

Title: Query Prediction for Log Search for Distributed Tracing with External Monitoring Alerts

(外部監視のアラートによる分散トレースのログ検索に対するクエリの予測)

Authors: Tomoyuki Koyama, Takayuki Kushida, Soichiro Ikuno

小山 智之(東京工科大 大学院生)、串田 高幸(東京工科大 教授)、生野 壮一郎(東京工科大 教授)

Journal: IEEE the 7th Conference on Cloud and Internet of Things

掲載年月: 2024 年 10 月

研究概要: この論文は、システム管理の分散トレーシングにおいて、管理者が検索クエリを発行するよりも前に検索結果をキャッシュとして自動生成するための検索クエリの予測方法を提案する。この検索クエリの予測方法を使うことによって発行される可能性が高い検索クエリを事前に作成することができる。この提案では、外部監視のアラートとトレースにある属性値を検索クエリの予測に利用する。これらのデータを使用することで、発行された検索クエリに対するキャッシュのヒット率を向上させることができる。評価実験では、提案方法を適用した場合と適用しない場合を比較して、検索クエリを発行して応答が受信されるまでの応答時間を測定する。

研究背景: 一般にマイクロサービスのシステムは、それぞれのサブシステムに分割された複数のサービスで構成される。そのため、マイクロサービスのシステムでは、ソフトウェアスタックのトレースを使ったエンドツーエンドの追跡をすることができないという課題がある。システム障害が発生した時に、モニタリングのシステムと同じようにマイクロサービスのシステムの根本原因の分析を行う必要がある。分散トレーシングは、マイクロサービスシステムの可観測性を向上させる方法である。システム管理者は、システム障害が発生したときにこの分散トレースを使用して、システム障害の原因となっているトランザクションやリクエストを見つける必要がある。分散トレースの結果のレコードは、検索エンジンに保存される。検索エンジンが、以前に発行されていないクエリを受信した場合に検索クエリに対するキャッシュがない。そのため、検索クエリの応答に時間がかかる。迅速に障害を解消するためには、この検索クエリに対する応答時間を短くする必要がある。

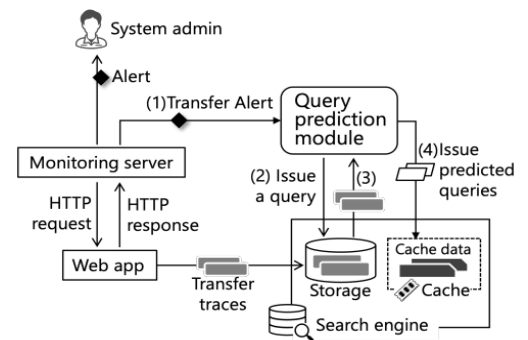


図 Query Prediction の提案方

研究成果: この論文では、障害の原因調査のときに時間がかかっているシステム管理のログに対する検索時間を短くするための方法を提案している。提案方式は、監視システムから出力されるアラートとトレースのデータをペアで分析することで使われる可能性高い検索クエリを自動的に生成できるところに特徴がある。

社会的・学術的なポイント: IT システム管理の分野で、大量のログの検索時間を短くする研究としてアラートとトレースデータの 2 つを入力にして検索を予測する方法は、今まで提案されていなかった。この方法を使うことによって、検索クエリに対するキャッシュのヒット率を上げることができ、その結果、検索時間を短縮することができるようになった。

用語解説:

分散トレース: マイクロサービスアーキテクチャによって構成されたシステムを監視するための方法である。それぞれのマイクロサービスで処理されるトランザクションやリクエストをモニターすることによって、問題や異常がある箇所を特定することができる。

マイクロサービスアーキテクチャ: 最小単位になる個別のサービスを組み合わせて、大きな一つのソフトウェアサービスを構築することができるアーキテクチャのことである。

検索キャッシュ: 検索結果を高速アクセスが可能なメモリや記憶装置に記録しておくことで、次の検索があった時に通常よりも高速に検索結果を返答するための方法である。

アラート: IT のシステム管理において、なんらかの異常状態があったときに管理者に対して、その異常状態を知らせる方法である。