March 2023

TECHNIQUES TO PROVIDE A RECOMMENDATION ENGINE FOR ALERT CONFIGURATIONS

Shubhankar Yash

Abhishek Dhar

Chakresh Tiwari

Shiva Sah

Sonali Hiranandani

TECHNIQUES TO PROVIDE A RECOMMENDATION ENGINE FOR ALERT CONFIGURATIONS

AUTHORS:
Shubhankar Yash
Abhishek Dhar
Chakresh Tiwari
Shiva Sah
Sonali Hiranandani

ABSTRACT

False alerts are a large problem in the observability space. Noisy alerts can be caused by a variety of factors but can be primarily caused due to incorrect alert configurations. Presented herein are techniques through which personalized recommendations can be provided for a particular enterprise regarding observability alert configurations that are based alerts of similarly situated enterprises. The recommendations may be applied only on explicit approval from the particular enterprise. Techniques presented herein may also enable enterprises to set up customized alerts and detect problems in their environments without a lot of configurations.

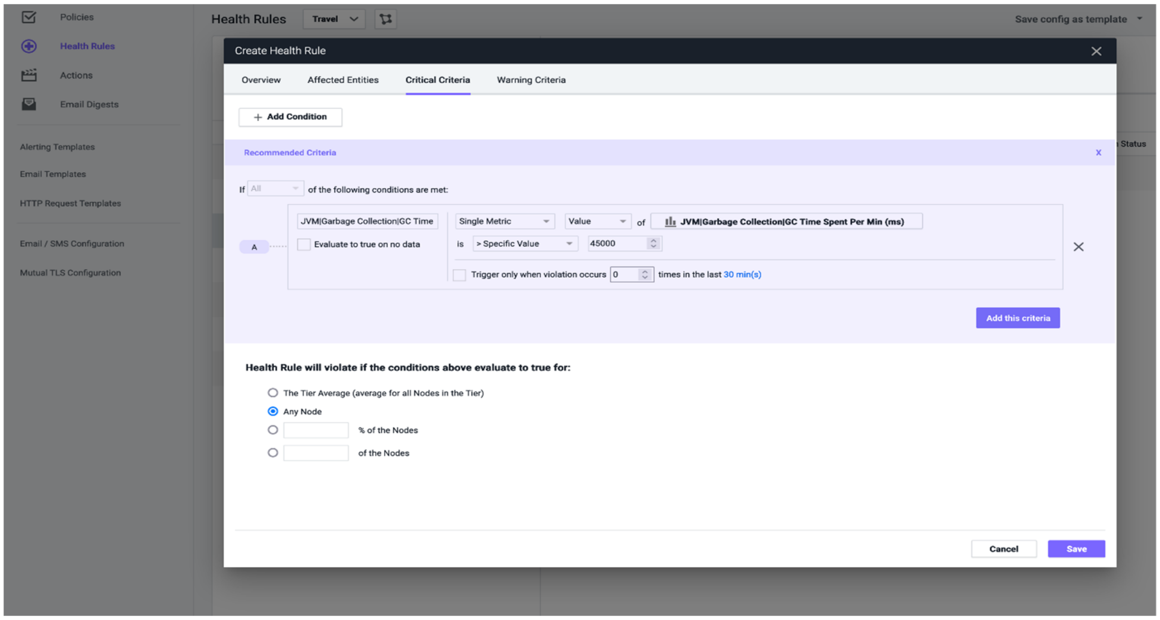
DETAILED DESCRIPTION

With regard application performance management/observability, false alerts are a massive problem. Even expert enterprises that have years of experience with application management/observability products struggle with false alerts. One cause for noisy alerts is often due to incorrectly configured alerts. For example, an enterprise may choose the wrong metrics, incorrect threshold values, etc. for configured alerts, which can lead to false alerts. If an enterprise sets up alerts with incorrect metrics, they will never detect the right problem at the right time.

For example, in a Kubernetes environment, if an enterprise sets up alerts on failed pods, once a pod fails, it will be too late to rectify the situation by the time they get an alert. It would be more suitable to setup alerts on resource utilization so that enterprises receive alerts preemptively before something big fails. On the other hand, if an enterprise chooses incorrect thresholds, they risk false positives, such as receiving an alert when there isn't a real issue or false negatives, for example, not receiving an alert when there is an actual issue. The problem that users of observability tools face is the lack of a scientific method to determine appropriate thresholds. Some enterprises have characterized the process of determining appropriate thresholds as a 'hit and trial'. It is not uncommon to adjust an alert many times before it is configured appropriately such that its alert behavior stabilizes, which can result not only in wasted time and resources for an enterprise but can also result in potentially false alerts for a considerable duration.

In order to address such issues, a recommendation engine is provided in accordance with techniques of this proposal in which the recommendation engine uses collaborative filtering to provide recommendations on the metrics on which an enterprise should setup alerts and what the appropriate thresholds should be for the metrics. Such a recommendation engine for alert configurations can reduce the amount of configuration that may be needed by enterprises while also giving them the control to have the final approval with regard to the configuration of an alert.

Alert recommendations can be determined on the basis of an enterprise profile such that the recommendation engine can analyze enterprises of a similar profile (e.g., environment size, environment type, region, industry, etc.) and may provide alert recommendations based on alert configurations for enterprises of a similar profile. Figure 1, below, illustrates an example alert configuration user interface (UI) through which a configuration can be provided for a given alert.



If All of the following conditions are met:

JVM|Garbage Collection|GC Time

□ Evaluate to true on no data

Single Metric Value of JVM|Garbage Collection|GC Time Spent Per Min (ms)

is > Specific Value 45000

□ Trigger only when violation occurs 0 times in the last 30 min(s)

Health Rule will violate if the conditions above evaluate to true for:

○ The Tier Average (average for all Nodes in the Tier)

● Any Node

○ % of the Nodes

○ of the Nodes

Figure 1: Example Alert Configuration UI

In summary, techniques are presented herein through which personalized recommendations can be provided for a particular enterprise regarding observability alert configurations that are based alerts of similarly situated enterprises. The recommendations may be applied only on explicit approval from the particular enterprise. Techniques presented herein may also enable enterprises to set up customized alerts and detect problems in their environments without a lot of configurations.