure and behavioral vulnerabilities, benchmarked against CIS/STIG and CVE standards.
- Together, they provide a robust, integrated data security posture management system—combining visibility, risk assessment, compliance, and actionable remediation.
- For the purpose of this workshop we will explore a small fraction of these capabilities. It is important however that you are aware of what can be done. This workshop will leave you with a working version of GDP for a period of time, so you can ofcourse continue to experiment with some self paced study into the above topics.

"of course"
"self-paced"

If you enter the wrong username or password into SLP, there is no feedback.

Step 6

Replace the text with the following, and hit run:
INSERT INTO crm.tbl_crm_accounts (Idx) values ('a');



I assuming we press "Run" after updating the query? Add that to the instructions?

Step 8

Now pat yourself on the back, we have generated an exception. We can now pivot to Guardium [GDP_URL] and verify it was picked up, by leveraging the exception count tile in GDP.

You can generate exceptions of all kinds with the 4 users (Polly, Liher, John and Jason) set up in SLP and verify the number of exceptions detected increases.

It would help to explain why this generated an exception, what an exception is and why we want to detect them.

Step 8

Now pat yourself on the back, we have generated an exception. We can now pivot to Guardium [GDP_URL] and verify it was picked up, by leveraging the exception count tile in GDP.

You can generate exceptions of all kinds with the 4 users (Polly, Liher, John and Jason) set up in SLP and verify the number of exceptions detected increases.

Put a red box around the "excep" in the search box to show users they need to type that.

Wrap up the "Generating data" section with a summary of what they did and the value.

Event dashboard > DAM and Policy Creation

DAM and Policy Creation

1. DAM & Policy Creation

Guardium supports DAM for new platforms, including Amazon Redshift, RDS for SQL Server, OpenSearch, Percona MySQL, YugabyteDB, PostgreSQL 16, Neo4j 5.x, MongoDB 7.x, and more via updated Linux UNIX STAPs.

DAM supports both agent-based (STAPs) and agentless monitoring using connectors for cloud streams and database event streams. It supports real-time alerting and recording of database access across multiple deployment topologies (on premise, hybrid, cloud)

It also supports old platforms :) maybe say, "many platforms, including new platforms such as……", and you could link to the webpage that shows all the supported platforms.

1.1 Classification & Sensitive Data Discovery

Guardium provides resource discovery and classification via regex-based, exact match, and metadata scanning across structured and unstructured data. Classification Process Builder (Discover → Classifications → Classification Process Builder) allows defining policies to discover sensitive values (e.g. credit card regex), assign data sources and schedule executions guardiumnotes.

Remove the work "regex"
What does assign data sources mean? Assigning to what?
What does schedule executions mean? If the sentence remains you need a space between guardium and notes. Also Guardium should always be capitalized.

1.2 Policy Creation & Management

Policy Builder (DAM Policy Setup)Policies are constructed in the Policy Builder interface, which organizes criteria into session-level, SQL-level, and other categories for clarity and ordering guardiumnotes. You define rules by selecting triggers such as activity type (e.g. SELECT, INSERT, DDL), user, object, time-of-day, IP, and sensitive columns. Guardium includes prebuilt compliance templates for PCI DSS, GDPR, HIPAA, SOX, CCPA that can be customized

Space and small "p" in policies.
What are "guardiumnotes"??

1.3 Rule Logic & Order

Rules execute in specified order; you can copy, import, and reorder them to optimize policy performance and reduce false positives . Policy Analyzer (introduced in Guardium v11 and available in 12.1) provides visibility into which rules fired, which never fired, and helps tune heading level and ordering .

In "the" specified order.

1.4 Actions & Alerts

You configure real-time alert actions for rules: logs, email, SNMP, or integration to SIEM/SOAR. You can designate alert receivers and roles; after saving, notifications can be configured. For advanced deployments, Guardium supports Advanced DAM packages that add blocking/masking capabilities for prevention—not just detection.

The sentence is confusing.
Should "Advanced" be lowercase "A" or is Advanced DAM packages a proper name?

1.5 Analytics, Outlier Mining & Exclusions

Active Threat Analytics and Outlier Mining detect anomalies and flag unusual behavior (e.g. off-hours access, massive queries) leveraging UEBA models. You can exclude known benign activity or sources (e.g. trusted applications, temp tables) from analytics mining. Exclusions can be time-bound (future date ranges).

Remove "and"

1.7 Central Management & Deployment

You manage multiple Collectors from a centralized Central Manager, including policy distribution, agent management, compliance schedules, and reports.

Deployment can be done on-prem, containerized or cloud; S-TAPs can be deployed via GIM or Kubernetes; advanced scaling with container orchestration supports elasticity.

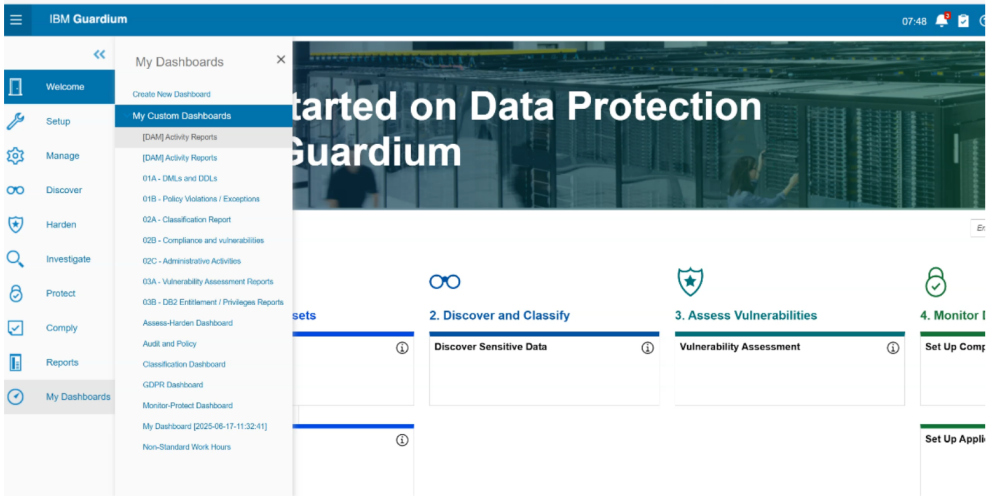
Spell out Guardium Installation Manager (GIM).

2. Workshop activities

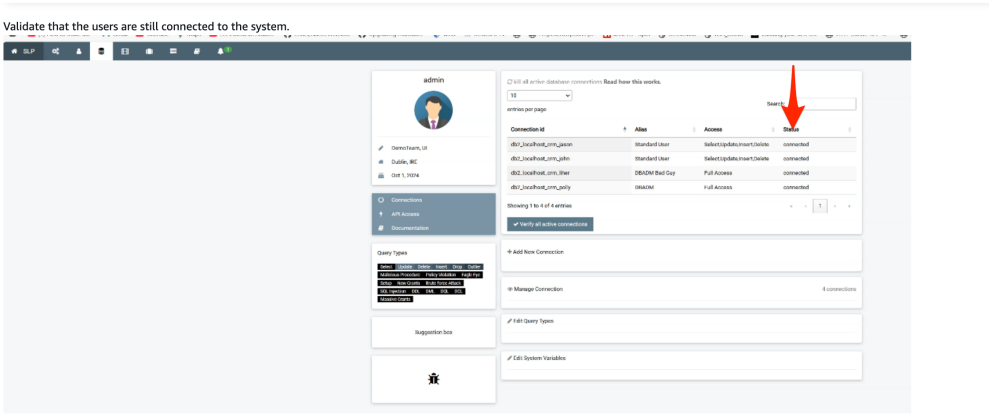
For the purpose of this workshop we will explore a small fraction of these capabilities. It is important however that you are aware of what can be done. This workshop will leave you with a working version of GDP for a period of time, so you can ofcourse continue to experiment with some self paced study into the above topics.

"of course"

We have now successfully generated traffic and we can now visit Guardium DAM reports to see what has been generated. We do this by clicking on My Custom Dashboards, [DAM] Activity Reports.

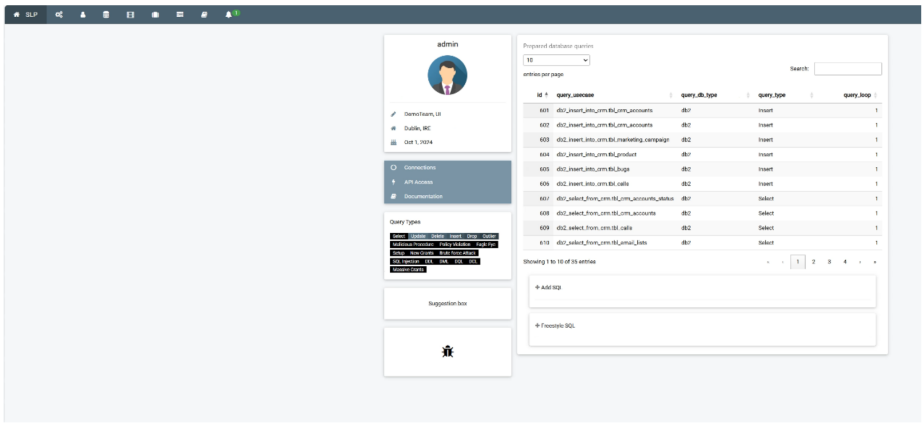


Put red boxes around "My Dashboards" and "My Custom Dashboards". Since "Welcome" is solid blue it makes you think you clicked on that to get to "My Custom Dashboards".



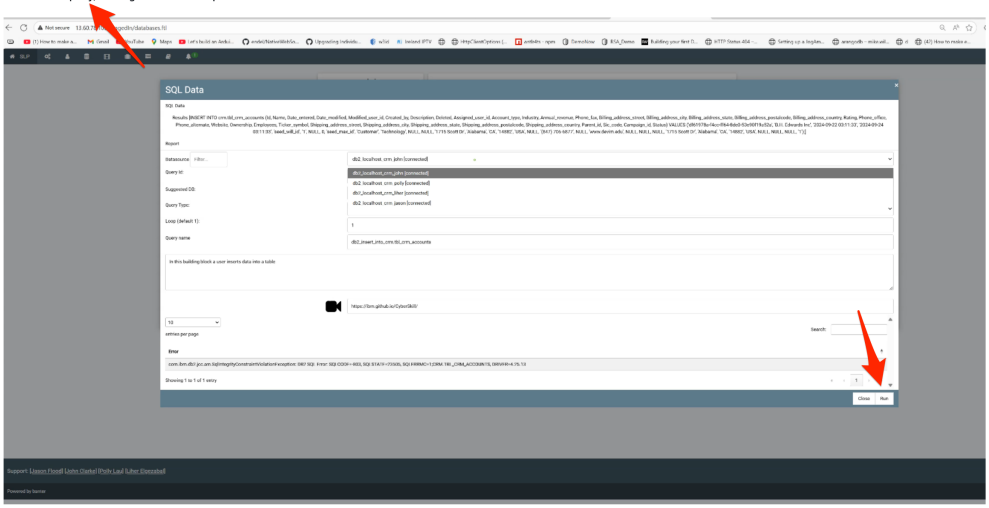
Clarify that they validate that the users are connected by looking at the "Status column".

Now click on the database icon in the top nav

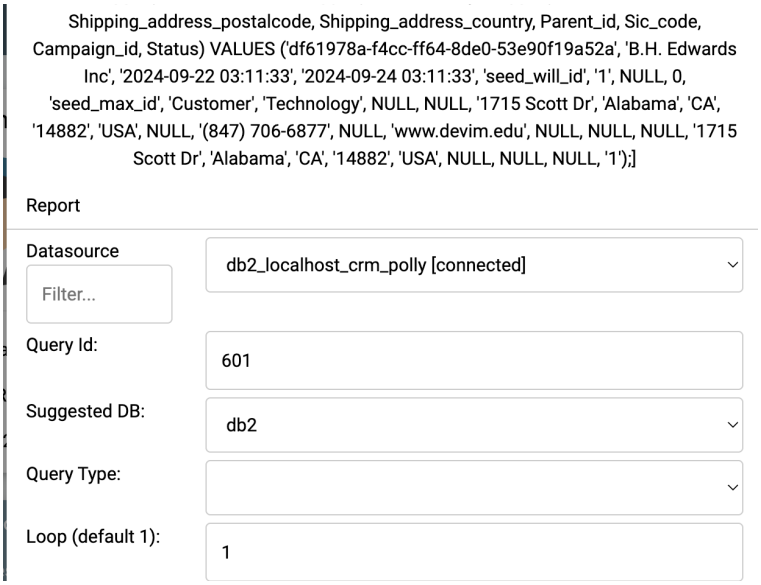


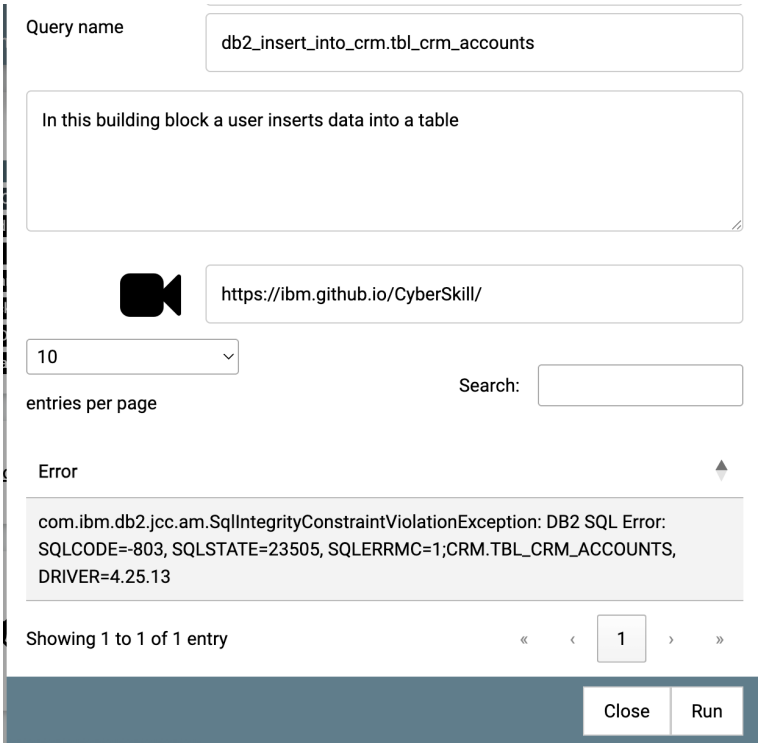
Put a red box around the database icon you want them to click, and the first query.

Execute this query, it will generate an exception.

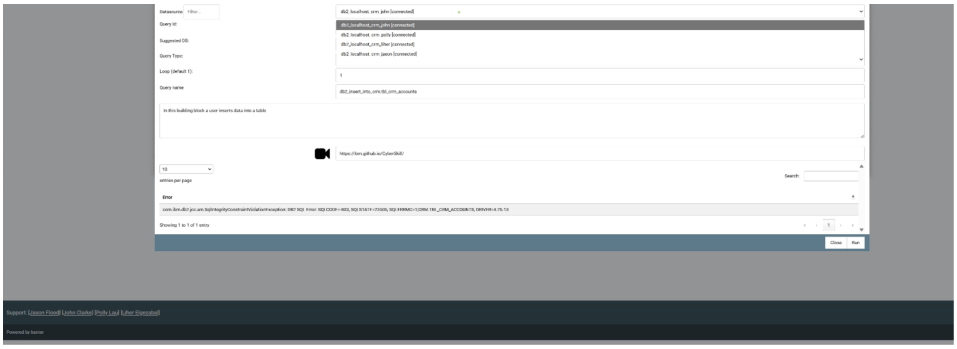


Execute this query by clicking "Run" ....
Red box around the "Run" button.





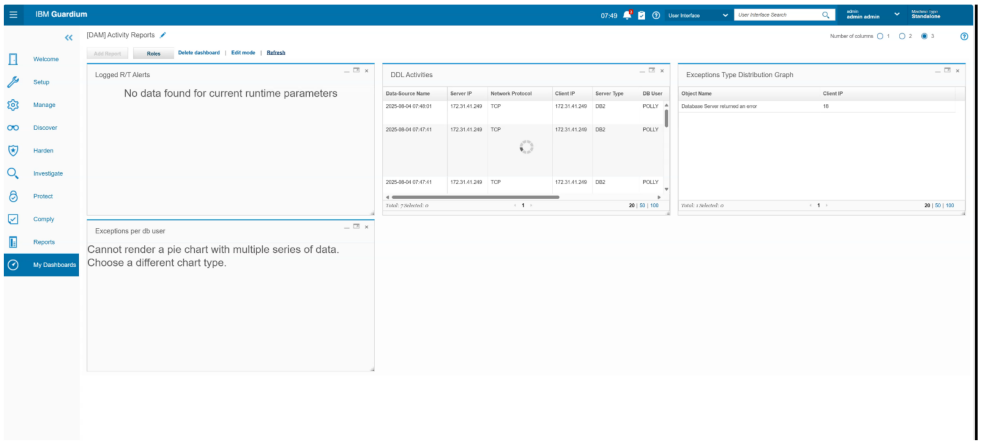
It's not clear when running the query for the other users if I just change the user in the drop-down and click run. If so, there is no feedback that it ran. If I close the window, select a different user and then click run I do get feedback, when it shows the error. ????



Now change between all the available users on the list and submit the query. Then return to GDP.

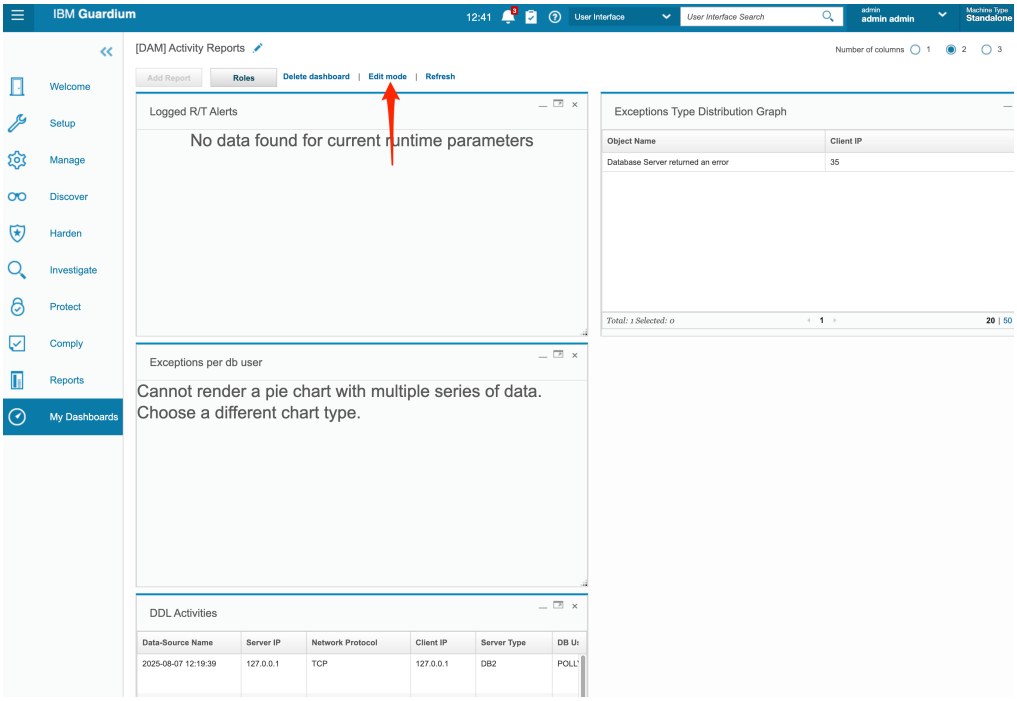
More details about the process for running it for each user.

….return to the [DAM] Activity Reports screen in the GDP console.



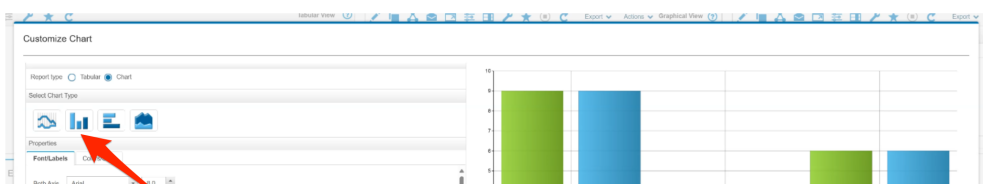
You will now see an error about bening unable to render data, click on edit mode. This will make the dashboard editable.

The error didn't show up right away. I think I refreshed etc. Initially the tile was still blank.

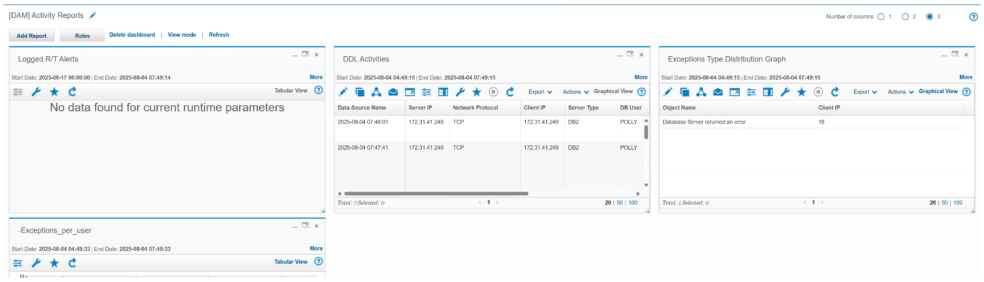


Clarify that the "Edit mode" button is at the top on the console and put a red box around the text to be selected.

This will allow you to customize the chart.



Change the chart to be a line chart.



Put a red box around the bar chart icon.
Change the text from "Change the chart to be a line chart" to "Change the chart to be a bar chart"

A list of potential reports can be added. You are free to experiment here, but to start lets add some of the basic reports. Use the filter to find and select the following items.

- Full SQL
- Count of DB traffic type per server
- Available VA tests
- Execution of ALTER commands
- Count of DB type
- Available Test Notes
- Execution of Create commands
- Commands List
- Assessment tests
- Exceptions Report
- Commands Execution Summary
- Analyze Limits
- Exceptions Monitor
- Analytic Status
- DML Executions Per Day
- Application Objects Summary
- ALTER Commands Execution
- DDL Distribution
- Execptions_per_user
- All Activities
- DDL commands
- Available VA tests
- All Roles - User
- DDL Activities
- Available VA tests - detailed
- Activity By Client IP
- Create Commands Execution
- Available VA tests
- All Guardium Applications - Role

Available VA tests is here 3 times. You must love that report ;)