## **Technical Disclosure Commons**

**Defensive Publications Series** 

March 2023

# **TECHNIQUES TO PROVIDE A RECOMMENDATION ENGINE FOR** ALERT CONFIGURATIONS

Shubhankar Yash

Abhishek Dhar

Chakresh Tiwari

Shiva Sah

Sonali Hiranandani

Follow this and additional works at: https://www.tdcommons.org/dpubs\_series

#### **Recommended Citation**

Yash, Shubhankar; Dhar, Abhishek; Tiwari, Chakresh; Sah, Shiva; and Hiranandani, Sonali, "TECHNIQUES TO PROVIDE A RECOMMENDATION ENGINE FOR ALERT CONFIGURATIONS", Technical Disclosure Commons, (March 13, 2023)

https://www.tdcommons.org/dpubs\_series/5734



This work is licensed under a Creative Commons Attribution 4.0 License.

This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

#### Yash et al.: TECHNIQUES TO PROVIDE A RECOMMENDATION ENGINE FOR ALERT CONFIGURA

#### 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

1

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.

Vexish Indee     Vexish Indee <th>Policies</th> <th>Health Rules Travel V 🗓</th> <th>Save config as</th> <th>s template 💌</th>	Policies	Health Rules Travel V 🗓	Save config as	s template 💌
Actions   True Doess     Actions     Actions </th <th>Health Rules</th> <th>Create Health Rule</th> <th></th> <th>×</th>	Health Rules	Create Health Rule		×
In the Dependence of the Add Control of the Kodes   A tring Turpistie # 4 dd Control of the Kodes   The Prepared Transform # # # Control of the Kodes   The Dependence of the Kodes # # # # # # # # # # # # # # # # # # #	Actions	Overview Affected Entities Critical Criteria Warning Criteria		
Addring Templates   Email Templates   HTTP Recensit Templates   Email / SMS Configuration   Mutual TLS Configuration   Health Rule will violate if the conditions are met:   Image: Problem Rule will violate if the conditions above evaluate to true for:   Image: Problem Rule will violate if the conditions above evaluate to true for:   Image: Problem Rule will violate if the conditions above evaluate to true for:   Image: Problem Rule will violate if the conditions above evaluate to true for:   Image: Problem Rule will violate if the conditions above evaluate to true for:   Image: Problem Rule will violate if the conditions above evaluate to true for:   Image: Problem Rule will violate if the conditions above evaluate to true for:   Image: Problem Rule will violate if the conditions above evaluate to true for:   Image: Problem Rule will violate if the conditions above evaluate to true for:   Image: Problem Rule will violate if the conditions above evaluate to true for:   Image: Problem Rule will violate if the conditions above evaluate to true for:   Image: Problem Rule will violate if the conditions above evaluate to true for:   Image: Problem Rule will violate if the conditions above evaluate to true for:   Image: Problem Rule will will will will will will will wi	Email Digests	+ Add Condition		
Erail Templates Final Template	Alerting Templates	Recommended Citteria		× Status
The Products (Programs)         Email / SMS Configuration         Mutual TLS Configuration         Mutual TLS Configuration	Email Templates	If All " of the following conditions are met:		
Mutual TLS Donfiguration       Trigger only when violation occurs       images in the last 30 min(s)         Mutual TLS Donfiguration       Mutual TLS Donfiguration       Mutual TLS Donfiguration	Email / SMS Configuration	JVM(Garbage Collection(GC Time ) Single Metric - Value - of <u>II JVM(Garbage Collection(GC Time Spent Per Min (ms)</u> A Evaluate to true on no data is >Specific Value - 4500 0	>	<
Mad this enters         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tier)         Internet Transverage (average for all Nodes in the Tie	Mutual TLS Configuration	Trigger only when violation occurs 0 0 times in the last 30 min(s)		
Health Rule will violate if the conditions above evaluate to true for: <ul> <li>The Tier Average (average for all Nodes in the Tier)</li> <li>Any Mode</li> <li>of the Nodes</li> <li>of the Nodes</li> </ul> <ul> <li>of the Nodes</li> </ul>			Add this criteria	
The Tier Average (average for all Nodes in the Tier) Any Node  the of the Nodes of the Nodes Cancel Save		Health Rule will violate if the conditions above evaluate to true for:		
Any Node     Supervision     Supervision     Cancet     Supervision		The Tier Average (average for all Nodes in the Tier)		
Cancel Save		Any Node     % of the Nodes		
Cancel		O of the Nodes		
Cancel				
Cancel				
			Cancel Sav	

Figure 1: Example Alert Configuration UI

2

#### Yash et al.: TECHNIQUES TO PROVIDE A RECOMMENDATION ENGINE FOR ALERT CONFIGURA

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.

3