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.

IBM

Speaker for today:

Sachin Marawar

Technical Support Professional, Data Security

IBM

Data **Security**

IBM

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!

IBM

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

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

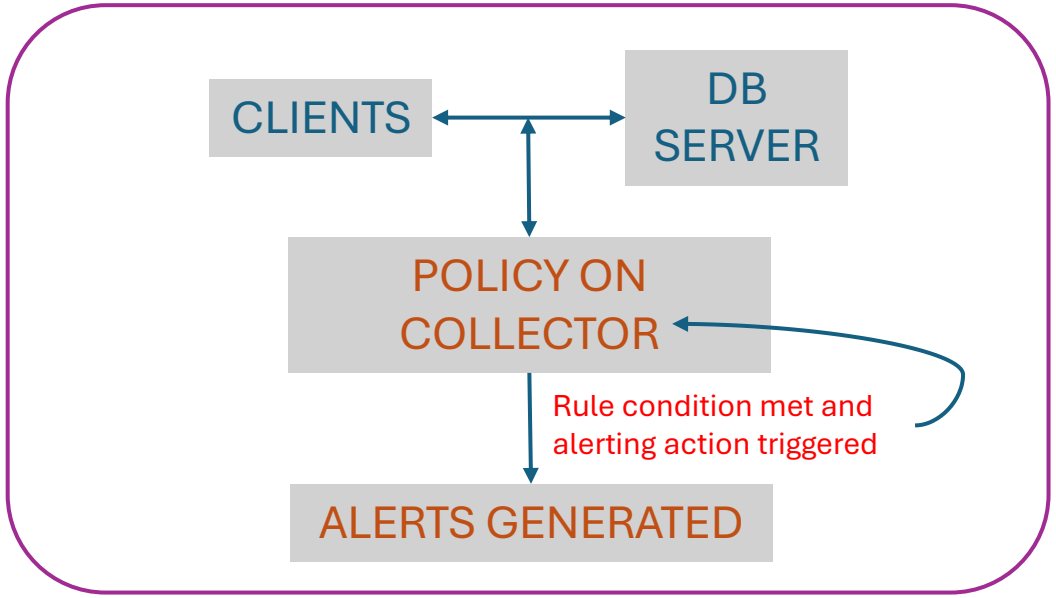
IBM

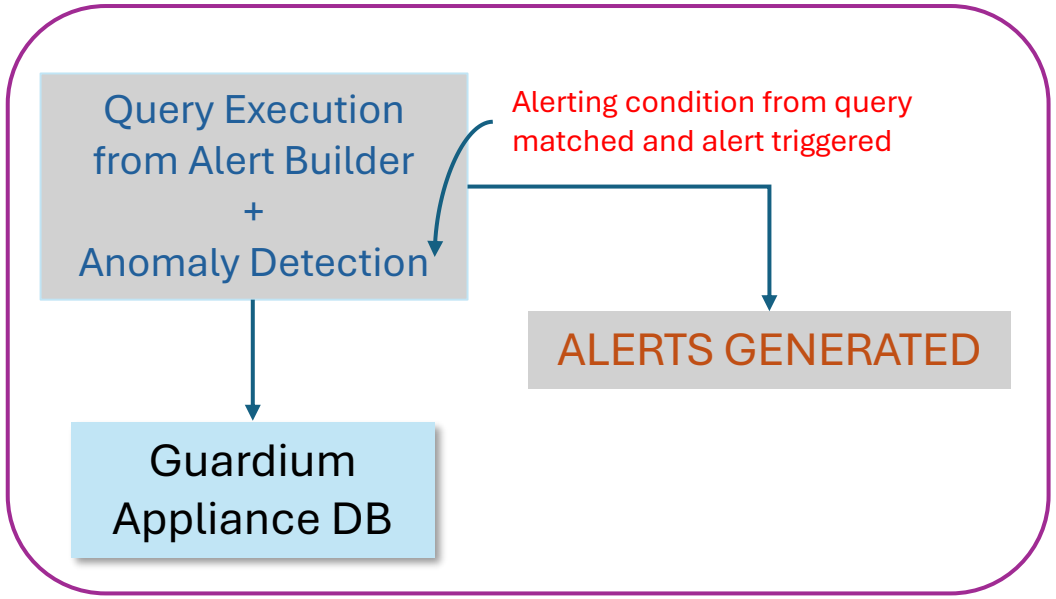
Alerts in IBM® Guardium® Data Protection?

- 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

IBM

Notification Mechanisms

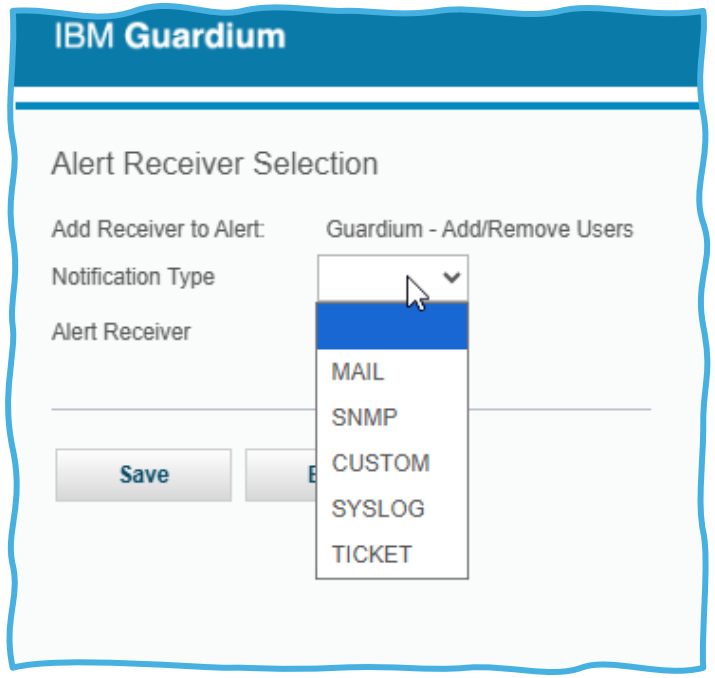
MAIL: Addressed to Guardium users, and will be sent via the SMTP server configured for Guardium

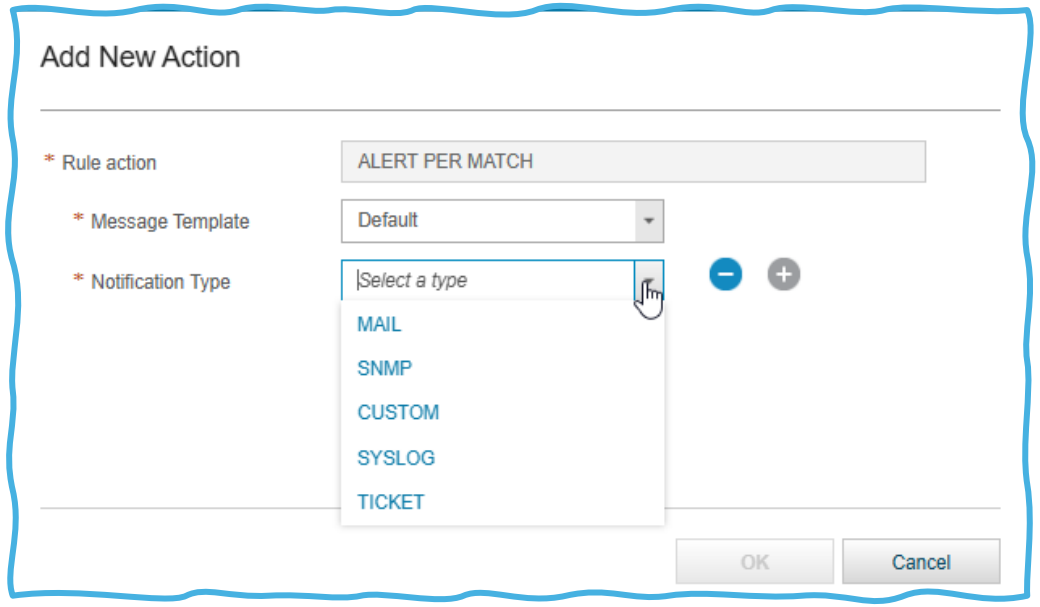
SNMP: Sent to the trap community configured for the Guardium appliance.

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

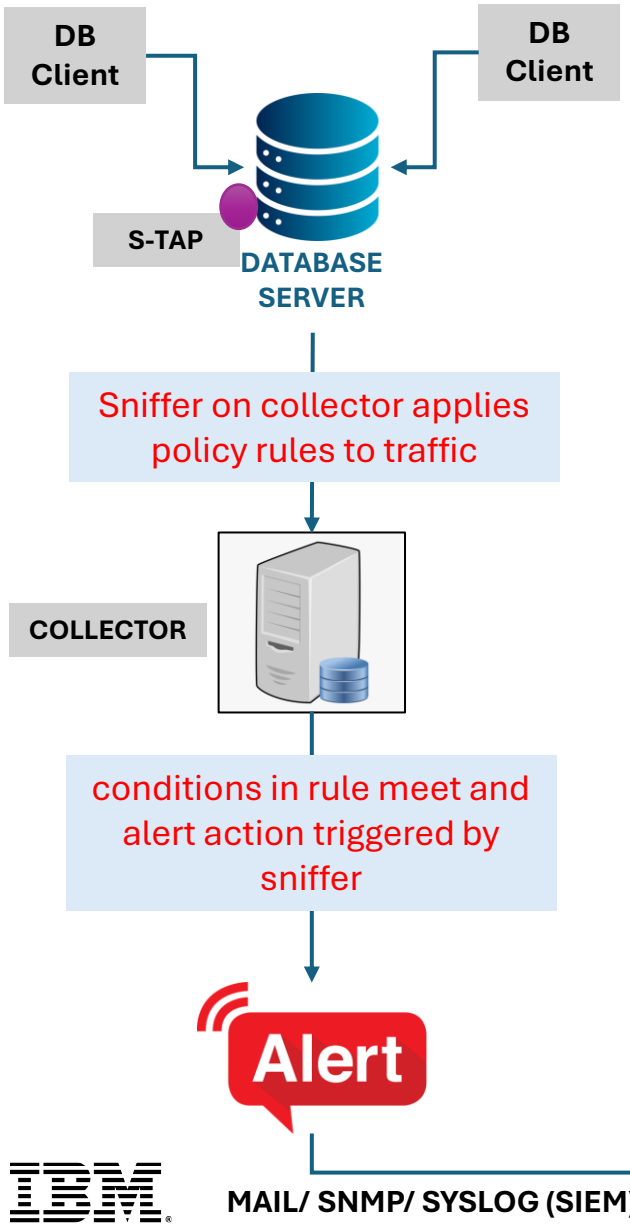
SYSLOG: Written to syslog. This can be configured for external repository integration (QRadar)

TICKET: External Ticketing System Integration.



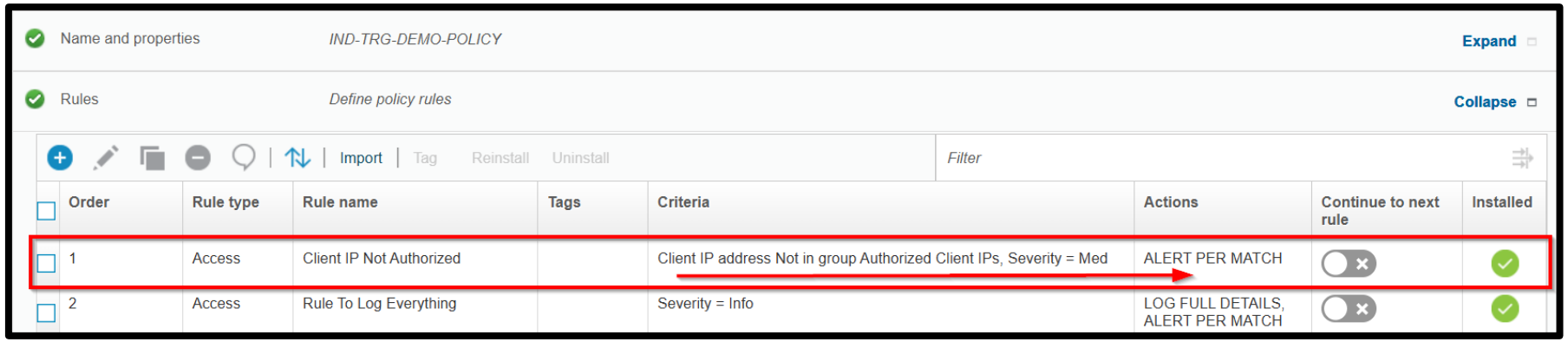


What is real-time alert?



- **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.



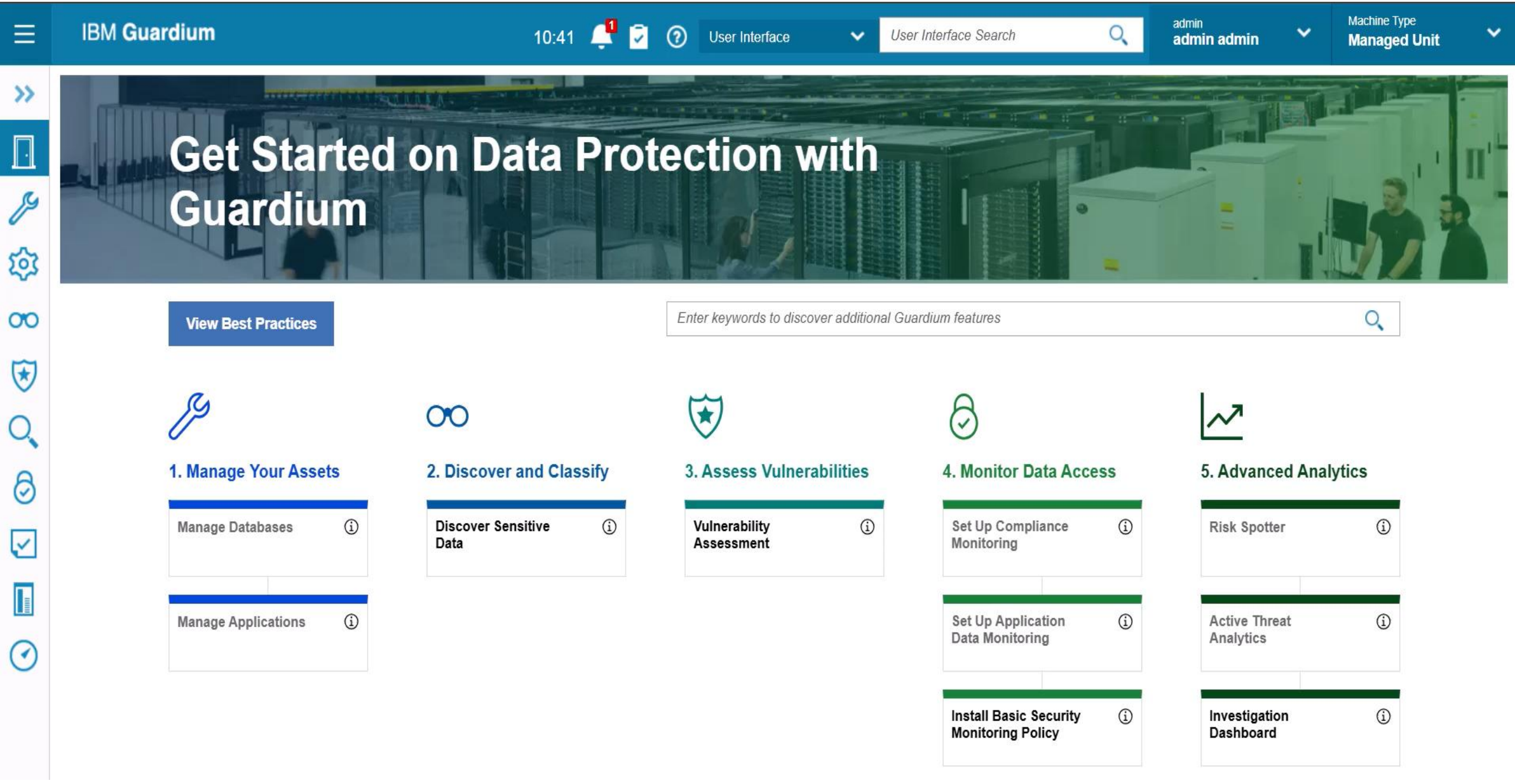
IBM

Radar

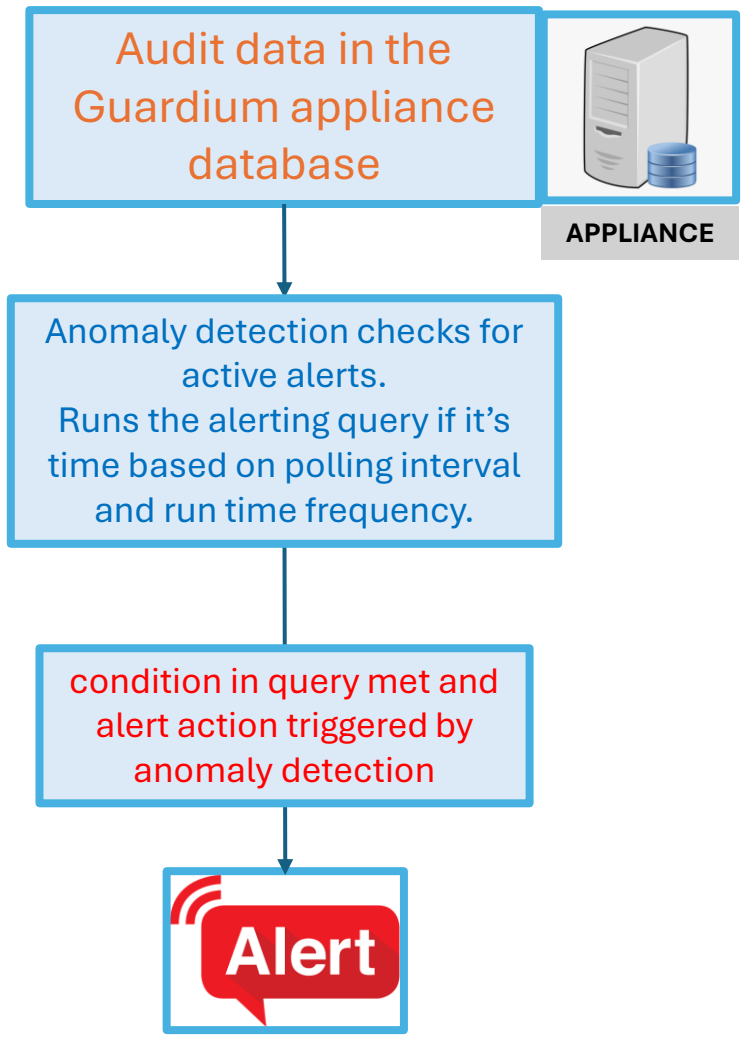
Alerting Actions:

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.

Real-time alert in action:



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

2 Alert Builder

- select query to be used
- define alert parameters

3 Alerter

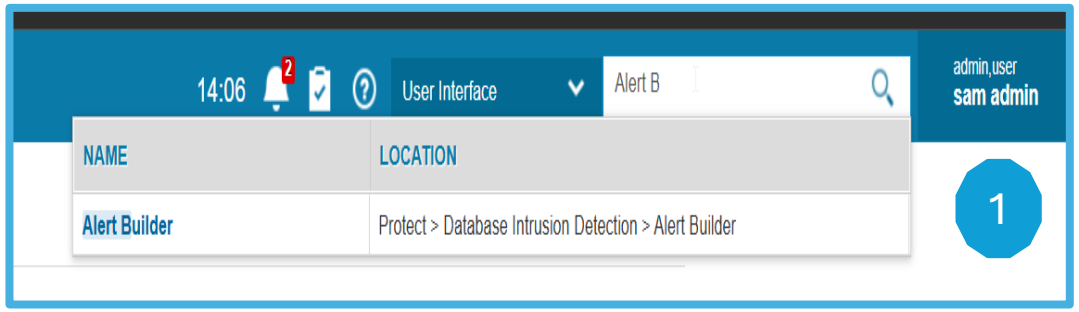
- must be active
- define frequency at which alerter checks for and sends messages
- configure SMTP, SNMP

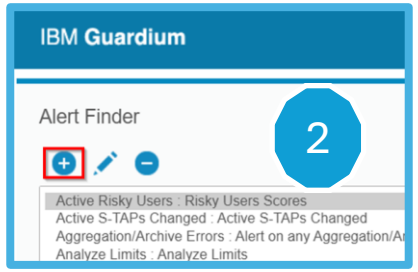
4 Anomaly Detection

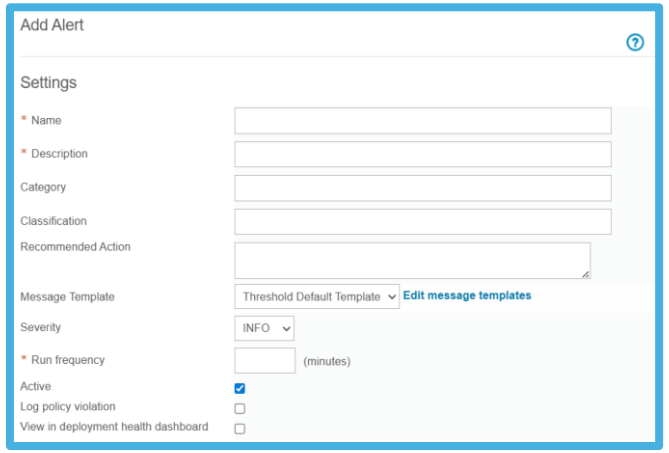
- must be active
- creates and saves, but does not send notifications

IBM

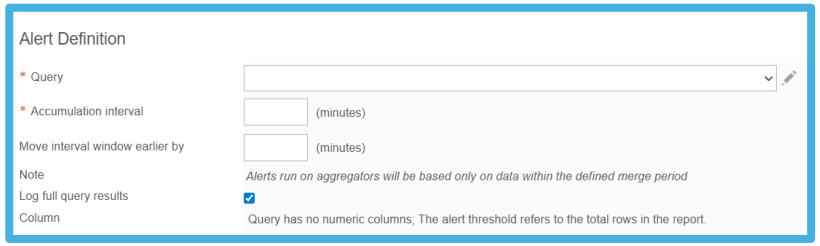
Creating a Correlation Alert



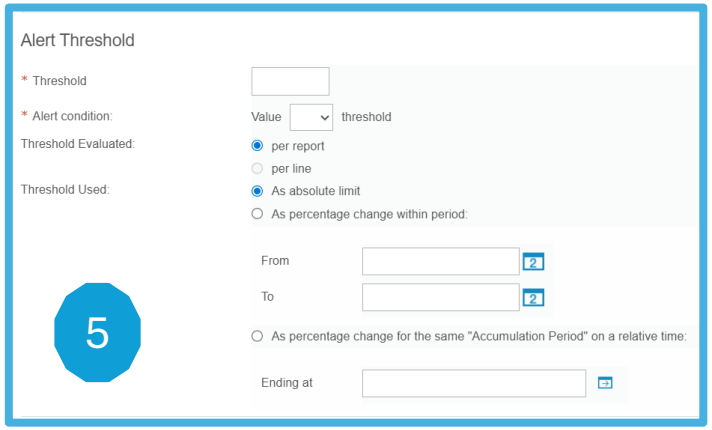


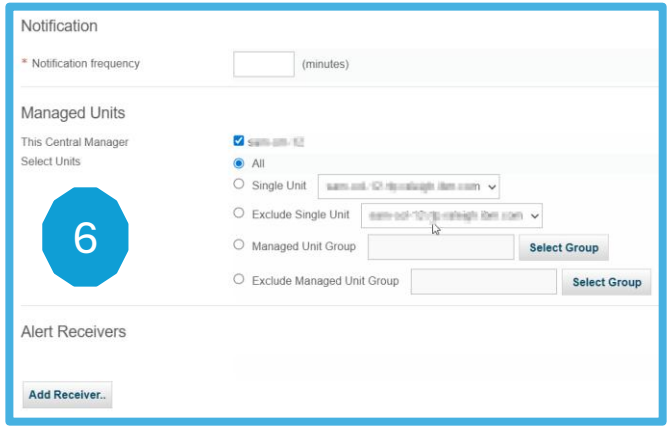


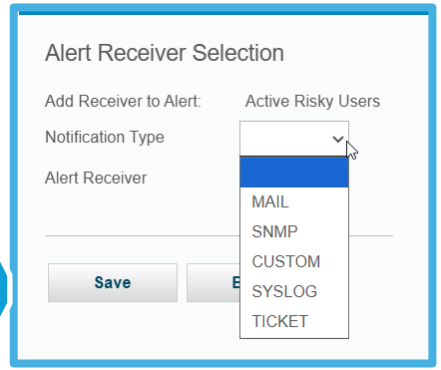
3



4



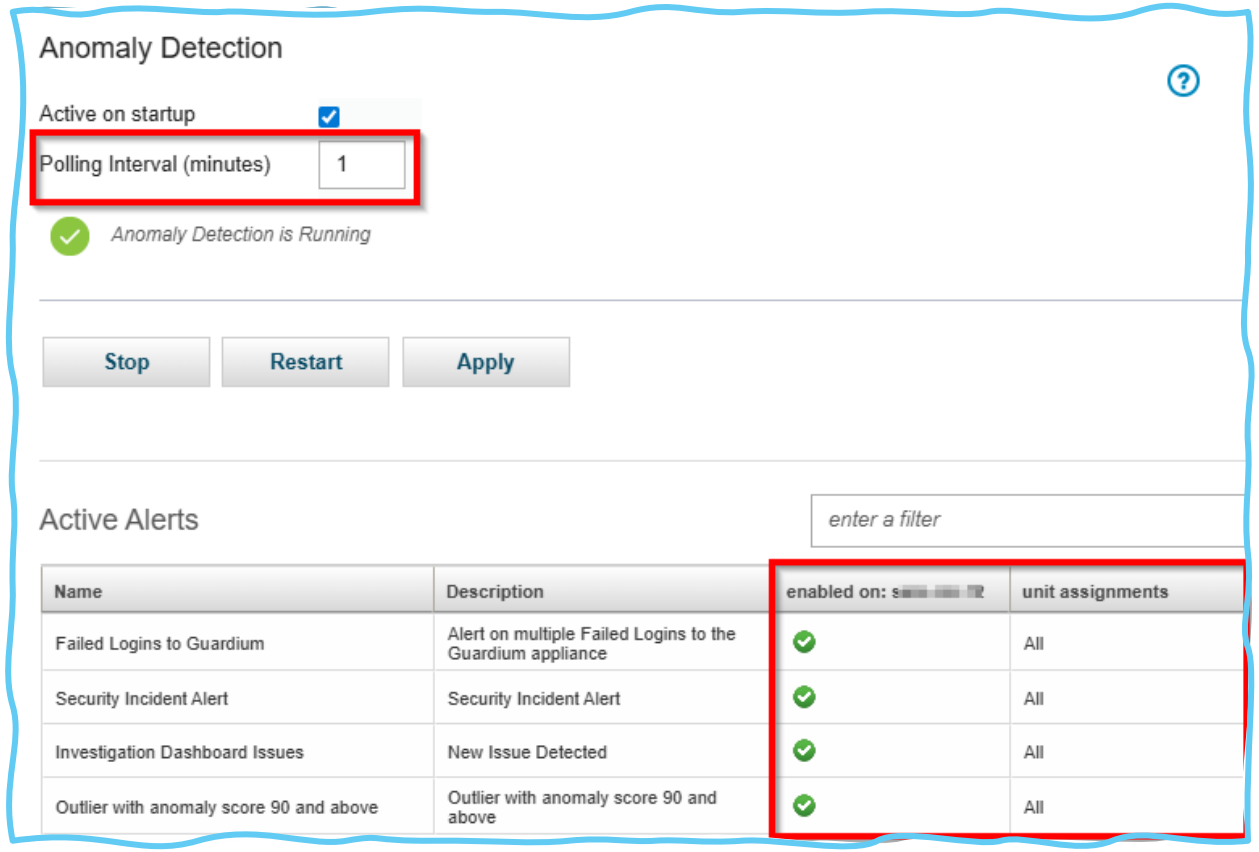


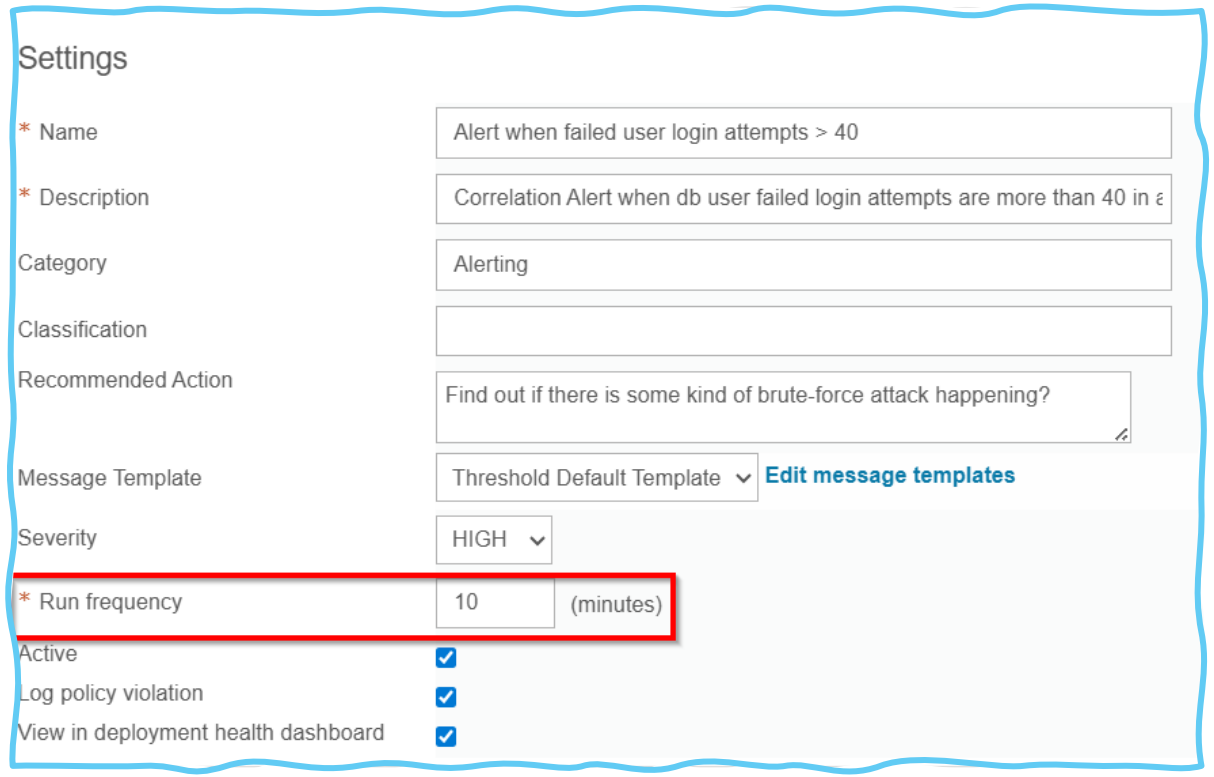


Anomaly Detection
+
Active Alerts

query must contain count and timestamp

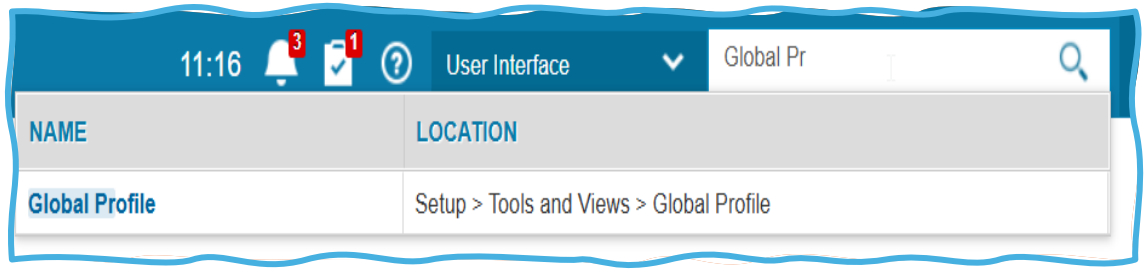
Anomaly Detection & Run Frequency

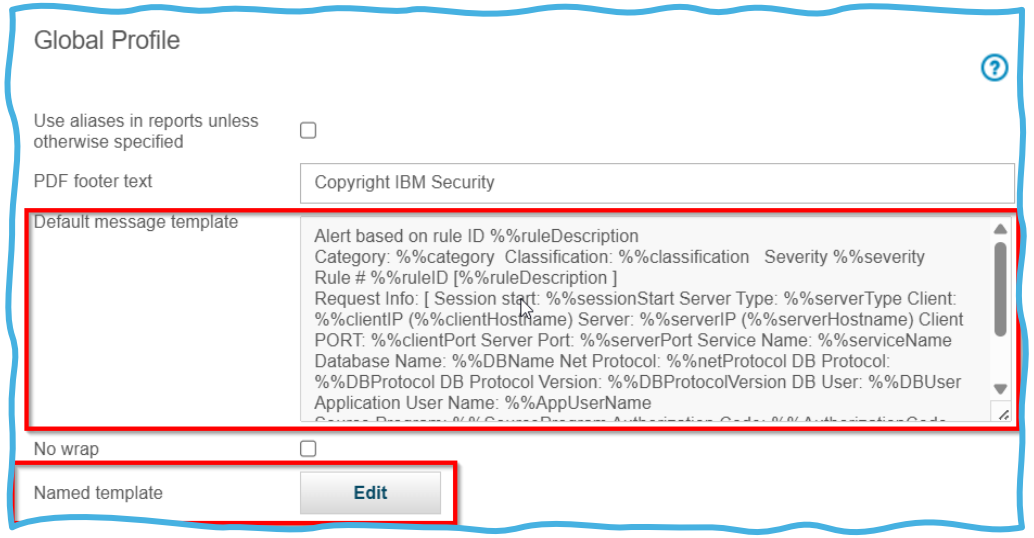


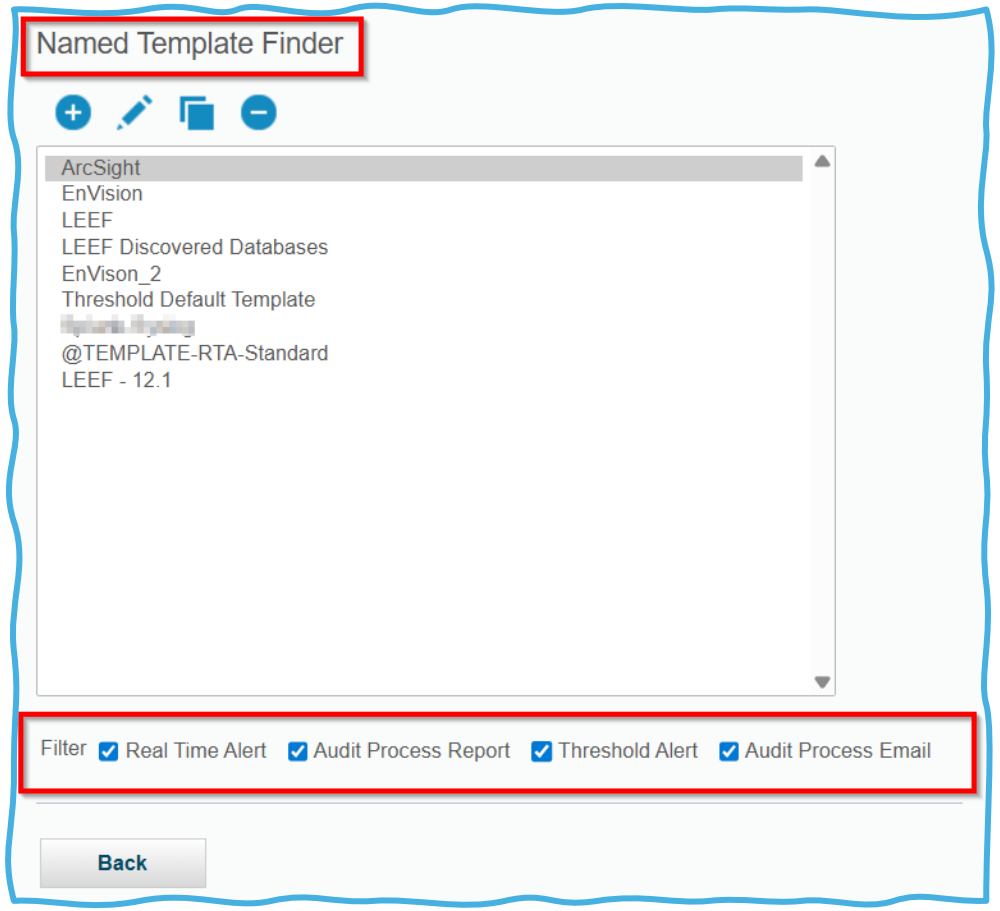


Polling interval should be smaller than the smallest “Run Frequency”

Message Template







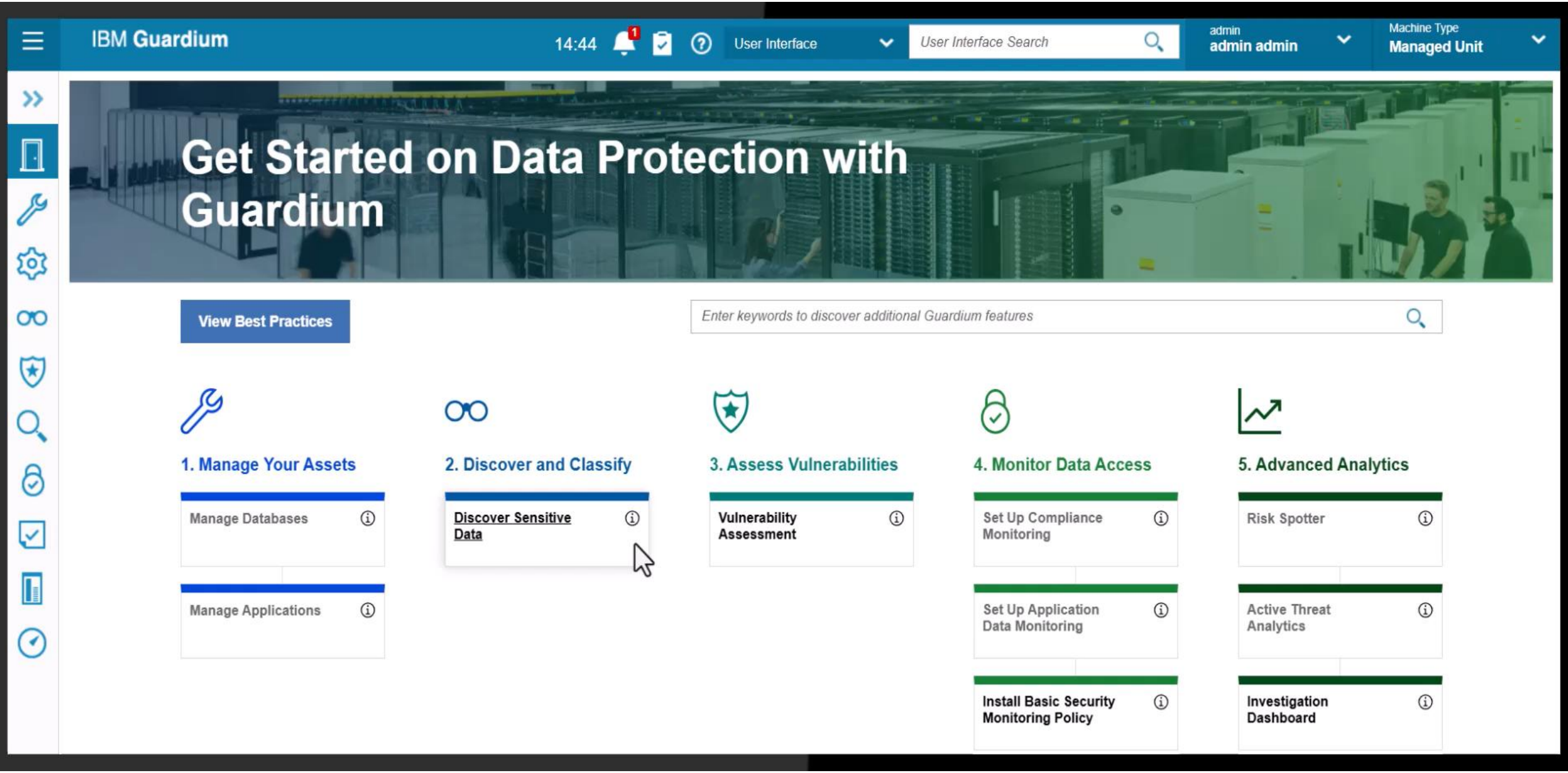
Alert message template variables

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

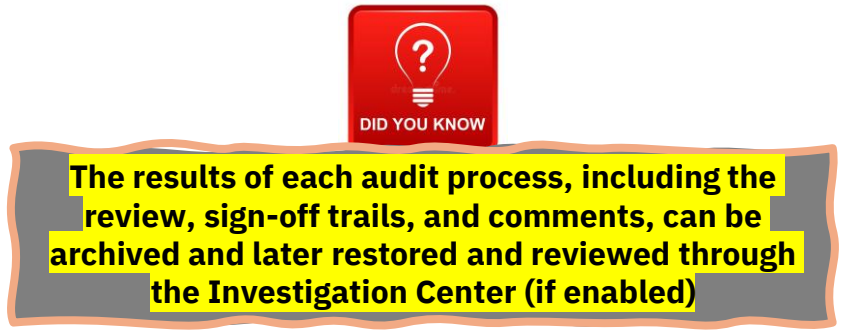


Audit Process

- 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

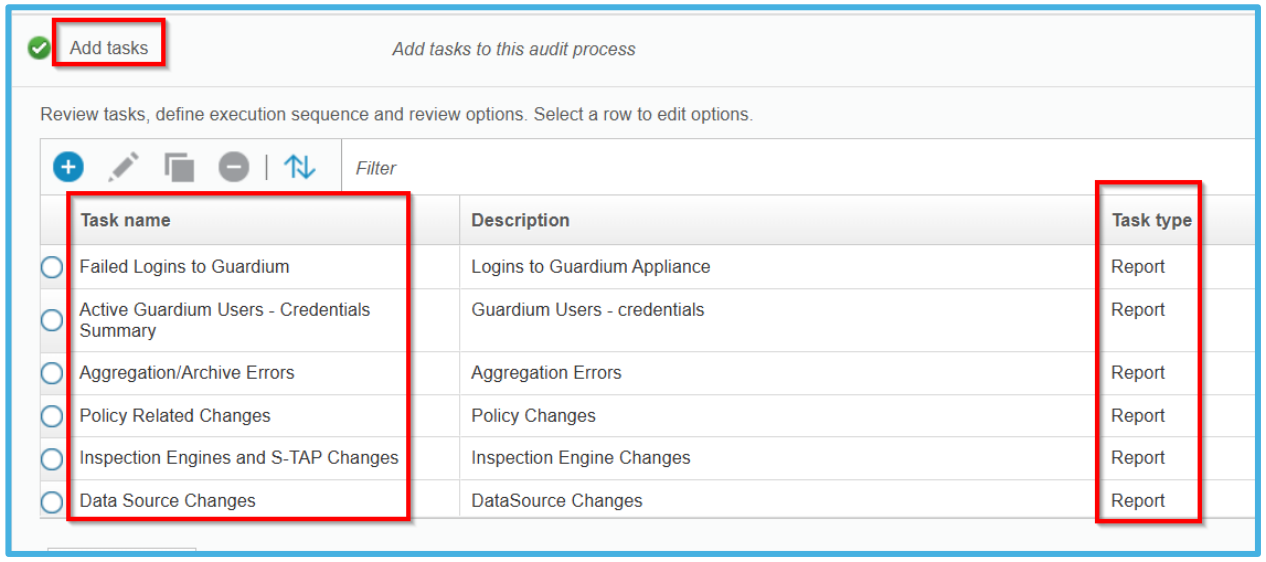
- Centralized tool for managing audit workflows
- Supports compliance tasks: discovery, assessment, monitoring, reporting
- Automates processes for privacy, governance, and regulatory needs
- Export options: Syslog, CSV, CEF
- Archiving via Investigation Center

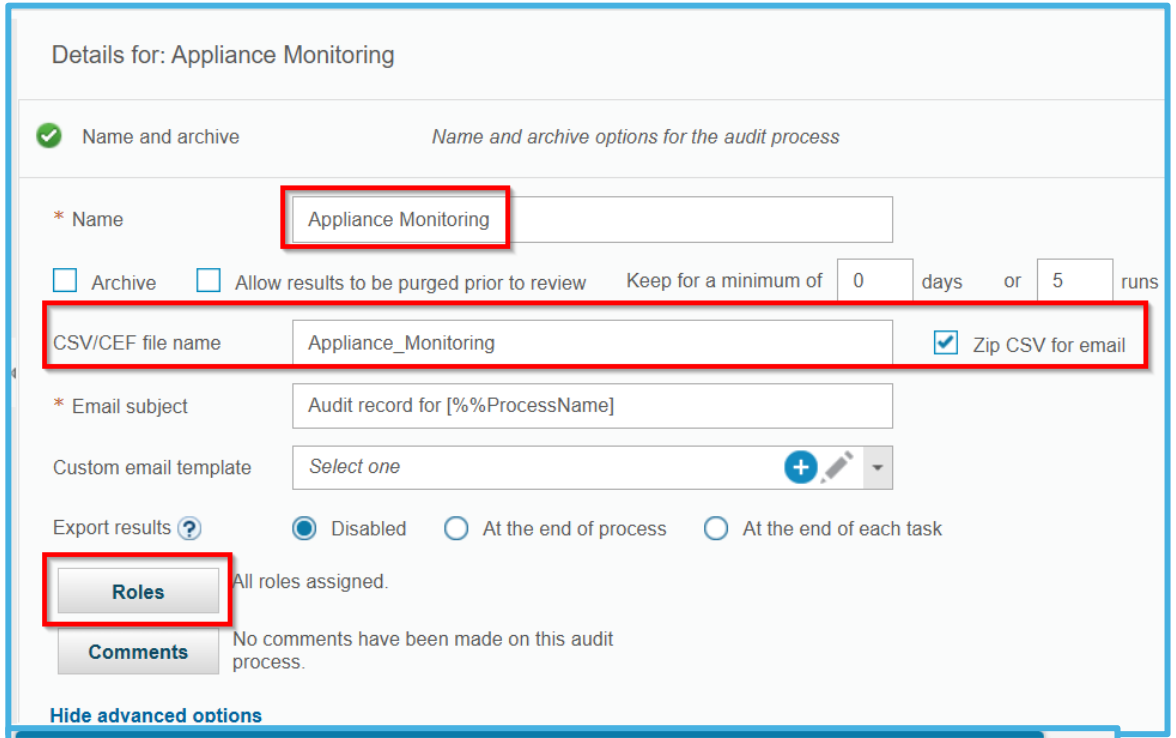


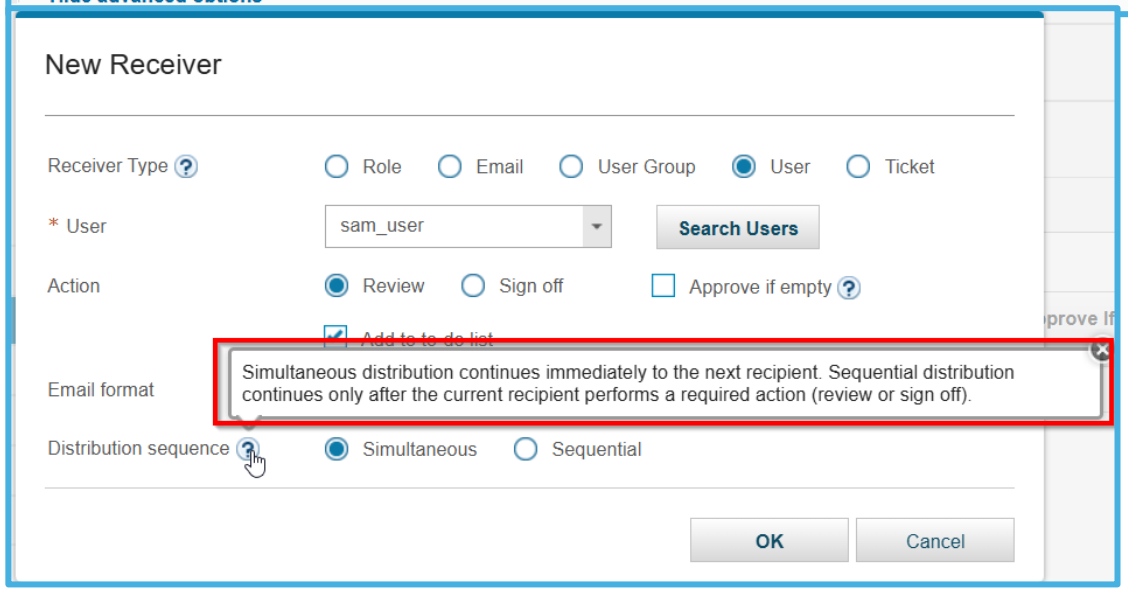
Audit Process (continued)

Elements of an Audit Process

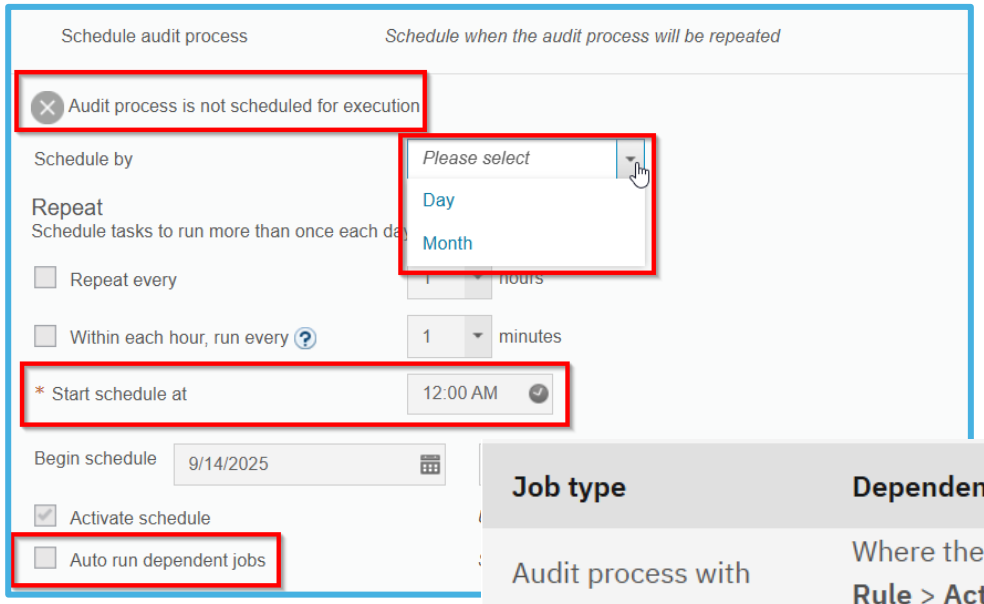
- process definition
- set of tasks
- distribution plan
- schedule
- workflow/ events & sign-off
- reports, export & archive

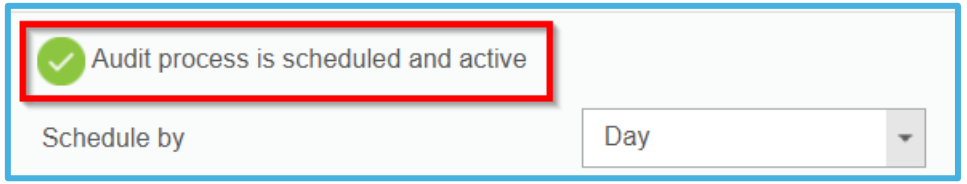


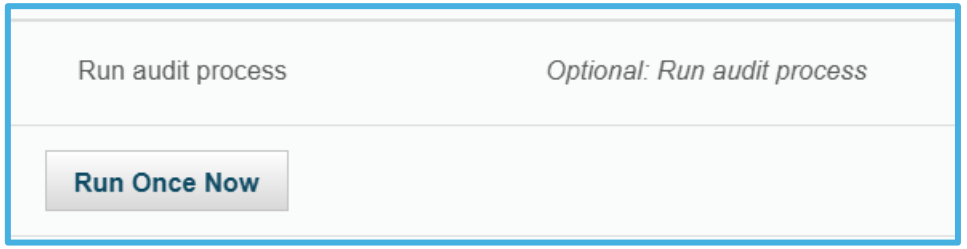




Audit Process Scheduling



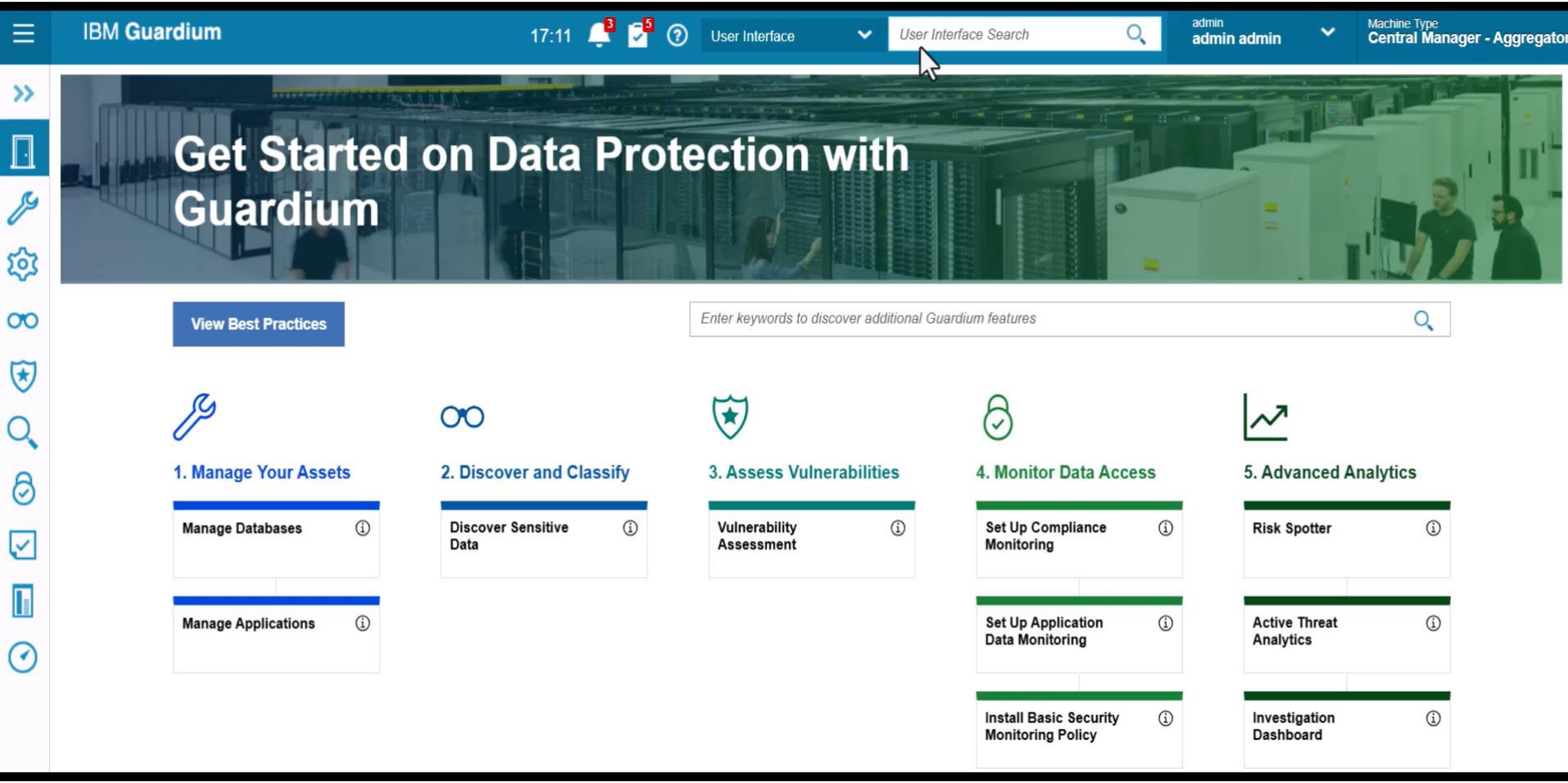




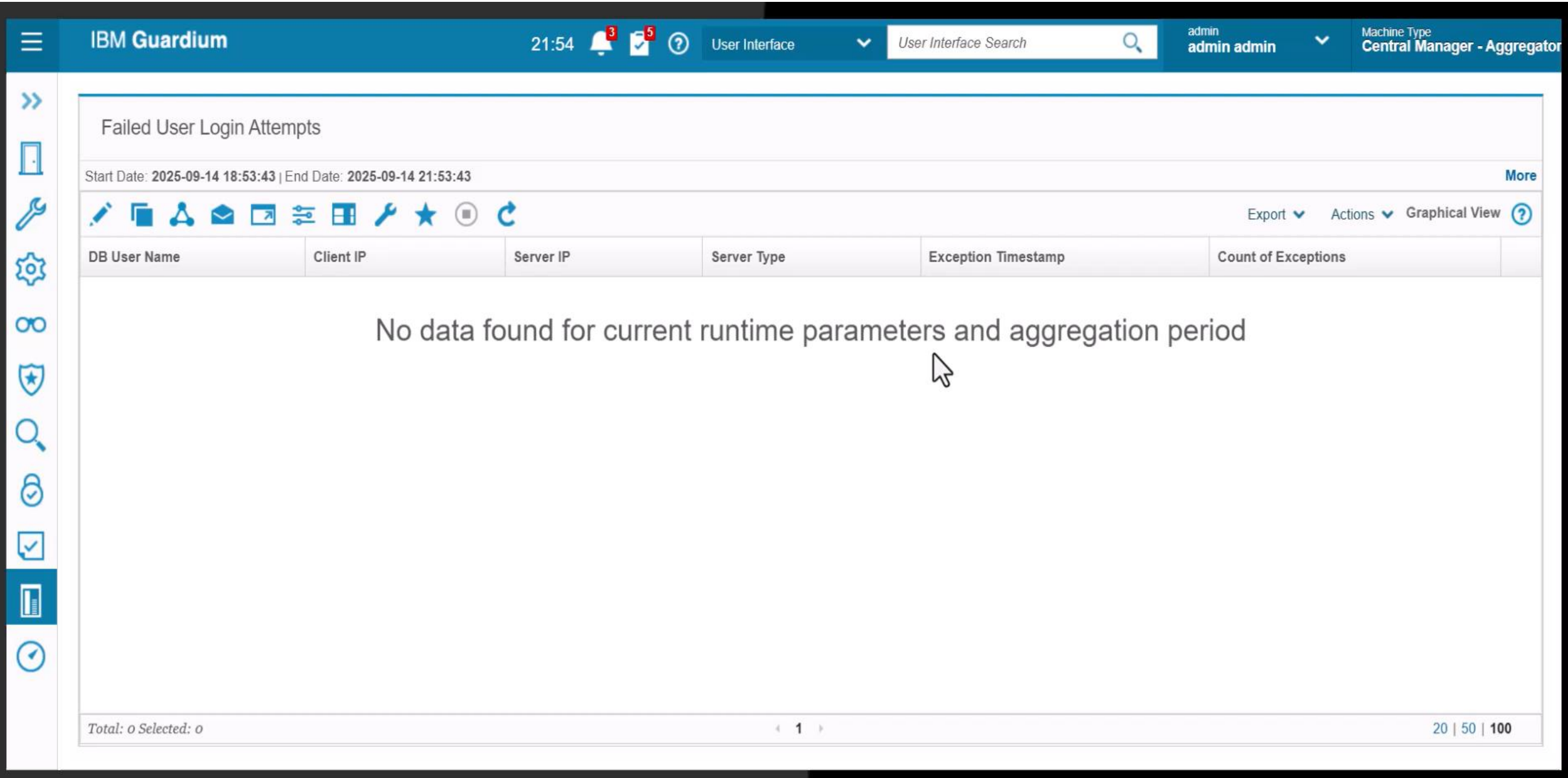
Aggregators are the best place to run audit processes

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 *Add To Group of Objects*, *Add To Group of Object/Fields* or *Add To Access Rule*. 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.

Build Audit Process & Execution



Adhoc Audit Process



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

Q&A

Any Questions?

- Register for-
18-September-2025
Thursday
Session 8: ibm.biz/IBMGE-S8

Aggregation/ Backup/ Restore

Thank you for your attention!

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

IBM