PER SCHOLAS

Lesson 200.8 Creating Scheduled Reports and Alerts

PER SCHOLAS

Learning Objectives

At the end of this lesson, learners will be able to:

- Describe alerts.
- Create alerts.
- View triggered alerts.

PER SCHOLAS

Introduction

Alerts in Splunk enable proactive monitoring, allowing you to identify and respond to critical events or anomalies in your data.

By configuring alerts, you can stay informed and take timely actions based on specific conditions or events that are important to your business or operational needs.

Alerts use a saved search to look for events in real time or on a schedule.

Alerts trigger when search results meet specific conditions. You can use alert actions to respond when alerts trigger.

image: Freepik.com

8.3 Describe Alerts

The alerting workflow

Alerts **combine** a saved **search**, configurations for **type** and **trigger** conditions, and alert **actions**.

Here are some details about how the different parts of an alert work together:

- **Search: What do you want to track?**
  - Start with a search for the events you want to track. Save the search as an alert.
- **Alert type: How often do you want to check for events?**
  - Adjust the alert type to configure how often the search runs.
    - Use a **scheduled alert** to check for events on a **regular** basis.
    - Use a **real-time alert** to monitor for events **continuously**.

8.3 Describe Alerts (continued)

The alerting workflow

- **Alert trigger conditions and throttling: How often do you want to trigger an alert?**
  - An alert does not have to trigger every time it generates search results.
  - Set trigger conditions to manage when the alert triggers.
  - You can also throttle an alert to control how soon the next alert can trigger after an initial alert.
- **Alert Action: What happens when the alert triggers?**
  - When an alert triggers, it can initialize one or more alert actions.
  - An alert action can notify you of a triggered alert and help you start responding to it.
  - You can configure alert action frequency and type.

8.3 Describe Alerts (continued)

Alert types

- There are **two** alert types: **scheduled** and **real-time**.
- Alert **type definitions** are based on alert **search timing**.
- Depending on the **scenario**, you can configure **timing**, **triggering**, and other behaviors for **either** alert type.

Alert type	Scheduled	Real-time

image: screenshot, splunk Alerts

8.3 Describe Alerts (continued)

Alert type comparison

The following is a comparison of scheduled and real-time alerts.

Alert type	When it searches for events	Triggering options	Throttling options
Scheduled	Searches according to a schedule. Choose from the available timing options or use a cron expression to schedule the search.	Specify conditions for triggering the alert based on result or result field counts. When a set of search results meets the trigger conditions, the alert can trigger one time or once for each of the results.	Specify a time period for suppression.
Real-time	Searches continuously.	**Per-result**: Triggers every time there is a search result.	Specify a time period and optional field values for suppression.
Real-time	Searches continuously.	**Rolling time window**: Specify conditions for triggering the alert based on result or result field counts within a rolling time window. For example, a real-time alert can trigger whenever there are more than ten results in a five minute window.	Specify a time period for suppression.

image: https://docs.splunk.com/Documentation/SplunkCloud/9.0.2303/Alert/AlertTypesOverview

8.4 Create Alerts

Scheduled alert

Use a **scheduled alert** to search for **events** on a **regular basis** and monitor whether they meet **specific conditions**.

A scheduled alert is useful if immediate or real-time monitoring is **not** a priority.

Scenario:

An online retailer has a daily goal of 800 sales. An admin for the retailer creates a scheduled alert to monitor sales performance. The admin schedules the alert to search for sales events each day at 23:00. She configures the alert to trigger if the number of results is lower than 800.

8.4 Create Alerts (continued)

Scheduled alert

The admin enters the following search into the Splunk Search & Reporting App. It **counts** the **number** of **events** that contain the value **purchase** in the **action** field.

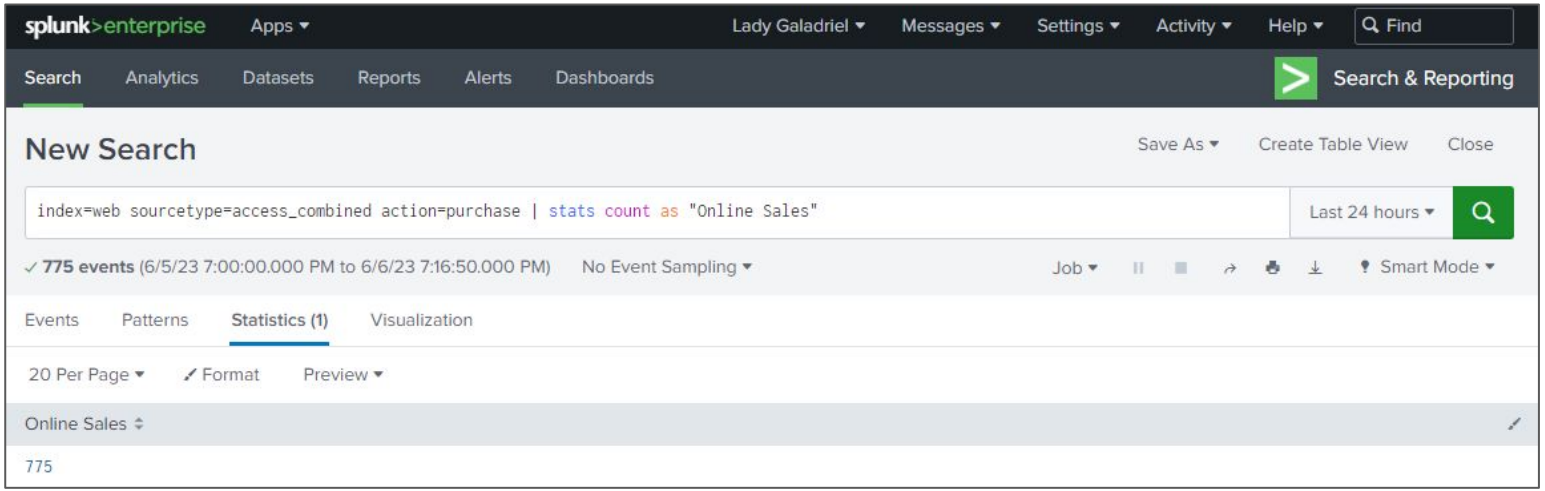


image: screenshot, splunk Search & Reporting app

PER SCHOLAS

8.4 Create Alerts (continued)

Scheduled alert

From the **Save As** drop-down menu, she selects **Alert.**

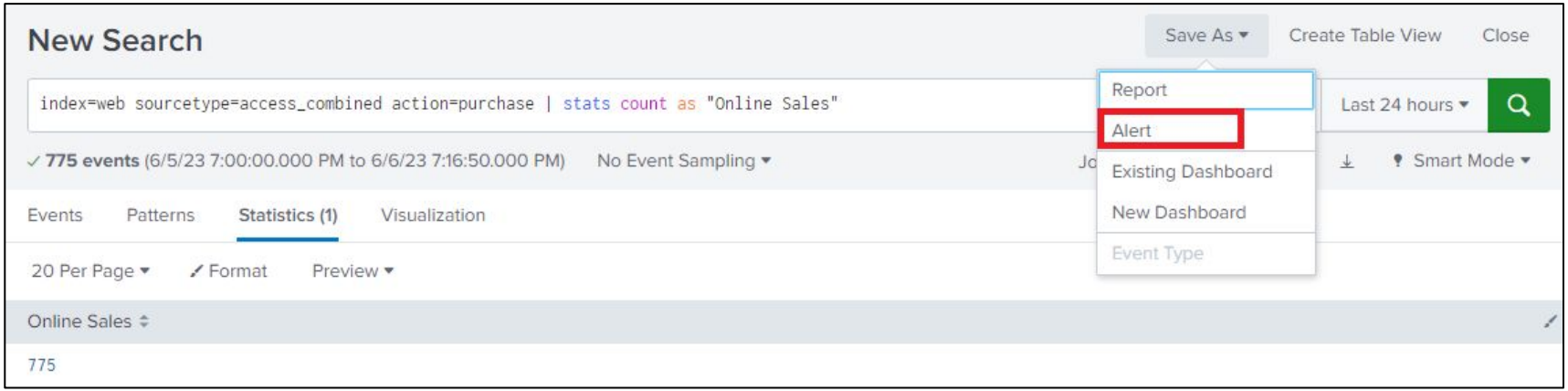


image: screenshot, splunk Search & Reporting app

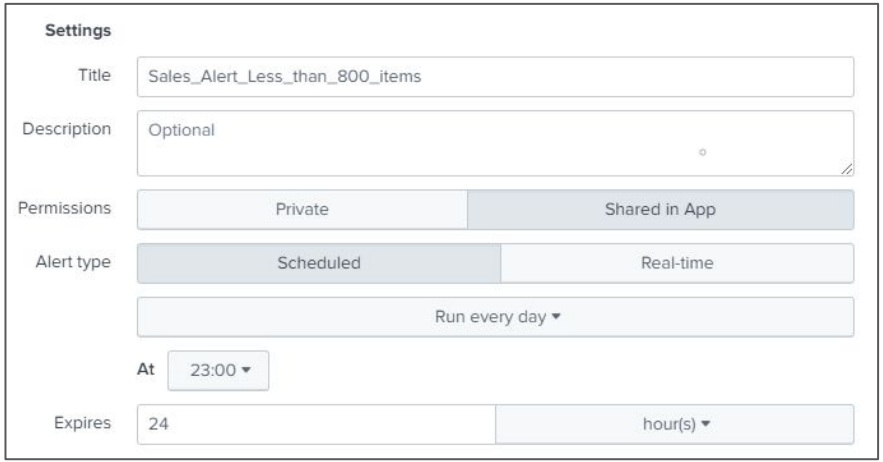
8.4 Create Alerts (continued)

Scheduled alert

There are many options available on the **Save As Alert** dialog box. Use a live Splunk environment to explore them all.

For **this** scenario - **Settings**:

- Title: **Sales_Alert_Less_than_800_items**
- Description: **Optional**
- Permissions: **Shared in App**
- Alert type: **Scheduled**
- Configure alert scheduling.
  - **Run every day At 23:00**
- Expires: **24 hour(s)**



The **Expires** setting controls the lifespan of triggered alert records, which appear on the Triggered Alerts page.

image: screenshot, splunk Search & Reporting app

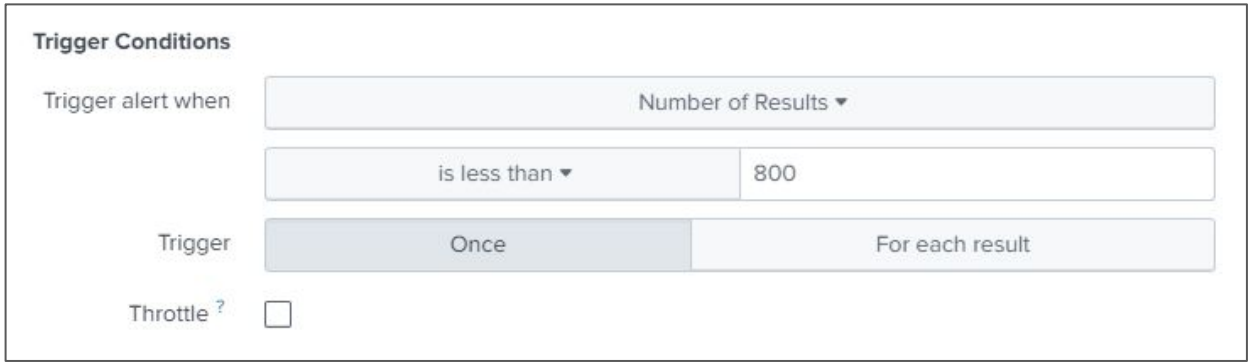
PER SCHOLAS

8.4 Create Alerts (continued)

Scheduled alert

For **this** scenario - **Trigger Conditions**:

- Trigger alert when: **Number of Results is less than 800**
- Trigger: **Once For each result**
- Throttle: **Uncheck**



The Throttle settings allow for suppressing subsequent alerts for a specified time period.

Throttle does not apply to this example.

image: screenshot, splunk Search & Reporting app

PER SCHOLAS

8.4 Create Alerts (continued)

Scheduled alert

For **this** scenario - **Trigger Actions**:

- **+ Add Actions**
  - When triggered: **Add to Triggered Alerts**
  - Severity: **Medium**
- Click **Save**.

Note: You can add one or more alert actions that should happen when the alert triggers.

Severity is a tag that is appended to the Alert in the Triggered Alerts page to help filter and locate alerts based on severity.

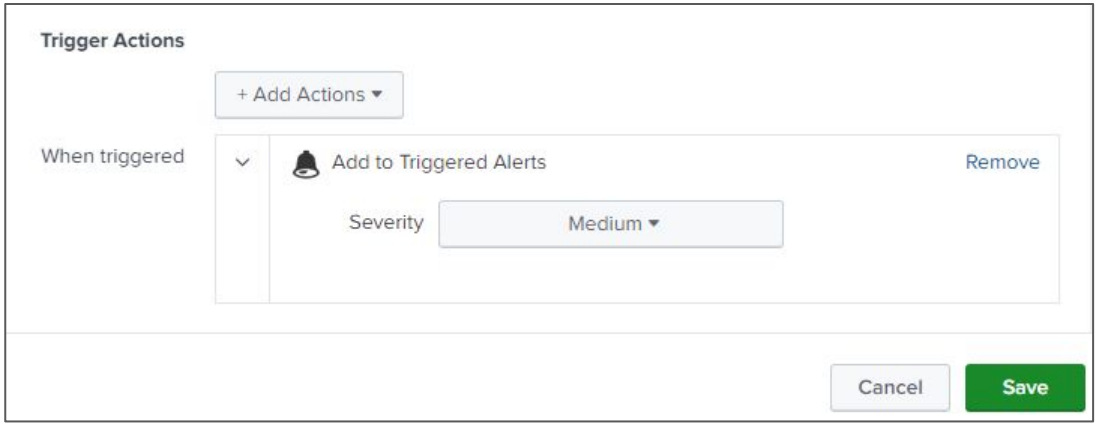


image: screenshot, splunk Search & Reporting app

8.4 Create Alerts (continued)

Scheduled alert

Alert has been saved:

- At this point, you can **edit** the Alert **Permissions**, continue **Editing** the Alert, or **View** the Alert.
- Click on the **View Alert** button.

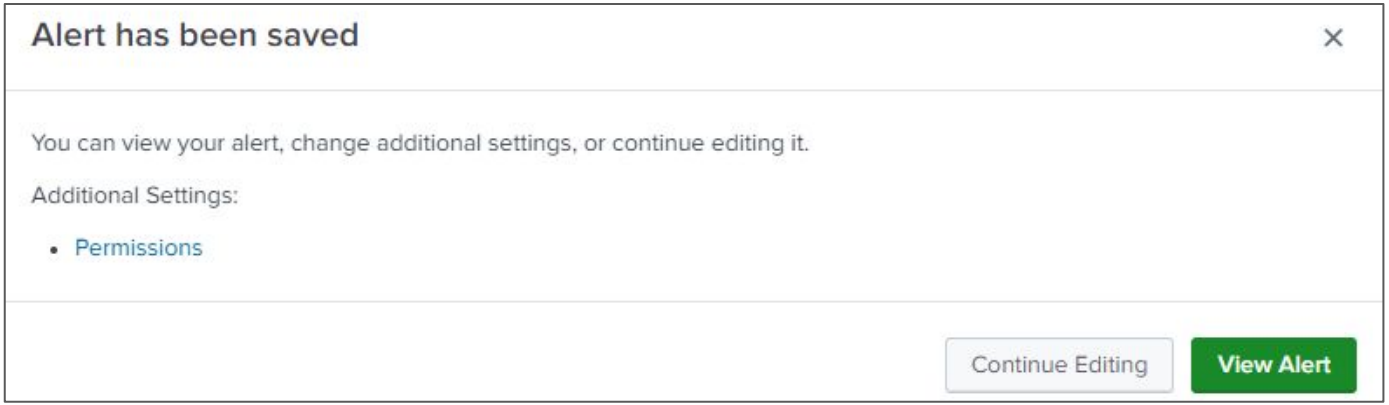


image: screenshot, splunk Search & Reporting app

8.4 Create Alerts (continued)

Scheduled alert

Viewing the **Sales_Alert_Less_than_800_items** Alert.

- You can **review** and **edit** the alert **settings**.

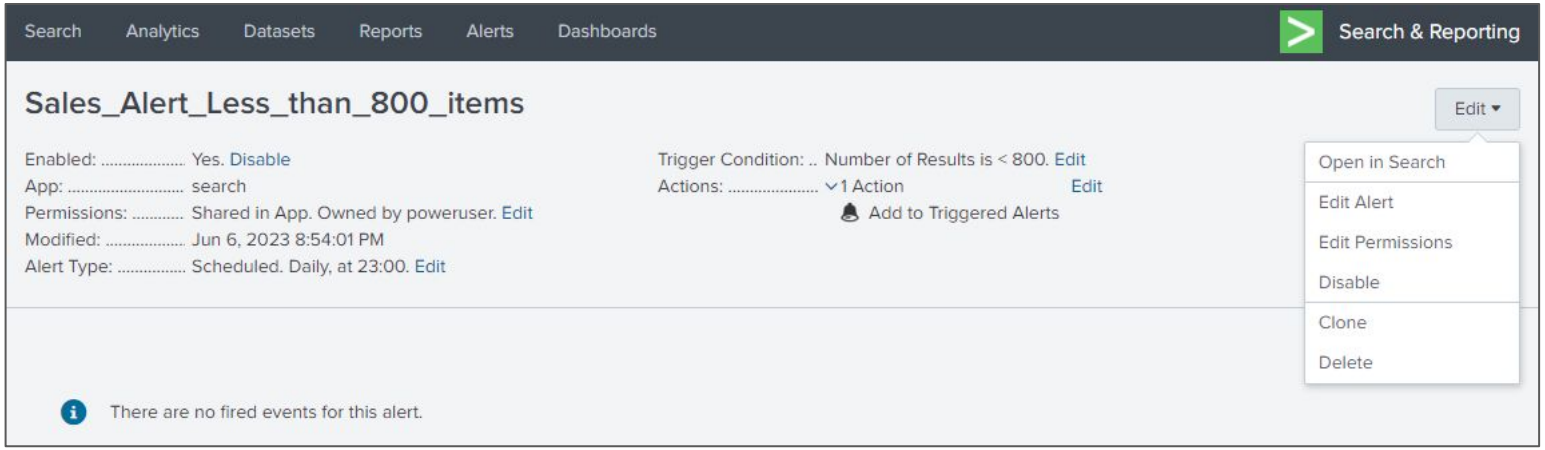


image: screenshot, splunk Search & Reporting app

8.4 Create Alerts (continued)

Differences between scheduled reports and alerts

- A scheduled report is like a scheduled or real-time alert in certain ways. You can schedule a report and set up an action that runs **each time** the scheduled report runs.
- The difference is as follows:
  - A **Scheduled report** runs its **action every time the report completes**.
  - A **Scheduled alert** runs its action **only** when it is **triggered by search results**.

8.4 Create Alerts (continued)

Real-time alerts

Real-time alerts **search** for events **continuously**. They can be useful in situations where **immediate monitoring** and responses are important. You can use real-time alerts that trigger once **per result** or only if certain conditions are met within a specific **rolling time window**.

- Use a real-time alert to monitor events or event patterns as they happen.

Per-result triggering

A real-time alert with a **per-result triggering condition** is sometimes known as a "**per-result alert.**"

- Use this alert type and **triggering** to search **continuously** for events and to **receive notifications** when events **occur**.

8.4 Create Alerts (continued)

Real-time alerts

Per-result triggering - example scenario:

- An admin wants to monitor a set of Web servers for HTTP Server error responses in real-time (Status 500 - 599).
- The admin sets up a real-time alert with a per-result trigger condition.
- If there is an issue with the server, the admin assumes that the server will generate many status 500 - 599 messages (one for every page request) and the system will be flooded with alerts.
- To avoid this, he throttles the alert to a one-hour suppression period, so that the alert will not be triggered for every server error response that occurs within one hour.

8.4 Create Alerts (continued)

Real-time alert

Per-result triggering - example scenario:

- The admin **searches** the **web index** for **values** that are **equal** to or **larger** than **500** in the **status** field for the **www1**, **www2**, and **www3** web servers.
- Next, the admin saves the search as an **Alert**.

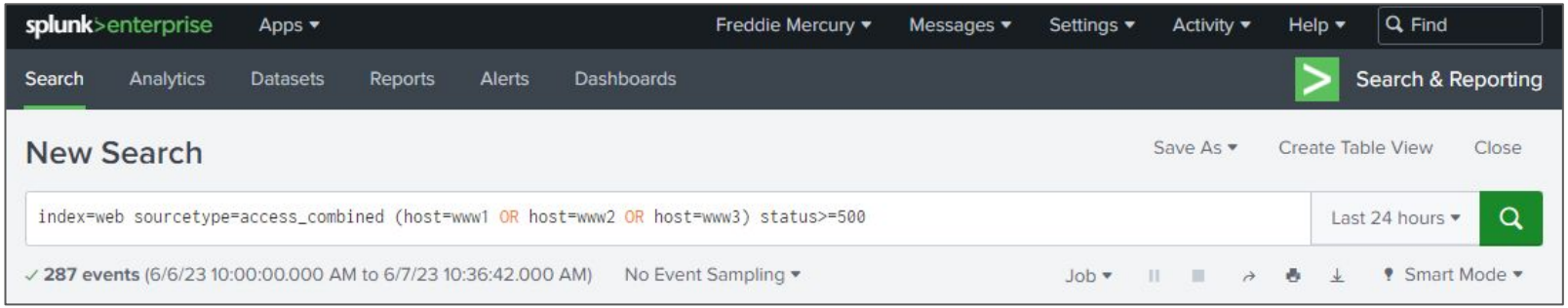


image: screenshot, splunk Search & Reporting app

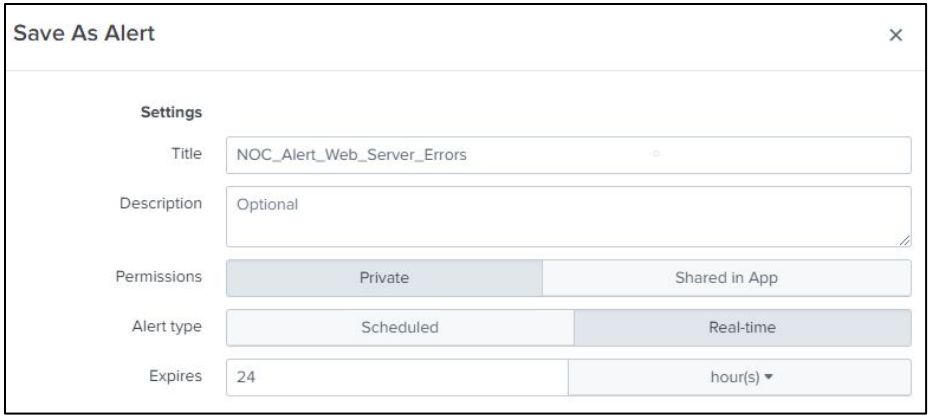
8.4 Create Alerts (continued)

Real-time alert - Per-result triggering.

There are many options available on the **Save As Alert** dialog box. Use a live Splunk environment to explore them all.

For **this** scenario - **Settings**:

- Title: **NOC_Alert_Web_Server_Errors**
- Description: **Optional**
- Permissions: **Private**
- Alert type: **Real-time**
- Expires: **24 hour(s)**



The Expires setting controls the lifespan of triggered alert records, which appear on the Triggered Alerts page.

image: screenshot, splunk Search & Reporting app

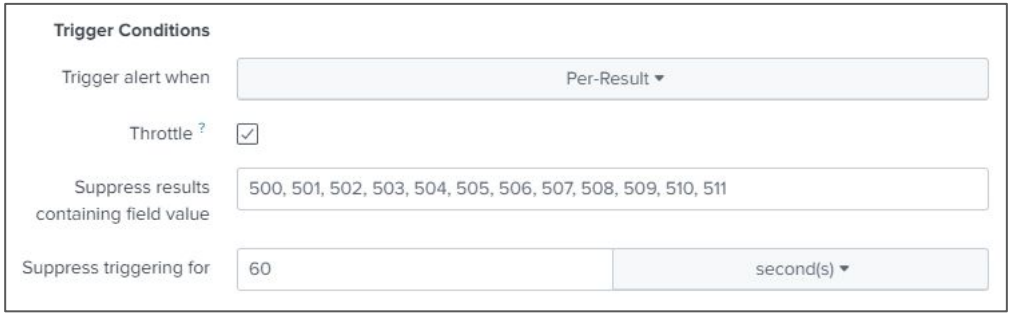
PER SCHOLAS

8.4 Create Alerts (continued)

Real-time alert - Per-result triggering.

For **this** scenario - **Trigger Conditions**:

- Trigger alert when: **Per-Result**
- Throttle: **Check**
- Suppress results containing field value: **500 - 511**
- Suppress triggering for: **60 minute(s)**



Within the Throttle settings, you can choose specific field values as conditions to suppress subsequent alerts.

In this case, only one alert will be triggered during a one-hour window for each status value between 500 and 511.

image: screenshot, splunk Search & Reporting app

PER SCHOLAS

8.4 Create Alerts (continued)

Real-time alert - Per-result triggering.

For **this** scenario - **Trigger Actions**:

- **+ Add Actions**
  - When triggered: **Add to Triggered Alerts**
  - Severity: **High**
- Click **Save**.

Note: In a real-world scenario, an admin may also want to send the alert via email to ensure resolving of the issue as soon as possible.

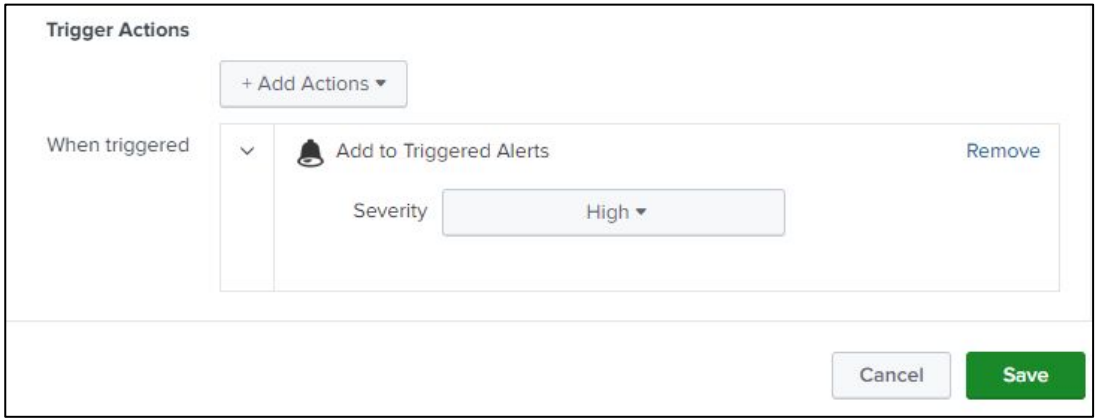


image: screenshot, splunk Search & Reporting app

8.4 Create Alerts (continued)

Rolling time window triggering

A real-time alert with **rolling time window triggering** is sometimes known as a "**rolling window alert.**"

This alert type and triggering are useful when a **specific time window** is an important part of the **event pattern** you are monitoring in **real time**.

8.4 Create Alerts (continued)

Real-time alerts

Rolling time window triggering - example scenario:

- An admin wants a notification whenever there are more than twenty failed login attempts in a five-minute window.
- The admin sets up a real-time alert to search for failed logins, and configures a rolling five-minute time window.
- The admin throttles the alert so that it triggers only once in an hour for failed logins.

8.4 Create Alerts (continued)

Real-time alert

Rolling time window triggering - example scenario:

- The admin **searches** the **security index** for the **values** Failed and password.
- Next, the admin saves the search as an **Alert**.

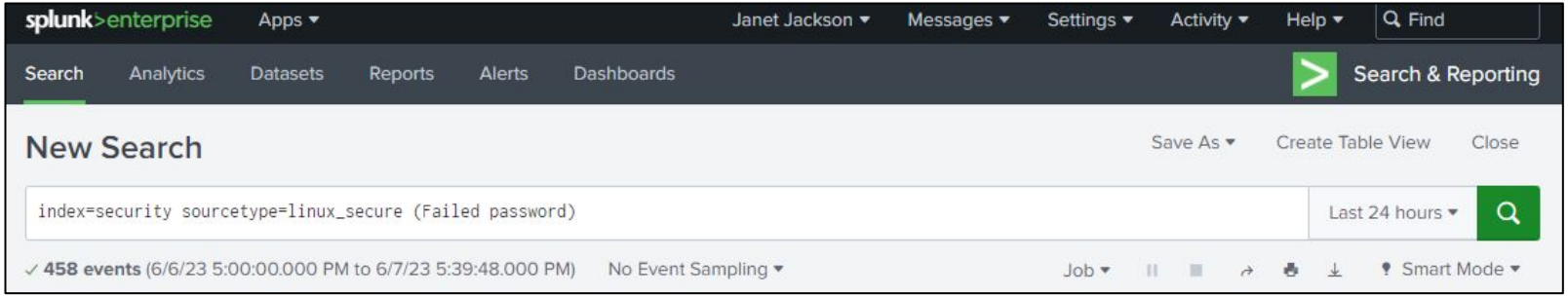


image: screenshot, splunk Search & Reporting app

8.4 Create Alerts (continued)

Real-time alert - Rolling time window triggering.

There are many options available on the **Save As Alert** dialog box. Use a live Splunk environment to explore them all.

For **this** scenario - **Settings**:

- Title: **SEC_Alert_20_failed_login**
- Description: **Optional**
- Permissions: **Private**
- Alert type: **Real-time**
- Expires: **24 hour(s)**

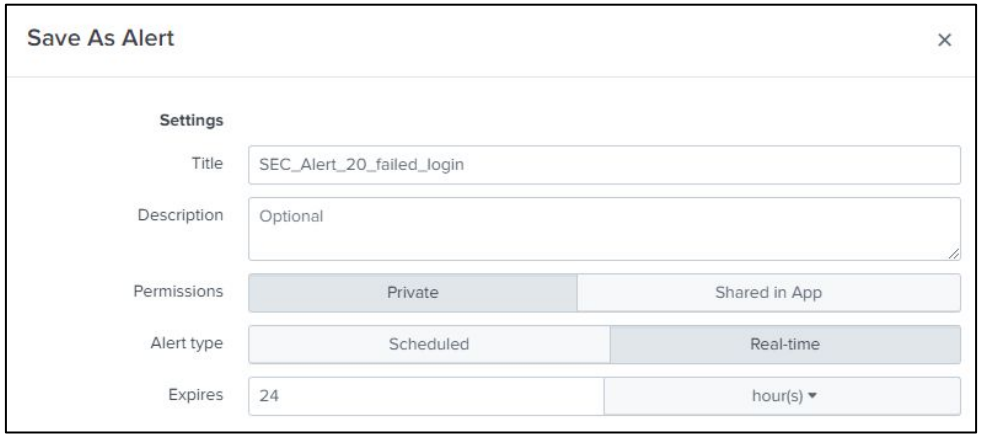


image: screenshot, splunk Search & Reporting app

PER SCHOLAS

8.4 Create Alerts (continued)

Real-time alert - Rolling time window triggering.

For **this** scenario - **Trigger Conditions**:

- Trigger alert when: **Number of Results is greater than 20**
- in: **5 minute(s)**
- Trigger: **Once For each result**
- Throttle: **check**
- Suppress triggering for: **30 minute(s)**

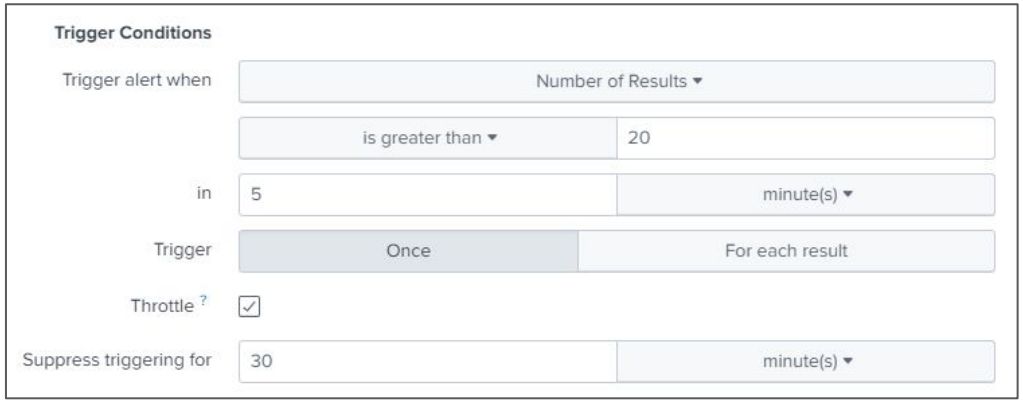


image: screenshot, splunk Search & Reporting app

PER SCHOLAS

8.4 Create Alerts (continued)

Real-time alert - Rolling time window triggering.

For **this** scenario - **Trigger Actions**:

- **+ Add Actions**
  - When triggered: **Add to Triggered Alerts**
  - Severity: **High**
- Click **Save**.

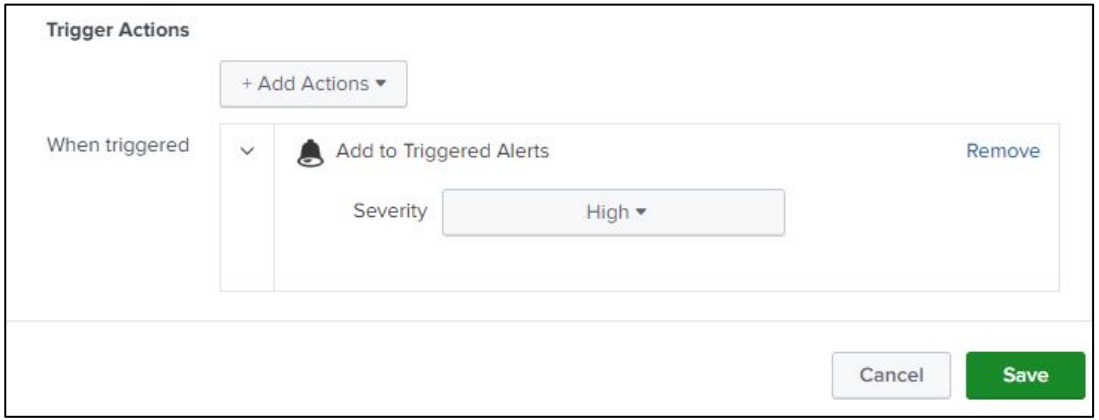


image: screenshot, splunk Search & Reporting app

8.4 Create Alerts (continued)

View and manage Alerts.

- The **Alerts page** lists all alerts for an app. It is available from the **top-level navigation menu** for an app.

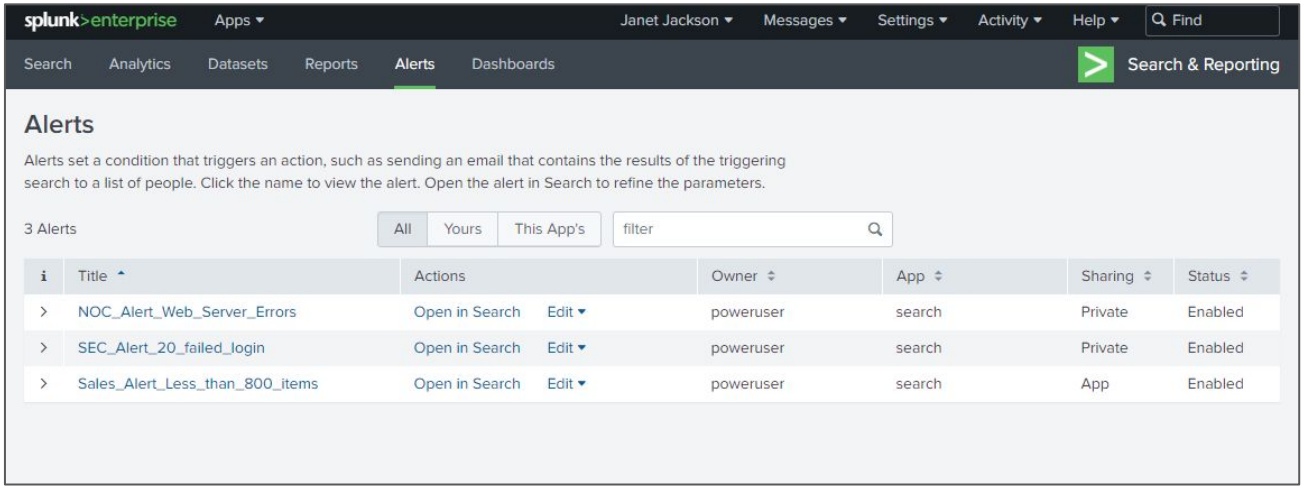


image: screenshot, splunk Search & Reporting app

8.4 Create Alerts (continued)

View and manage Alerts.

- From the Alerts page you can use the following options:

Option	Description
Select a filtering option for displayed alerts.	• **All**. View all alerts for which you have view permission. • **Yours**. View alerts that you own. • **This App's**. View alerts for the current app. Only alerts for which you have permission to view display in the list.
Select any displayed alert	Opens the detail page for an alert. You can review and make additional edits to the alert on the detail page.
Open in Search	View or modify the alert's search in the **Search** page.
Edit	Opens the detail page for an alert. You can review and make additional edits to the alert on the detail page.

image: https://docs.splunk.com/Documentation/Splunk/9.0.4/Alert/Alertspage

PER SCHOLAS

8.4 Create Alerts (continued)

View and manage Alerts.

- **Expanding** an alert entry on the Alerts page provides many **editing options**. Use a live Splunk environment to explore them all.

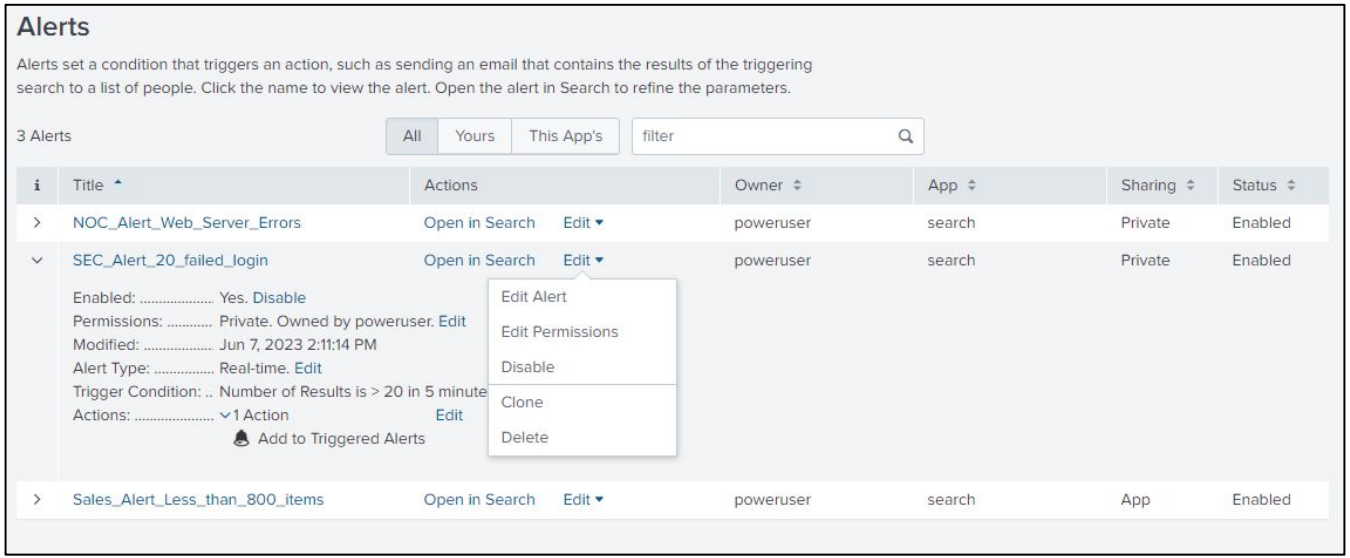


image: screenshot, splunk Search & Reporting app

8.5 View Triggered Alerts

You can see records of **recently triggered alerts** from the **Triggered Alerts** page or from an **Alert Details** page.

The **Triggered Alerts** page shows **all instances** of triggered alerts.

Records of triggered alert details are available for **24 hours** by **default**.

- **Access** the triggered alerts page by clicking on the **Activity** menu on the **Splunk Web interface** and selecting **Triggered Alerts** from to drop-down menu.

image: screenshot, splunk Search & Reporting app

8.5 View Triggered Alerts (continued)

Alerts **appear** on the **Triggered Alerts** page under the following **conditions**:

- The "**Add to Triggered Alerts**" action is **enabled** for the alert.
- The alert **triggered** recently.
- The alert **retention** time is **not complete**.
- The triggered alert listing has **not been deleted**.

As mentioned before, records of triggered alerts are available for **24 hours** by default.

You can **configure** this **expiration** time on a **per-alert basis**.

For example, you can **arrange** to have the triggered alert records for an alert have a **lifespan** of **7 days** instead of 24 hours.

image: screenshot, splunk Search & Reporting app

8.5 View Triggered Alerts (continued)

On the Triggered Alerts page, details appear in the following categories:

Category	Description
Time	Trigger date and time.
Fired alerts	Triggered alert name(s).
App	Alert app context.
Type	Alert type.
Severity	Assigned alert severity level. Severity levels can help you sort or filter alerts on this page.
Mode	Alert triggering configuration mode. "Per-result" means that the alert triggered because of a single event. "Digest" means that the alert triggered because of a group of events.

image: https://docs.splunk.com/Documentation/Splunk/9.0.4/Alert/Reviewtriggeredalerts

PER SCHOLAS

8.5 View Triggered Alerts (continued)

Examples of triggered alerts **used in this presentation** appear on the Triggered Alerts page.

splunk>enterprise Apps ▾ Janet Jackson ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

App Search & Reporting (search) Owner Janet Jackson (powerus... Severity All Filter

Alert All

«Prev Next» Showing 1-4 of 4 results

	Time	Fired alerts	App	Type	Severity	Mode	Actions
☐	2023-06-07 14:54:45 EDT	NOC_Alert_Web_Server_Errors	search	Real-time	High	Per Result	View results | Edit search | Delete
☐	2023-06-07 14:45:47 EDT	SEC_Alert_20_failed_login	search	Real-time	High	Digest	View results | Edit search | Delete
☐	2023-06-07 14:15:45 EDT	SEC_Alert_20_failed_login	search	Real-time	High	Digest	View results | Edit search | Delete
☐	2023-06-07 13:53:32 EDT	NOC_Alert_Web_Server_Errors	search	Real-time	High	Per Result	View results | Edit search | Delete

image: https://docs.splunk.com/Documentation/Splunk/9.0.4/Alert/Reviewtriggeredalerts

8.5 View Triggered Alerts (continued)

Delete a triggered alert listing

There are a **few ways** to change whether a **triggered alert** listing **appears** on this page.

- **Update** triggered alert listing **expiration time**.
- **Delete** a triggered alert listing from the **Triggered Alerts page**.
- **Disable** an alert to prevent it from triggering.

image: https://docs.splunk.com/Documentation/Splunk/9.0.4/Alert/Reviewtriggeredalerts

PER SCHOLAS

8.5 View Triggered Alerts (continued)

Click on the **View results** for the **NOC_Alert_Web_Server_Errors** link under the **Actions** column.

splunk>enterprise Apps ▾ Janet Jackson ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

App Search & Reporting (search) Owner Janet Jackson (powerus... Severity All Filter

Alert All

«Prev Next» Showing 1-4 of 4 results

	Time	Fired alerts	App	Type	Severity	Mode	Actions
☐	2023-06-07 14:54:45 EDT	NOC_Alert_Web_Server_Errors	search	Real-time	High	Per Result	View results | Edit search | Delete
☐	2023-06-07 14:45:47 EDT	SEC_Alert_20_failed_login	search	Real-time	High	Digest	View results | Edit search | Delete
☐	2023-06-07 14:15:45 EDT	SEC_Alert_20_failed_login	search	Real-time	High	Digest	View results | Edit search | Delete
☐	2023-06-07 13:53:32 EDT	NOC_Alert_Web_Server_Errors	search	Real-time	High	Per Result	View results | Edit search | Delete

image: https://docs.splunk.com/Documentation/Splunk/9.0.4/Alert/Reviewtriggeredalerts

8.5 View Triggered Alerts (continued)

The results will open (in this case) in the Search & Reporting App, displaying the **event** that **triggered** the Alert.

This a good starting point in **troubleshooting** the issue. From the event, you can learn the source IP address, the action performed on the server, the server host name, HTTP version, the HTTP error code, and so on

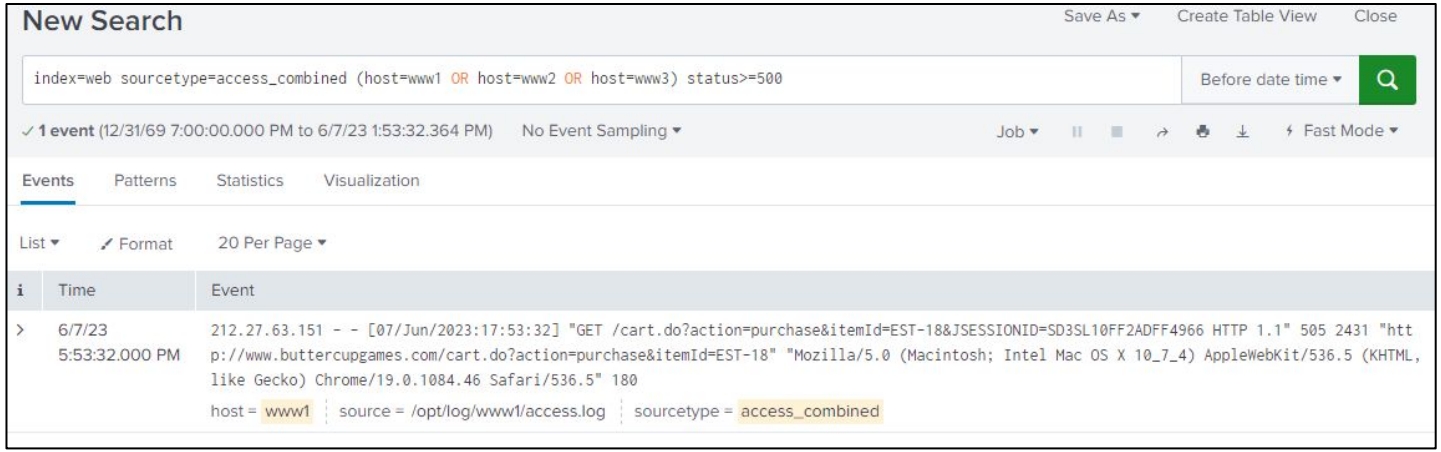


image: https://docs.splunk.com/Documentation/Splunk/9.0.4/Alert/Reviewtriggeredalerts

8.3 - 5: Describe, Create and View Alerts - Summary

Splunk alerts provide a mechanism for proactive monitoring and notification within the Splunk platform. Alerts enable you to define specific conditions or events that when met, trigger notifications or actions.

Alerts can be scheduled or occur in real time. Scheduled alerts trigger based on a predefined schedule, while real-time alerts trigger immediately when the specified conditions are met.

Triggered Alerts can perform various actions, such as sending email notifications, executing scripts, or adding the alert to triggered alerts list.

PER SCHOLAS

Knowledge Check

- What are the two alert types?
- What is the difference between a scheduled alert and a scheduled report?
- What is an advantage and disadvantage of a real-time alert?
- What some of the options available when scheduling a time for a scheduled alert to run?
- What is the difference between a real-time alert with a per-result trigger and a real-time alert with a rolling window trigger?
- In what scenario would an administrator select to throttle an alert?
- What are the conditions for an alert to appear in the triggered alerts page?
- When selecting the Add to Triggered Alerts action, what does selecting a Severity level provide?