NetIQ Security Solutions for IBM i
TGDetect 2.1
Report Reference Guide
Revised August 2019

Legal Notice

Table of Contents

What's New in Version 2.1

No major modifications to TGDetect reports were produced in this release.

1. Introduction

This reference guide provides information about each build-it report in TGDetect.

Please refer to the TGDetect User Guide for detailed information and concepts on how to use TGDetect.

1.1. Report Categories

There are three categories of TGDetect reports:

- Activity History Reports
- Configuration Reports
- Change Reports

2. Activity History Reports

2.1. Activity History Reports

This section contains descriptions for the following reports:

- All Activity
- History Log Activity
- Message Queue Activity
- Command Monitor Activity
- Journal Monitor Activity
- SIEM Activity

2.2. All History Activity

This report displays all monitor activities.

The report is based on the following collector:

- Det_Act_History

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Activity History Reports).
5) Press **Enter**.

Note: The **Activity History Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **1** (All Activity).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Column	Description
Monitor Name	Name of the monitor
Monitor Library	Library to be monitored
Monitor Type	Type of monitor: ***CMD** - Command monitor

	***JRN** - Journal monitor ***MSGQ** - Message queue monitor ***QHST** - History log monitor ***SIEM** - Journal archival monitor (used for batch jobs)
Rule ID	ID assigned to monitor rule
Event Timestamp	Time at which the monitor identified the system activity
Activity Type	Type of a system activity
Activity Status	Status of the system activity
Activity Timestamp	Time at which the system activity took place
Activity Details	Description of the system activity
Syslog IP Address	IP address of the Syslog (system log) server
Syslog Port	Port used to communicate to the Syslog
Syslog Protocol	Protocol used to communicate to the Syslog
Syslog Facility	Type of program logging the message
Syslog Severity	Severity of message as defined by Syslog
Job Number	Number assigned to the job
Job Name	Name assigned to the job
Message Severity	Severity of message
Message Queue	Name of message queue
Message Queue Library	Library in which the message queue resides
Message ID	ID assigned to the message
Program Name	Name of the program
System Name	IBM agent (system)
User Name	Name user who performed system activity

See Also

Activity History Reports

2.3. History Log Activity

This report displays a list of history log activities.

The report is based on the following collector:

- Det_Act_History

To run this report

1) Access the TGDetect main menu.

2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Activity History Reports).
5) Press **Enter**.

Note: The **Activity History Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **2** (History Log Activity).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Column	Description
Monitor Name	Name of the monitor
Monitor Library	Library to be monitored
Monitor Type	Type of monitor: ***QHST** - History log monitor
Rule ID	ID assigned to monitor rule
Event Timestamp	Time at which the monitor identified the system activity
Activity Type	Type of a system activity
Activity Status	Status of the system activity
Activity Timestamp	Time at which the system activity took place
Activity Details	Description of the system activity
Syslog IP Address	IP address of the Syslog (system log) server
Syslog Port	Port used to communicate to the Syslog
Syslog Protocol	Protocol used to communicate to the Syslog
Syslog Facility	Type of program logging the message
Syslog Severity	Severity of message as defined by Syslog
Job Number	Number assigned to the job
Job Name	Name assigned to the job
Message Severity	Severity of message
Message Queue	Name of the message queue
Message Queue Library	Library in which the message queue resides
Message ID	ID assigned to the message

Program Name	Name of the program
System Name	IBM agent (system)
User Name	Name user who performed system activity

See Also

Activity History Reports

2.4. Message Queue Activity

This report displays a list of message queue activities.

The report is based on the following collector:

- Det_Act_History

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Activity History Reports).
5) Press **Enter**.

Note: The **Activity History Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **3** (Message Queue Activity).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Column	Description
Monitor Name	Name of the monitor
Monitor Library	Library to be monitored
Monitor Type	Type of monitor: ***MSGQ** - Message queue monitor
Rule ID	ID assigned to monitor rule
Event Timestamp	Time at which the monitor identified the system activity
Activity Type	Type of a system activity

Activity Status	Status of the system activity
Activity Timestamp	Time at which the system activity took place
Activity Details	Description of the system activity
Syslog IP Address	IP address of the Syslog (system log) server
Syslog Port	Port used to communicate to the Syslog
Syslog Protocol	Protocol used to communicate to the Syslog
Syslog Facility	Type of program logging the message
Syslog Severity	Severity of message as defined by Syslog
Job Number	Number assigned to the job
Job Name	Name assigned to the job
Message Severity	Severity of message
Message Queue	Name of message queue
Message Queue Library	Library in which the message queue resides
Message ID	ID assigned to the message
Program Name	Name of the program
System Name	IBM agent (system)
User Name	Name user who performed system activity

See Also

Activity History Reports

2.5. Command Monitor Activity

This report displays a list of command monitor activities.

The report is based on the following collector:

- Det_Act_History

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Activity History Reports).
5) Press **Enter**.

Note: The **Activity History Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **4** (Command Monitor Activity).
7) Press **Enter**.

8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Column	Description
Monitor Name	Name of the monitor
Monitor Library	Library to be monitored
Monitor Type	Type of monitor: ***CMD** - Command monitor
Rule ID	ID assigned to monitor rule
Event Timestamp	Time at which the monitor identified the system activity
Activity Type	Type of a system activity
Activity Status	Status of the system activity
Activity Timestamp	Time at which the system activity took place
Activity Details	Description of the system activity
Syslog IP Address	IP address of the Syslog (system log) server
Syslog Port	Port used to communicate to the Syslog
Syslog Protocol	Protocol used to communicate to the Syslog
Syslog Facility	Type of program logging the message
Syslog Severity	Severity of message as defined by Syslog
Job Number	Number assigned to the job
Job Name	Name assigned to the job
Message Severity	Severity of message
Message Queue	Name of message queue
Message Queue Library	Library in which the message queue resides
Message ID	ID assigned to the message
Program Name	Name of the program
System Name	IBM agent (system)
User Name	Name user who performed system activity

See Also

Activity History Reports

2.6. Journal Monitor Activity

This report displays a list of journal monitor activities.

The report is based on the following collector:

- Det_Act_History

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Activity History Reports).
5) Press **Enter**.

Note: The **Activity History Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **5** (Journal Monitor Activity).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Column	Description
Monitor Name	Name of the monitor
Monitor Library	Library to be monitored
Monitor Type	Type of monitor: ***JRN** - Journal monitor
Rule ID	ID assigned to monitor rule
Event Timestamp	Time at which the monitor identified the system activity
Activity Type	Type of a system activity
Activity Status	Status of the system activity
Activity Timestamp	Time at which the system activity took place
Activity Details	Description of the system activity
Syslog IP Address	IP address of the Syslog (system log) server
Syslog Port	Port used to communicate to the Syslog
Syslog Protocol	Protocol used to communicate to the Syslog
Syslog Facility	Type of program logging the message

Syslog Severity	Severity of message as defined by Syslog
Job Number	Number assigned to the job
Job Name	Name assigned to the job
Message Severity	Severity of message
Message Queue	Name of the message queue
Message Queue Library	Library in which the message queue resides
Message ID	ID assigned to the message
Program Name	Name of the program
System Name	IBM agent (system)
User Name	Name user who performed system activity

See Also

Activity History Reports

2.7. SIEM Activity

This report displays a list of SIEM (Security Information and Event Management) activities.

The report is based on the following collector:

- Det_Act_History

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Activity History Reports).
5) Press **Enter**.

Note: The **Activity History Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **6** (SIEM Activity).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Column	Description
Monitor Name	Name of the monitor

Monitor Library	Library to be monitored
Monitor Type	Type of monitor: ***SIEM** - Journal archival monitor (used for batch jobs)
Rule ID	ID assigned to monitor rule
Event Timestamp	Time at which the monitor identified the system activity
Activity Type	Type of a system activity
Activity Status	Status of the system activity
Activity Timestamp	Time at which the system activity took place
Activity Details	Description of the system activity
Syslog IP Address	IP address of the Syslog (system log) server
Syslog Port	Port used to communicate to the Syslog
Syslog Protocol	Protocol used to communicate to the Syslog
Syslog Facility	Type of program logging the message
Syslog Severity	Severity of message as defined by Syslog
Job Number	Number assigned to the job
Job Name	Name assigned to the job
Message Severity	Severity of message
Message Queue	Name of message queue
Message Queue Library	Library in which the message queue resides
Message ID	ID assigned to the message
Program Name	Name of the program
System Name	IBM agent (system)
User Name	Name user who performed system activity

See Also

Activity History Reports

3. Configuration Reports

3.1. Configuration Reports

This section of contains descriptions for the following reports:

- Default Settings
- Monitor Master
- SIEM Providers
- Message Queue Rules
- Command Monitor Rules
- Message Queue and Command Alerts
- Journal Monitor Rules
- Journal Monitor Alerts
- Journal Monitor Rules and SIEM

3.2. Defaults Settings

This report displays the default settings for monitors.

The report is based on the following collector:

- Det_Defaults

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Configuration Reports).
5) Press **Enter**.

Note: The **Configuration Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **1** (Defaults Settings).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Column	Description
Audit Status	Status of auditing **Note**: Auditing must be enabled (***YES**) to capture data for reporting purposes

Audit Journal Name	Name of journal
Audit Journal Library	Library in which journal resides
Audit Entry Type	Audit journal type
Collection Interval QHST	How often to collect data for the history log monitor
Collection Interval MSGQ	How often to collect data for the message queue monitor
Collection Interval CMD	How often to collect data for the command monitor
Collection Interval JRN	How often to collect data for the journal monitor
Collection Interval SIEM	How often to collect data for the SIEM (Security Information and Event Management) monitor
SIEM Method	Method used for SIEM data sharing
SIEM IP Address	IP address of the SIEM
SIEM Port	Port used for communication with SIEM
Enable SSL	Whether SSL is enabled
Alert User Profile	Sending of system notification
Email Origination User	Sending of email notification
SMTP Trap OID	SMTP Trap object identifier

See Also

Configuration Reports

3.3. Monitor Master

This report displays the complete list of monitors (built-in and custom).

The report is based on the following collector:

- Det_Mon_Master

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Configuration Reports).
5) Press **Enter**.

Note: The **Configuration Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **2** (Monitor Master).

7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Column	Description
Monitor Name	Name of the monitor
Monitor Library	Library to be monitored
Monitor Type	Type of monitor: ***CMD** - Command monitor ***JRN** - Journal monitor ***MSGQ** - Message queue monitor ***QHST** - History log monitor ***SIEM** - Journal archival monitor (used for batch jobs)
Monitor Description	Description of monitor
Monitor Protect	Whether monitor is internal (built-in): **Note**: Internal monitors are shipped with the product and cannot be deleted compare to custom message queue monitors which can be deleted. **Y** - Internal (cannot be deleted) **N** - Custom (can be deleted)
Last Processed Status	Time at which data was last collected
Alerts Processed Today	Number of alerts triggered today
Alerts Processed This Month	Number of alerts triggered this month
Alerts Processed This Year	Number of alerts triggered this year
Monitor Job Name	Name assigned to the job
Monitor Job User	User who performed the job
Monitor Job Number	Number assigned to the job

See Also

Configuration Reports

3.4. SIEM Providers

This report displays the list of SIEM (Security Information and Event Management) providers.

The report is based on the following collector:

- Det_SIEM_Providers

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Configuration Reports).
5) Press **Enter**.

Note: The **Configuration Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **3** (SIEM Providers).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Column	Description
Syslog Provider Name	Name of Syslog provider
Syslog Provider Description	Description of Syslog provider
Syslog IP Address	IP address for Syslog server
Syslog Port	Port used to communicate with Syslog
Syslog Protocol	Protocol used to communicate with Syslog
Message Log Format	Format in which messages are communicated to Syslog
Syslog Facility	Type of program logging the message
Syslog Severity	Severity of message

See Also

Configuration Reports

3.5. Message Queue Rules

This report displays the list of message queue monitor rules.

The report is based on the following collector:

- Det_Msq_Rules

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Configuration Reports).
5) Press **Enter**.

Note: The **Configuration Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **4** (Message Queue Rules).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Column	Description
Rule ID	ID assigned to the rule
Rule Name	Name assigned to the rule
Calendar Name	Calendar that defines when the rule is valid
Alerts Processed Today	Number of alerts triggered today
Alerts Processed This Month	Number of alerts triggered this month
Alerts Processed This Year	Number of alerts triggered this year
Message Queue	Name of message queue
Message Queue Library	Library in which the message queue resides
Message ID	ID assigned to the message
Message File	Name of message file object
Message File Library	Library in which message file object resides
Filter Sequence	Sequence in which rules are applied (in increments of 10)
Before Nesting Lvl	Character used to begin a nested filter (open parenthesis)
And OR	Boolean operator used in rule definition
Field Name	Field to be analyzed using the rule
Condition	Condition used in the rule definition
Value	Field value used in the rule definition
After Nesting Lvl	Character used to end a nested filter (close parenthesis)

Message Field Compare	Identifies whether a field-level filter exists **Note**: Field-level filters all you to apply additional granularity to your monitor rules. **Y** - Field-level filter exists **N** - No field-level filter exits
Message Omit or Select	Identifies whether the rule criteria is used for selecting or omitting: **S** - Rule criteria used to identify messages to include (trigger alerts) **O** - Rule criteria used to identify messages to exclude (should not trigger alerts)
Message Reply?	Identifies whether a reply exists. Some actions require a reply in order to execute a follow-up action. **Note**: This allows you to set up the required reply to ensure that the workflow is not hindered.

See Also

Configuration Reports

3.6. Command Monitor Rules

This report displays the list of command monitor rules.

The report is based on the following collector:

- Det_Cmd_Rules

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Configuration Reports).
5) Press **Enter**.

Note: The **Configuration Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **5** (Command Monitor Rules).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Column	Description
Rule ID	ID assigned to the rule
Rule Name	Name assigned to the rule

Calendar Name	Calendar that defines when the rule is valid **Note**: ***NONE** appears if no calendar is applicable.
Alerts Processed Today	Number of alerts triggered today
Alerts Processed This Month	Number of alerts triggered this month
Alerts Processed This Year	Number of alerts triggered this year
Command Name	Name of command to be monitor
Command Library	Name of library to be monitor
Command User	Name of user to be monitor

See Also

Configuration Reports

3.7. Message Queue and Command Alerts

This report displays the list of message queue and command alerts.

The report is based on the following collector:

- Det_Msq_Cmd_Alr

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Configuration Reports).
5) Press **Enter**.

Note: The **Configuration Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **6** (Message Queue and Command Alerts).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Note: The fields populated are dependent on the alert type.

Column	Description
Monitor Name	Name of the monitor
Monitor Library	Library to be monitored

Monitor Type	Type of monitor: ***CMD** - Command monitor ***MSGQ** - Message queue monitor ***QHST** - History log monitor
Rule Name	Name assigned to the monitor rule
Alert Sequence	Sequence in which alerts are to be sent
Alert Type	Type of alert to be sent: ***EMAIL** - Send an email alert to a specific user/group ***MSG** - Send a system message (message that appears when a user logs into the system) ***CMD** - Execute a command ***SYSLOG** - Send a notification to the system archive ***EMAILDIST** - Send an email alert to a specific user (legacy IBM method of sending email alerts) ***TGCENTRAL** - Send a notification to TGCentral
Forward Message Queue	Name of message queue
Forward Message Queue Library	Library in which message queue resides
Email Address	Email address of the designated recipient
Email Message	Email message to be sent to the designated recipient
Command to Execute	Command to be executed (as defined by monitor rule definition)
SNMP Trap ID	SMTP Trap object identifier
SIEM Name	Name of the SIEM
Alert Criteria Volume	Number of alert events required to trigger a notification. **Alternatively**, enter ***ALL** to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the **Event Frequency** field.
Alert Criteria Frequency	Frequency of alert events required to trigger a notification. This field works in conjunction with the **Number of Events** field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1-hour period.
Alert Criteria Measurement	Enter the frequency unit: **MIN** - Minutes **HR** - Hours **DAYS** - Days

Alert Criteria First Processed Time	Time at which first alert was sent
Alert Criteria Alerts in Period	Number of alerts sent

See Also

Configuration Reports

3.8. Journal Monitor Rules

This report displays the list of journal monitor rules.

The report is based on the following collector:

- Det_JrnMon_Rules

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Configuration Reports).
5) Press **Enter**.

Note: The **Configuration Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **7** (Journal Monitor Rules).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Column	Description
Journal Name	Name of journal to be monitored
Journal Library	Library in which journal resides
Journal Code	Code that identifies the type of journal entry
Journal Type	Code that identifies the type of journal
Calendar Name	Calendar that defines when the rule is valid **Note**: ***NONE** appears if no calendar is applicable.
Journal Alert	Identifies whether an alter has been defined
Journal Filter	Identifies whether a filter has been defined

Alerts Processed Today	Number of alerts triggered today
Alerts Processed This Month	Number of alerts triggered this month
Alerts Processed This Year	Number of alerts triggered this year

See Also

Configuration Reports

3.9. Journal Monitor Alerts

This report displays the list of journal monitor alerts.

The report is based on the following collector:

- Det_JrnMon_Alerts

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Configuration Reports).
5) Press **Enter**.

Note: The **Configuration Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **8** (Journal Monitor Alerts).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Note: The fields populated are dependent on the alert type.

Column	Description
Journal Name	Name of journal to be monitored
Journal Library	Library in which journal resides
Journal Code	Code that identifies the type of journal entry
Journal Type	Code that identifies the type of journal
Alert Sequence	Sequence in which alerts are to be sent
Alert Type	Type of alert to be sent: ***EMAIL** - Send an email alert to a specific user/group

	***MSG** - Send a system message (message that appears when a user logs into the system) ***CMD** - Execute a command ***SYSLOG** - Send a notification to the system archive ***EMAILDIST** - Send an email alert to a specific user (legacy IBM method of sending email alerts) ***TGCENTRAL** - Send a notification to TGCentral
Forward Message Queue	Name of message queue
Forward Message Queue Library	Library in which message queue resides
Email Address	Email address of the designated recipient
Email Message	Email message to be sent to the designated recipient
Command to Execute	Command to be executed (as defined by monitor rule definition)
SNMP Trap ID	SMTP Trap object identifier
SIEM Name	Name of the SIEM
Alert Criteria Volume	Number of alert events required to trigger a notification **Alternatively**, enter ***ALL** to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the **Event Frequency** field.
Alert Criteria Frequency	Frequency of alert events required to trigger a notification. This field works in conjunction with the **Number of Events** field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1-hour period.
Alert Criteria Measurement	Enter the frequency unit: **MIN** - Minutes **HR** - Hours **DAYS** - Days
Alert Criteria First Processed Time	Time at which first alert was sent
Alert Criteria Alerts in Period	Number of alerts sent

See Also

Configuration Reports

3.10. Journal Monitor Rules for SIEM

This report displays the list of journal monitor rules for SIEM (Security Information and Event Management).

The report is based on the following collector:

- Det_Jrn_SIEM_Rules

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Configuration Reports).
5) Press **Enter**.

Note: The **Configuration Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **9** (Journal Monitor Rules for SIEM).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Column	Description
Journal Name	Name of journal to be monitored
Journal Library	Library in which journal resides
Journal Code	Code that identifies the type of journal entry
Journal Type	Code that identifies the type of journal
Filter Sequence	Sequence in which filters (rules) are to be applied
Before Nesting Lvl	Character used to begin a nested filter (open parenthesis)
And OR	Boolean operator used in rule definition
Field Name	Field to be analyzed using the rule
Condition	Condition used in the rule definition
Value	Field value used in the rule definition
After Nesting Lvl	Character used to end a nested filter (close parenthesis)
Field Name	Name of field to be communicated with SIEM
Field Sequence	Sequence in which fields should be communicated to SIEM
Secondary Field?	** This field is reserved for future use **

See Also

Configuration Reports

4. Change Reports

4.1. Change Reports

This section of contains descriptions for the following reports:

- Default Setting Changes
- SIEM Provider Changes
- Msg Queue Rule Detail Changes
- Msg Queue Rule Header Changes
- Msg Queue and Command Alert Changes
- Cmd Monitor Rule Header Changes
- Journal Monitor Rule Detail Changes
- Journal Monitor Rule SIEM Changes

4.2. Detect Defaults Changes

This report displays the list of changes made to the default settings.

The report is based on the following collector:

- Database_Auditing

To enable this report:

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **11** (TGDetect Defaults).
3) Press **Enter**.
4) Enter **Y** as the **Audit Configuration Changes** flag.
5) Press **Enter**.

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Change Reports).
5) Press **Enter**.

Note: The **Change Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **1** (Detect Defaults Changes).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Column	Description
Type	Type of journal entry
Timestamp	Time at which the activity was performed
Job Name	Name assigned to job
User Name	User how performed activity
Job Number	Number assigned to the job
Program Name	Name of the program
Program Library	Name of library in which the program resides
Object Name	Name of object
Library Name	Name of library in which the object resides
Member Name	Name of member
User Profile	Profile name assigned to user
System Name	IBM agent (System)
Remote Address	Remote address of agent
Audit Status	Status of auditing **Note**: Auditing must be enabled (***YES**) to capture data for reporting purposes
Audit Journal Name	Name of journal
Audit Journal Library	Library in which journal resides
Audit Entry Type	Audit journal type
Collection Interval QHST	How often to collect data for the history log monitor
Collection Interval MSGQ	How often to collect data for the message queue monitor
Collection Interval CMD	How often to collect data for the command monitor
Collection Interval JRN	How often to collect data for the journal monitor
Collection Interval SIEM	How often to collect data for the SIEM (Security Information and Event Management) monitor
SIEM Method *JSON/*SYSLOG	Method used to communicate with external system
SIEM IP Address	IP address of the SIEM (Security Information and Event Management)
SIEM Port	Port used for communication with SIEM
Enable SSL?	Whether SSL is enabled
Alert User Profile	Sending of system notification
Email Origination User	Sending of email notification

SMTP Trap OID	SMTP Trap object identifier

See Also

Change Reports

4.3. SIEM Providers Changes

This report displays list of changes made to SIEM (Security Information and Event Management) provider.

The report is based on the following collector:

- Database_Auditing

To enable this report:

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **11** (TGDetect Defaults).
3) Press **Enter**.
4) Enter **Y** as the **Audit Configuration Changes** flag.
5) Press **Enter**.

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Change Reports).
5) Press **Enter**.

Note: The **Change Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **2** (SIEM Providers Changes).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Column	Description

See Also

4.4. Message Queue Rules Detail Changes

This report displays the list of changes made to message queue rule details (i.e., compare rule, filter sequence, etc.).

The report is based on the following collector:

- Database_Auditing

To enable this report:

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **11** (TGDetect Defaults).
3) Press **Enter**.
4) Enter **Y** as the **Audit Configuration Changes** flag.
5) Press **Enter**.

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Change Reports).
5) Press **Enter**.

Note: The **Change Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **3** (Msg Queue Rules Header Changes).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Column	Description
Type	Type of journal entry
Timestamp	Time at which the activity was performed
Job Name	Name assigned to job
User Name	User how performed activity
Job Number	Number assigned to the job
Program Name	Name of the program
Program Library	Name of library in which the program resides

Object Name	Name of object
Library Name	Name of library in which the object resides
Member Name	Name of member
User Profile	Profile name assigned to user
System Name	Name assigned to server (agent)
Remote Address	IP address of remote server
Rule ID	ID assigned to the rule
Message Queue	Name of message queue
Message Queue Library	Library in which the message queue resides
Message ID	ID assigned to the message
Message File	Name of message file object
Message File Library	Library in which message file object resides
Filter Sequence	Sequence in which rules are applied (in increments of 10)
Before Nesting Lvl	Character used to begin a nested filter (open parenthesis)
And OR	Boolean operator used in rule definition
Field Name	Field to be analyzed using the rule
Condition	Condition used in the rule definition
Value	Field value used in the rule definition
After Nesting Lvl	Character used to end a nested filter (close parenthesis)

See Also

Change Reports

4.5. Message Queue Rules Header Changes

This report displays the list of changes made to message queue rule header (i.e., omit, select, reply, etc.).

The report is based on the following collector:

- Database_Auditing

To enable this report:

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **11** (TGDetect Defaults).
3) Press **Enter**.
4) Enter **Y** as the **Audit Configuration Changes** flag.
5) Press **Enter**.

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Change Reports).
5) Press **Enter**.

Note: The **Change Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **4** (Msg Queue Rules Details Changes).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Column	Description
Type	Type of journal entry
Timestamp	Time at which the activity was performed
Job Name	Name assigned to job
User Name	User how performed activity
Job Number	Number assigned to the job
Program Name	Name of the program
Program Library	Name of library in which the program resides
Object Name	Name of object
Library Name	Name of library in which the object resides
Member Name	Name of member
User Profile	Profile name assigned to user
System Name	Name assigned to server (agent)
Remote Address	IP address of remote server
Rule ID	ID assigned to the rule
Message Queue	Name of message queue
Message Queue Library	Library in which the message queue resides
Message ID	ID assigned to the message
Message File	Name of message file object
Message File Library	Library in which message file object resides

Message Field Compare	Identifies whether a field-level filter exists **Note**: field-level filters all you to apply additional granularity to your monitor rules. **Y** - Field-level filter exists **N** - No field-level filter exits
Message Omit or Select	Identifies whether the rule criteria is used for selecting or omitting: **S** - Rule criteria used to identify messages to include (trigger alerts) **O** - Rule criteria used to identify messages to exclude (should not trigger alerts)
Message Reply?	Identifies whether a reply exists. Some actions require a reply in order to execute a follow-up action. **Note**: This allows you to set up the required reply to ensure that the workflow is not hindered.

See Also

Change Reports

4.6. Message Queue and Command Alert Changes

This report displays the list of changes made to message queue and command alerts.

The report is based on the following collector:

- Database_Auditing

To enable this report:

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **11** (TGDetect Defaults).
3) Press **Enter**.
4) Enter **Y** as the **Audit Configuration Changes** flag.
5) Press **Enter**.

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Change Reports).
5) Press **Enter**.

Note: The **Change Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **5** (Msg Queue and Command Alerts Changes).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

Report Column Description

Column	Description
Type	Type of journal entry
Timestamp	Time at which the activity was performed
Job Name	Name assigned to job
User Name	User how performed activity
Job Number	Number assigned to the job
Program Name	Name of the program
Program Library	Name of library in which the program resides
Object Name	Name of object
Library Name	Name of library in which the object resides
Member Name	Name of member
User Profile	Profile name assigned to user
System Name	Name assigned to server (agent)
Remote Address	IP address of remote server
Rule ID	ID assigned to the rule
Monitor Name	Name of the monitor
Monitor Library	Library to be monitored
Monitor Type	Type of monitor: ***CMD** - Command monitor ***JRN** - Journal monitor ***MSGQ** - Message queue monitor ***QHST** - History log monitor ***SIEM** - Journal archival monitor (used for batch jobs)
Rule Name	Name assigned to the rule
Alert Sequence	Sequence in which alerts are to be sent
Alert Type	Type of alert to be sent: ***EMAIL** - Send an email alert to a specific user/group ***MSG** - Send a system message (message that appears when a user logs into the system) ***CMD** - Execute a command ***SYSLOG** - Send a notification to the system archive ***EMAILDIST** - Send an email alert to a specific user (legacy IBM method of sending email alerts) ***TGCENTRAL** - Send a notification to TGCentral

Forward Message Queue	Name of message queue
Forward Message Queue Library	Library in which message queue resides
Email Address	Email address of the designated recipient
Email Message	Email message to be sent to the designated recipient
Command to Execute	Command to be executed (as defined by monitor rule definition)
SNMP Trap ID	SMTP Trap object identifier
SIEM Name	Name of the SIEM
Alert Criteria Volume	Number of alert events required to trigger a notification. **Alternatively**, enter ***ALL** to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the **Event Frequency** field.
Alert Criteria Frequency	Frequency of alert events required to trigger a notification. This field works in conjunction with the **Number of Events** field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1 hour period.
Alert Criteria Measurement	Enter the frequency unit: **MIN** - Minutes **HR** - Hours **DAYS** - Days
Alert Criteria First Processed Time	Time at which first alert was sent
Alert Criteria Alerts in Period	Number of alerts sent

See Also

Change Reports

4.7. Command Monitor Rules Header Changes

This report displays the list of changes made to command rule headers.

The report is based on the following collector:

- Database_Auditing

To enable this report:

1) Access the TGDetect main menu.

2) At the **Selection or command** prompt, enter **11** (TGDetect Defaults).
3) Press **Enter**.
4) Enter **Y** as the **Audit Configuration Changes** flag.
5) Press **Enter**.

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Change Reports).
5) Press **Enter**.

Note: The **Change Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **6** (Cmd Monitor Rules Header Changes).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

See Also

Change Reports

4.8. Journal Monitor Rules SIEM Changes

This report displays the list of changes made journal monitor rules used for SIEM (Security Information and Event Management).

The report is based on the following collector:

- Database_Auditing

To enable this report:

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **11** (TGDetect Defaults).
3) Press **Enter**.
4) Enter **Y** as the **Audit Configuration Changes** flag.
5) Press **Enter**.

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Change Reports).
5) Press **Enter**.

Note: The **Change Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **7** (Journal Monitor Rules SIEM Changes).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

See Also

Change Reports

4.9. Journal Monitor Rules Details Changes

This report displays the list of changes made to journal monitor rule details.

The report is based on the following collector:

- Database_Auditing

To enable this report:

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **11** (TGDetect Defaults).
3) Press **Enter**.
4) Enter **Y** as the **Audit Configuration Changes** flag.
5) Press **Enter**.

To run this report

1) Access the TGDetect main menu.
2) At the **Selection or command** prompt, enter **20** (Reporting).
3) Press **Enter**.

Note: The **TGDetect Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Change Reports).
5) Press **Enter**.

Note: The **Change Reports** interface is displayed.

6) At the **Selection or command** prompt, enter **8** (Journal Monitor Rules SIEM Changes).
7) Press **Enter**.
8) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

See Also

Change Reports