**Types of alerts:**

1. **Scheduled Alerts**:
   * These alerts run searches at regular intervals based on a defined schedule.
   * They are useful for monitoring conditions that do not require immediate attention.
   * For example, you might set a scheduled alert to run every hour and trigger if the number of 404 errors exceeds a certain threshold.
2. **Real-Time Alerts**:
   * These alerts continuously monitor events as they occur.
   * They are ideal for scenarios where immediate action is required.
   * Real-time alerts can be configured to trigger per result (each time an event occurs) or based on conditions within a rolling time window.

**How to create feedback alert:**

Creating a feedback alert in Splunk Enterprise involves setting up an alert that triggers based on specific conditions in your data. Here’s a step-by-step guide to help you create one:

1. **Create a Search:**
   * Go to the Search & Reporting app in Splunk.
   * Create a search query that identifies the feedback events you want to monitor. For example:
   * index=feedback sourcetype=feedback\_logs "negative feedback"
2. **Save the Search as an Alert:**
   * Once you have your search results, click on Save As and select Alert.
3. **Configure the Alert:**
   * **Title:** Give your alert a meaningful name, such as “Negative Feedback Alert”.
   * **Description:** Optionally, add a description to explain what the alert does.
   * **Alert Type:** Choose between Scheduled or Real-time based on your needs.
     + **Scheduled Alert:** Runs at regular intervals (e.g., every hour).
     + **Real-time Alert:** Monitors events continuously and triggers as soon as conditions are met.
   * **Trigger Conditions:** Define when the alert should trigger. For example, you might set it to trigger if the number of negative feedback events exceeds a certain threshold within a specific time frame.
4. **Set Alert Actions:**
   * Decide what actions should be taken when the alert triggers. Common actions include:
     + **Send an Email:** Notify relevant team members.
     + **Run a Script:** Execute a custom script.
     + **Webhook:** Send data to an external system.
   * Configure the action details, such as email recipients or webhook URLs.
5. **Review and Save:**
   * Review your alert settings to ensure everything is configured correctly.
   * Click Save to create the alert.

Here’s an example configuration for a scheduled alert that runs every hour and triggers if there are more than 10 negative feedback events:

* **Title:** Negative Feedback Alert
* **Description:** Triggers when there are more than 10 negative feedback events in an hour.
* **Alert Type:** Scheduled
* **Time Range:** Last 60 minutes
* **Trigger Condition:** Number of results > 10
* **Actions:** Send an email to feedback\_team@example.com

**Difference between Normal alerts and feedback alerts:**

In Splunk, the difference between a normal alert and a feedback alert primarily lies in their purpose and the conditions they monitor:

1. **Normal Alert**:
   * **Purpose**: General monitoring of system performance, security events, or any other predefined conditions.
   * **Examples**: Alerts for high CPU usage, failed login attempts, or specific error codes.
   * **Trigger Conditions**: Based on thresholds or specific patterns in the data.
   * **Actions**: Can include sending notifications, running scripts, or creating incidents in IT service management systems.
2. **Feedback Alert**:
   * **Purpose**: Specifically designed to monitor user feedback or sentiment.
   * **Examples**: Alerts for negative feedback, high volumes of customer complaints, or specific keywords in feedback logs.
   * **Trigger Conditions**: Based on the presence of certain keywords, phrases, or patterns in feedback data.
   * **Actions**: Typically involves notifying customer service teams, creating tickets for follow-up, or triggering workflows to address the feedback.

While both types of alerts use similar mechanisms in Splunk, the key difference is in their focus and the specific conditions they are set to monitor. Normal alerts are more general and can cover a wide range of system and application metrics, whereas feedback alerts are tailored to track and respond to user feedback and sentiment.

**Sending feedback alerts to interlink and service now:**

**Sending Alerts to Interlink**

1. **Webhook Integration**:
   * If Interlink supports webhooks, you can configure a webhook action in Splunk to send the alert data to Interlink.
   * In the alert configuration, go to the Actions section and select Webhook.
   * Enter the webhook URL provided by Interlink and configure the payload as needed.

**Sending Alerts to ServiceNow**

1. **ServiceNow Integration**:
   * ServiceNow can be integrated using the Webhook action or a dedicated ServiceNow app/add-on for Splunk.
   * **Using Webhook**:
     + In the alert configuration, go to the Actions section and select Webhook.
     + Enter the webhook URL for your ServiceNow instance and configure the payload to create an incident or task.
   * **Using ServiceNow Add-on**:
     + Install the ServiceNow add-on for Splunk from Splunk base.
     + Configure the add-on with your ServiceNow instance details.