

IBM® Guardium®

Essentials-2025



Disclaimer:

- This session provides an introductory overview of product features and is intended solely as a supplementary learning resource. It is not suitable for implementation purposes. Accurate deployment requires a thorough understanding of the product, its intended use, and environment—none of which are covered in this session.
- Content is subject to change as the product evolves. We do not accept responsibility for decisions made based on this material, and any actions taken are at your own risk. We disclaim liability for any resulting damages.
- For the most current and accurate IBM documentation, please refer to: <https://www.ibm.com/docs/en/gdp>
- By continuing to participate, you acknowledge and accept these terms. If you do not agree, please disconnect from the session.

Speaker for today:



Sachin Marawar

Technical Support Professional, Data Security

IBM Guardium Essentials-2025

8-Session Kickstart Series

Master the Foundations of Data Security Monitoring & Compliance

Session	Date	Topic	Registration Link
Session 1	Aug 26 (Tue)	What is IBM Guardium & How It Works	https://ibm.biz/IBMGE-S1
Session 2	Aug 28 (Thu)	Installing & Configuring Guardium Appliances	https://ibm.biz/IBMGE-S2
Session 3	Sep 02 (Tue)	GIM & WINSTAP Deployment	https://ibm.biz/IBMGE-S3
Session 4	Sep 04 (Thu)	Introduction to Guardium Policies	https://ibm.biz/IBMGE-S4
Session 5	Sep 09 (Tue)	GIM & S-TAP for UNIX/Linux	https://ibm.biz/IBMGE-S5
Session 6	Sep 11 (Thu)	Guardium Reports, Entities & Attributes	https://ibm.biz/IBMGE-S6
Session 7	Sep 16 (Tue)	Guardium Alerts & Audit Process	https://ibm.biz/IBMGE-S7
Session 8	Sep 18 (Thu)	Aggregation, Backup & Restore in Guardium	https://ibm.biz/IBMGE-S8

Today

Use above links to Register for each session!

Session 7:

Alerts & Audit Process

-Sachin Marawar

Technical Support Engineer, IBM Software Support (Data Security)



Agenda

- Understanding Alerts
- ↓
- Types of Alerts
- ↓
- Real-time & Correlation Alerts
- ↓
- **Demo** on Real-time & Correlation Alerts.
- ↓
- Compliance Monitoring
- ↓
- Building Audit Process
- ↓
- **Demo** on Audit Process creation
- ↓
- Q&A



Alerts in IBM® Guardium® Data Protection?

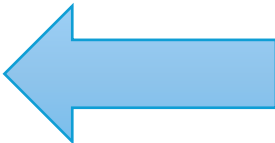
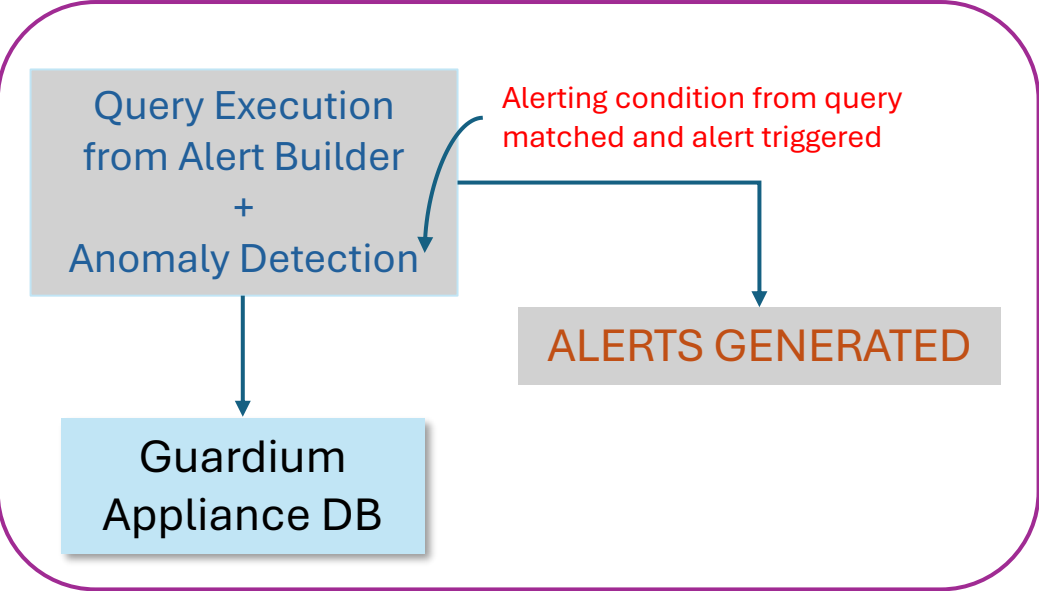
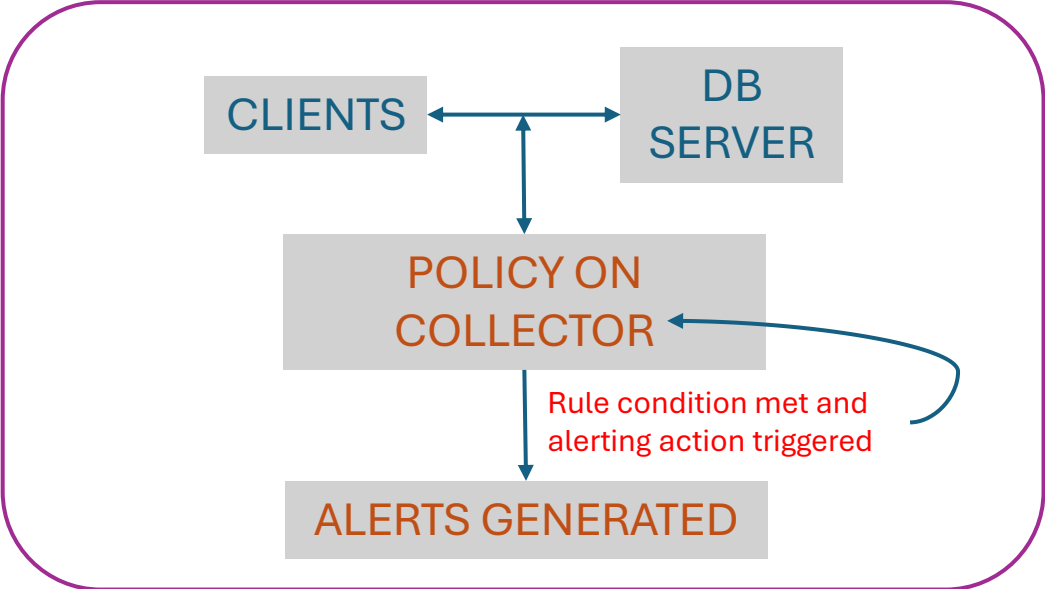


- Alerts notify administrators about potential security or compliance issues.
- Triggered by specific conditions or patterns in monitored data.
- **Requirement:**
 - Detect unauthorized access or data misuse
 - Ensure compliance with regulatory standards
 - Enable timely incident response
 - Automate monitoring across large environments

Types of Alerts?

- **Real-Time Alerts**

- Real-time
- Triggered immediately when a rule condition is met



- **Correlation Alerts**

- Not real-time
- Triggered by scheduled queries
- Based on Anomaly detection
- Also called threshold alerts

Notification Mechanisms

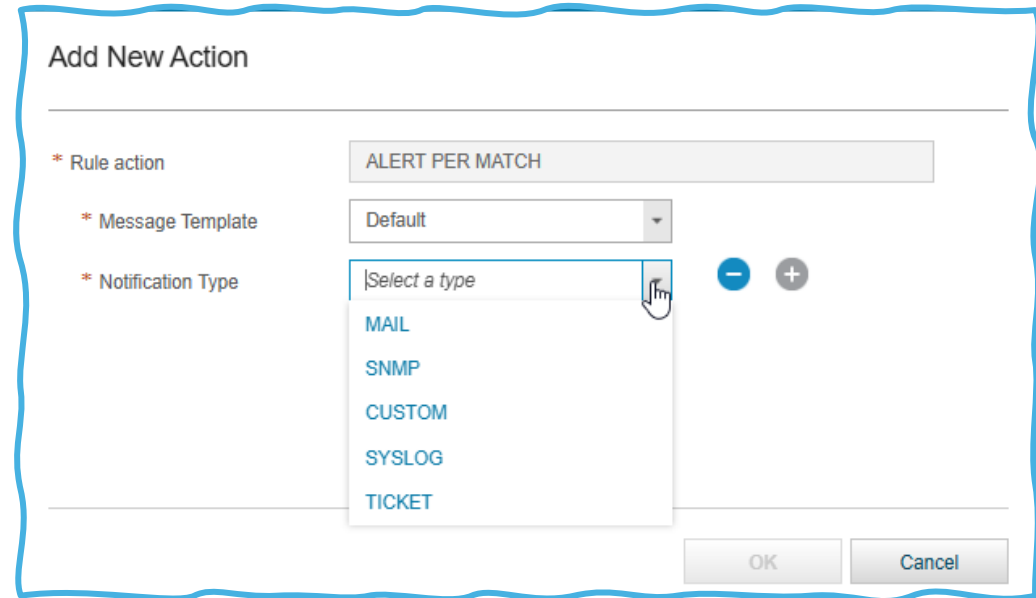
MAIL: Addressed to Guardium users, and will be sent via the SMTP server configured for Guardium

SNMP: Sent to the trap community configured for the Guardium appliance.

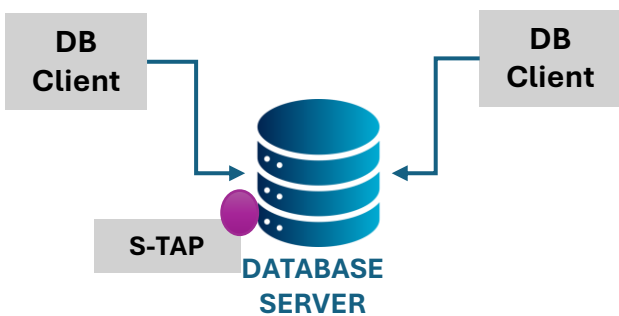
CUSTOM: Alert message and timestamp passed to a set of user-written notification handlers, implemented as Java classes

SYSLOG: Written to syslog. This can be configured for external repository integration (QRadar)

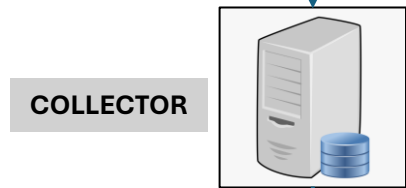
TICKET: External Ticketing System Integration.



What is real-time alert?



Sniffer on collector applies policy rules to traffic



conditions in rule meet and alert action triggered by sniffer



MAIL/ SNMP/ SYSLOG (SIEM) 

• Real-Time Alerts

- Real-time
 - Triggered immediately when a rule condition is met
 - Inspection engine involved here
 - Collector generated (because policy works on collector only)
- **Example:** send an alert if a client ip is not present in the authorized client ip group.

A screenshot of a web interface for configuring policy rules. The table below shows two rules, with the first rule highlighted in red. An arrow points from the 'Criteria' column of the first rule to the 'Alert' icon in the diagram above.

Order	Rule type	Rule name	Tags	Criteria	Actions	Continue to next rule	Installed
1	Access	Client IP Not Authorized		Client IP address Not in group Authorized Client IPs, Severity = Med	ALERT PER MATCH	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	Access	Rule To Log Everything		Severity = Info	LOG FULL DETAILS, ALERT PER MATCH	<input type="checkbox"/>	<input checked="" type="checkbox"/>



Alerting Actions:

Alert Action	Description	Use Case
Alert Daily	Sends a notification only the first time the rule is matched each day.	Ideal for recurring events where daily awareness is sufficient.
Alert Once Per Session	Sends a notification only once per session, even if the rule is matched multiple times.	Useful when monitoring bulk operations to avoid alert flooding.
Alert Only	Sends messages to /var/log/messages (for syslog) or to the MESSAGE table (for other types). Does not notify of policy violations.	Best for alerting only. No logging in violations at all
Alert Per Match	Sends a notification every time the rule is satisfied.	Suitable for critical conditions requiring immediate attention.
Alert Per Time Granularity	Sends notifications once per logging granularity period (e.g., hourly).	Useful for periodic monitoring without excessive alerts.



[View Best Practices](#)



1. Manage Your Assets

Manage Databases ⓘ

Manage Applications ⓘ



2. Discover and Classify

Discover Sensitive Data ⓘ



3. Assess Vulnerabilities

Vulnerability Assessment ⓘ



4. Monitor Data Access

Set Up Compliance Monitoring ⓘ

Set Up Application Data Monitoring ⓘ

Install Basic Security Monitoring Policy ⓘ



5. Advanced Analytics

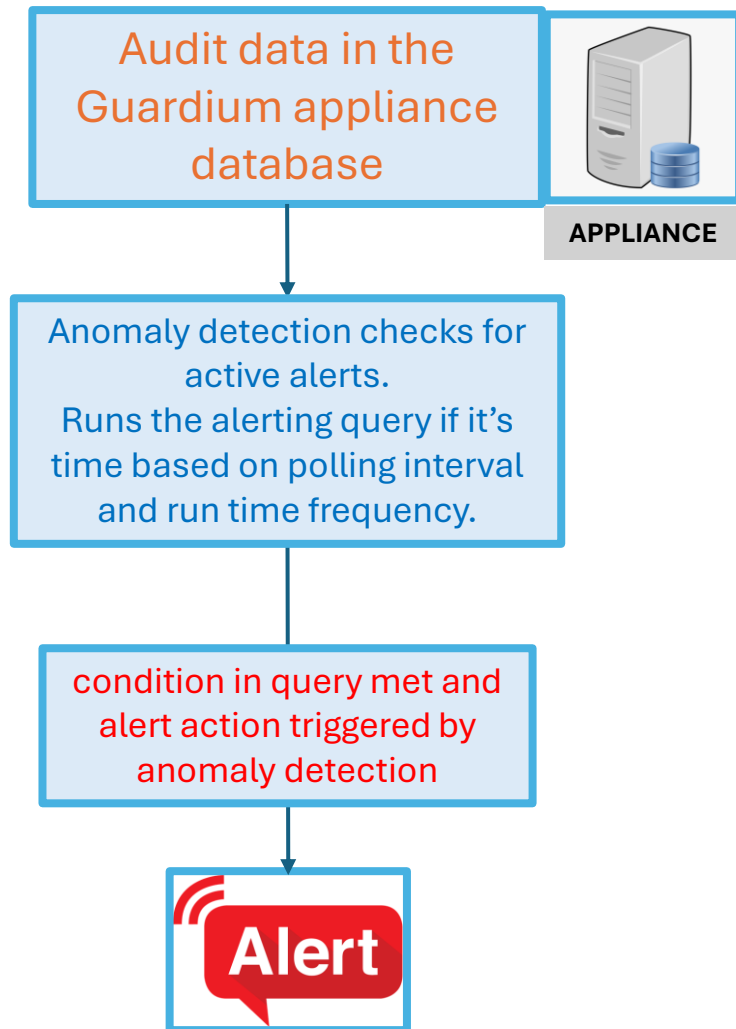
Risk Spotter ⓘ

Active Threat Analytics ⓘ

Investigation Dashboard ⓘ



What is Correlation Alert?



- **Not** real-time
- **Purpose:** Detect anomalies such as excessive SQL errors or login failures etc.
- **Mechanism:** Correlates events using queries that track thresholds over time.
- **Trigger:** Alerts are generated when defined thresholds are met.
- By default, does not log a policy violation (but can)
- Notification via SMTP, SNMP, Syslog, custom, tickets.
- Anomaly detection engine executes alerts
- **Example:** too many login failures to DBs in a defined time window

Key Components of a Correlation Alert

1

Query

- must contain a timestamp and count
- limit of 30 fields
- complex queries are expensive

3

Alerter

- must be active
- define frequency at which alerter checks for and sends messages
- configure SMTP, SNMP

2

Alert Builder

- select query to be used
- define alert parameters

4

Anomaly Detection

- must be active
- creates and saves, but does not send notifications

Creating a Correlation Alert

admin, user sam admin

NAME	LOCATION
Alert Builder	Protect > Database Intrusion Detection > Alert Builder

1

IBM Guardium

Alert Finder

- Active Risky Users : Risky Users Scores
- Active S-TAPs Changed : Active S-TAPs Changed
- Aggregation/Archive Errors : Alert on any Aggregation/A
- Analyze Limits : Analyze Limits

2

Add Alert

Settings

* Name

* Description

Category

Classification

Recommended Action

Message Template

Severity

* Run frequency

Active

Log policy violation

View in deployment health dashboard

3

Alert Definition

* Query

* Accumulation interval

Move interval window earlier by

Note

Log full query results

Column

Alerts run on aggregators will be based only on data within the defined merge period

Query has no numeric columns; The alert threshold refers to the total rows in the report.

4

Alert Threshold

* Threshold

* Alert condition:

Threshold Evaluated:

Threshold Used:

Value

threshold

per report

per line

As absolute limit

As percentage change within period:

From

To

As percentage change for the same "Accumulation Period" on a relative time:

Ending at

5

Notification

* Notification frequency

Managed Units

This Central Manager

Select Units

Alert Receivers

6



Anomaly Detection
+
Active Alerts



Alert Receiver Selection

Add Receiver to Alert: Active Risky Users

Notification Type

Alert Receiver

Save

7



query must contain
count and timestamp

Anomaly Detection & Run Frequency

Anomaly Detection

Active on startup

Polling Interval (minutes)

Anomaly Detection is Running

Active Alerts

enter a filter

Name	Description	enabled on: <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	unit assignments
Failed Logins to Guardium	Alert on multiple Failed Logins to the Guardium appliance	<input checked="" type="checkbox"/>	All
Security Incident Alert	Security Incident Alert	<input checked="" type="checkbox"/>	All
Investigation Dashboard Issues	New Issue Detected	<input checked="" type="checkbox"/>	All
Outlier with anomaly score 90 and above	Outlier with anomaly score 90 and above	<input checked="" type="checkbox"/>	All

Settings

* Name

* Description

Category

Classification

Recommended Action

Message Template [Edit message templates](#)

Severity

* Run frequency (minutes)

Active

Log policy violation

View in deployment health dashboard



Polling interval should be smaller than the smallest "Run Frequency"

Message Template

11:16 3 1 ? User Interface Global Pr 🔍

NAME	LOCATION
Global Profile	Setup > Tools and Views > Global Profile

Named Template Finder

+ ✎ 📄 -

- ArcSight
- EnVision
- LEEF
- LEEF Discovered Databases
- EnVison_2
- Threshold Default Template
- 🔍
- @TEMPLATE-RTA-Standard
- LEEF - 12.1

Filter Real Time Alert Audit Process Report Threshold Alert Audit Process Email

Back

Global Profile ?

Use aliases in reports unless otherwise specified

PDF footer text

Default message template

No wrap

Named template

Alert message template variables

Table 1. Alert message template variables.

- Note:** Only the following variables in the Alert template are available for correlation alerts.
- Subject: **%%Subject[Guardium Alert. Severity: (%%severity), Alert Name: %%alertName]**
 - Alert Name: **%%alertName**
 - Alert Description: **%%description**
 - Current value: **%%alertQueryValue**
 - Base query value: **%%alertBaseQueryValue**
 - Threshold: **%%alertThreshold**
 - Query period: **%%alertQueryFromDate - %%alertQueryToDate**
 - Alert Classification: **%%classification**
 - Category: **%%category**
 - Severity: **%%severity**
 - Recommended Action: **%%recommendation**

Build & Run Correlation Alerts

The screenshot displays the IBM Guardium user interface. At the top, the header includes the 'IBM Guardium' logo, the time '14:44', notification icons, and the user 'admin admin'. A search bar is also present. Below the header is a large banner with the text 'Get Started on Data Protection with Guardium' over a server room background. A left-hand navigation menu contains various icons. The main content area features a search bar with the placeholder text 'Enter keywords to discover additional Guardium features'. Below this is a grid of five feature categories, each with a list of specific actions:

- 1. Manage Your Assets**
 - Manage Databases ⓘ
 - Manage Applications ⓘ
- 2. Discover and Classify**
 - Discover Sensitive Data ⓘ
- 3. Assess Vulnerabilities**
 - Vulnerability Assessment ⓘ
- 4. Monitor Data Access**
 - Set Up Compliance Monitoring ⓘ
 - Set Up Application Data Monitoring ⓘ
 - Install Basic Security Monitoring Policy ⓘ
- 5. Advanced Analytics**
 - Risk Spotter ⓘ
 - Active Threat Analytics ⓘ
 - Investigation Dashboard ⓘ

Audit Process

- A structured workflow in IBM Guardium for managing compliance tasks
- Automates steps like:
 - Asset discovery
 - Vulnerability assessment
 - Monitoring and reporting
- Ensures alignment with privacy, governance, and regulatory standards
- Built using the **Audit Process Builder**
- Supports role-based access, scheduling, and export options (CSV, Syslog, CEF)

Audit Process Builder

- Centralized tool for managing audit workflows
- Supports compliance tasks: discovery, assessment, monitoring, reporting
- Automates processes for privacy, governance, and regulatory needs
- Export options: Syslog, CSV, CEF
- Archiving via Investigation Center



The results of each audit process, including the review, sign-off trails, and comments, can be archived and later restored and reviewed through the Investigation Center (if enabled)

Audit Process (continued)

Elements of an Audit Process

- process definition
- set of tasks
- distribution plan
- schedule
- workflow/ events & sign-off
- reports, export & archive

Add tasks *Add tasks to this audit process*

Review tasks, define execution sequence and review options. Select a row to edit options.

Task name	Description	Task type
<input type="checkbox"/> Failed Logins to Guardium	Logins to Guardium Appliance	Report
<input type="checkbox"/> Active Guardium Users - Credentials Summary	Guardium Users - credentials	Report
<input type="checkbox"/> Aggregation/Archive Errors	Aggregation Errors	Report
<input type="checkbox"/> Policy Related Changes	Policy Changes	Report
<input type="checkbox"/> Inspection Engines and S-TAP Changes	Inspection Engine Changes	Report
<input type="checkbox"/> Data Source Changes	DataSource Changes	Report

Details for: Appliance Monitoring

Name and archive *Name and archive options for the audit process*

* Name

Archive Allow results to be purged prior to review Keep for a minimum of days or runs

CSV/CEF file name Zip CSV for email

* Email subject

Custom email template

Export results Disabled At the end of process At the end of each task

All roles assigned.

No comments have been made on this audit process.

New Receiver

Receiver Type Role Email User Group User Ticket

* User

Action Review Sign off Approve if empty

Add to to-do list

Email format

Distribution sequence Simultaneous Sequential

Audit Process Scheduling

Schedule audit process Schedule when the audit process will be repeated

Audit process is not scheduled for execution

Schedule by Please select

Repeat
Schedule tasks to run more than once each day

Repeat every hours

Within each hour, run every 1 minutes

* Start schedule at 12:00 AM

Begin schedule 9/14/2025

Activate schedule

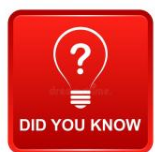
Auto run dependent jobs

Audit process is scheduled and active

Schedule by Day

Run audit process Optional: Run audit process

Job type	Dependent jobs	Reason
Audit process with discover sensitive data task	Where the task includes a discover sensitive data scenario with a Policy > Rule > Action for <i>Add To Group of Objects</i> , <i>Add To Group of Object/Fields</i> or <i>Add To Access Rule</i> . For more information, see Discovery scenarios and What to discover .	Before installing policy rules that use groups, the group data must be up to date.
Audit Process with report task	A custom table upload job where the custom table name is referred to by the report audit task.	Custom table data that is referred to by a report-type audit task must be populated with up-to-date data before the Audit Process can run.
Audit Process with report task	Groups that are defined in an audit task report condition that are populated by the 'Populate From Query' mechanism.	Groups that are referred to by a query condition must be populated with up-to-date data before a report-type Audit Task can run.
Audit Process (for aggregators)	Import	For aggregators only. Ensures that information is imported from all aggregated units before any audit process can run.



Aggregators are the best place to run audit processes



Build Audit Process & Execution



[View Best Practices](#)

Enter keywords to discover additional Guardium features



1. Manage Your Assets

Manage Databases ⓘ

Manage Applications ⓘ



2. Discover and Classify

Discover Sensitive Data ⓘ



3. Assess Vulnerabilities

Vulnerability Assessment ⓘ



4. Monitor Data Access

Set Up Compliance Monitoring ⓘ

Set Up Application Data Monitoring ⓘ

Install Basic Security Monitoring Policy ⓘ



5. Advanced Analytics

Risk Spotter ⓘ

Active Threat Analytics ⓘ

Investigation Dashboard ⓘ

Adhoc Audit Process

IBM Guardium 21:54 User Interface admin admin Machine Type Central Manager - Aggregator

Failed User Login Attempts

Start Date: 2025-09-14 18:53:43 | End Date: 2025-09-14 21:53:43 [More](#)

Export Actions Graphical View

DB User Name	Client IP	Server IP	Server Type	Exception Timestamp	Count of Exceptions
No data found for current runtime parameters and aggregation period					

Total: 0 Selected: 0 < 1 > 20 | 50 | 100

References:

Alerts: <https://www.ibm.com/docs/en/gdp/12.x?topic=system-alerts>

Creating Real-time alerts: <https://www.ibm.com/docs/en/gdp/12.x?topic=alerts-creating-real-time-alert>

Managing Correlation Alerts: <https://www.ibm.com/docs/en/gdp/12.x?topic=protect-managing-correlation-alerts>

Guardium Administrator Responsibilities: <https://www.ibm.com/support/pages/system/files/inline-files/Guardium%20Administrator%20Responsibilities%20Guide%20v2.pdf>

Guardium Redbook: <https://www.redbooks.ibm.com/redbooks/pdfs/sg248129.pdf>

Alerting Rule Actions: <https://www.ibm.com/docs/en/gdp/12.x?topic=actions-alerting-rule>

Predefined Admin reports: <https://www.ibm.com/docs/en/gdp/12.x?topic=reports-predefined-admin>

Investigation Center: <https://www.ibm.com/docs/en/gdp/11.5.0?topic=data-restoring-viewing-audit-results-in-investigation-center>

Message Template: <https://www.ibm.com/docs/en/gdp/12.x?topic=profile-alert-message-template>

[IBM Guardium Essentials-2025](#)



Q&A

Any
Questions?



Thank you for your attention!



- Register for-
18-September-2025
Thursday

Session 8: ibm.biz/IBMGE-S8

Aggregation/ Backup/ Restore

Feedback & Suggestions are welcome at:
datasec_ap_support@wwpdl.vnet.ibm.com