Frequently Asked Questions

Demystifying the Grok platform.

This FAQ covers the Grok application and underlying anomaly detection technology. It includes links to other documents for detailed information.

Anomaly Detection

How does Grok determine what is anomalous?

Grok has a unique approach to reporting anomalies that is designed to cut down on the number of false positives. Grok first learns patterns in your data and builds models that predict what is likely to happen next in the metric data stream. Based on the internal predictions, the algorithms generate a raw anomaly score for each data point.

The raw anomaly scores are smoothed with a short moving average. Then the scores are compared to a window of historical scores to determine the mathematical likelihood that the scores match past predictability.

This allows Grok to determine the statistical likelihood the system is behaving anomalously relative to recent history for the particular data stream. This normalizes the anomaly scores, allowing Grok to confidently detect anomalies if both predictable and unpredictable data.

What is the probationary learning period?

Grok begins building models on the selected instances immediately. The instance will be in ‘pending’ mode while the model is still the in the probationary learning phase, generally for the first one thousand records. While the model is still in this phase, it will display grey-scale bars.

It will then move to ‘active’ when the instance is actively being monitored, indicated by colored bars, and can be used for accurate anomaly detection. The model will continue learning beyond the probationary learning period through the life of the model and will adjust and adapt to changes in your data.

Notifications

When will I begin to receive notifications?

Notifications begin after the ‘probationary period’ has ended, after the first thousand records have been received. We do still display the anomalies that are found during the probationary period but you will not receive notifications during that time.

What is included in each notification?

Each notification includes the time of the anomaly, instance, metric and metric value including units when available. Copies of notifications are also maintained in the activity log.

How do I configure Grok to receive notifications?

Notifications can be received via the Grok Mobile UI or email. To activate notifications, visit the settings page in the Grok mobile app and enable notifications. Android notifications will be shown in the notification tray and email notifications will be sent to the email address specified.

How do I change the frequency with which I receive notifications?

The default setting notifies a user each time an anomaly is detected by their selected notification method. The frequency of notifications can be adjusted on a per instance basis, in the settings page of the app. The frequency of notifications is available in a range from no limit/all notifications to max 1 per 24 hours.

Automation

Why should I create an automation?

The automation feature provides a way for operations teams to conduct initial troubleshooting for a service that Grok detected anomalous behavior. Usually when a service failure occurs, operations teams will conduct a series of initial steps to diagnose and resolve the issue, including pulling error logs at the time of failure, restarting the server or rerouting traffic via a load balancer. Many of these steps can be initiated using scripts and API calls to your cloud provider. When Grok detects an issue, this can trigger a script. This cycle of detection and action has the potential to save an ops team time so they can focus on building awesome software instead!

What is the difference between a step and a branch?

A step runs a script after the previous script has run successfully with no errors, whereas a branch runs only if the provided conditional output is returned by the output of the script which ran before it. If a list of troubleshooting steps that must occur in a specific order, each script will only run after the previous script runs successfully. If a troubleshooting workflow requires confirming a specific output of the script before it, a branch can be added to confirm the output before moving forward.

Where can I view the output that resulted from a triggered automation script?

Script output and history can be viewed in two places: the list of automations or in the anomalies table. The automation list shows the full history in the context of the automation. The anomalies table shows any output that an automation provides as the result of being triggered by a detected anomaly. The output can be accessed via the Grok API as well.

Troubleshooting

Why am I not seeing any anomalies?

There are many reasons why this may occur, but some of the most common are:

1. The most common reason is that anomalies, by definition, are abnormal. Therefore, if your systems are functioning as normal, you won't see any anomalies.

2. Grok learns and builds models from your data during its probationary learning period. It is possible that Grok has not yet received enough data to confidently detect anomalies.

3. Grok has not detected any anomalies during a given time period for that instance. Some data may look unusual but if Grok has previously learned the patterns then it will not find it anomalous.

Try looking at the instance data over the last few days or weeks to see if similar patterns have previously occurred.

Why do similar metrics with similar patterns of data produce different anomalies?

Grok builds a single model per metric. The models for custom metrics estimate the value range of the data based on the first few hundred records and the anomaly detection is based on the patterns learned from data in the past. It is normal to see slight variations between models with similar data. Even if the patterns look identical between two metrics, it is likely that past behavior was different, resulting in different predictions for new data from the models.

I am having an issue that I can't resolve. How do I contact support?

Please email Grok support at support@grokstream.com