HOW AI-ENABLED ROOT CAUSE ISOLATION CAN REDUCE RISK

Artificial-intelligence (AI)-enabled root cause isolation is an important component of the incident management strategy that allows organizations to proactively mitigate risk of service outages and downtime. Modern IT infrastructure environments consist of a complex and convoluted mix of hardware components, running software applications in a variety of service delivery architecture: on-premises, multicloud, software-defined, and containerized instances. The sheer volume of metrics, events, and log data containing insights on patterns of issues such as performance downtime and network infringements can easily overwhelm teams running traditional analytics and automation tools for root cause analysis.

AI has emerged as a promising application for incident management use cases. Unlike traditional automation, AI-enabled tools not only identify insights into past log metrics data but also predict future trends and then automate a proactive remediation action or provide guidance on best possible proactive risk management actions.

How it works

Root cause isolation capabilities should be an essential part of your AIOps tooling portfolio and is focused on predicting the most likely root cause situation underlying a service dependability issue. The technology that makes these predictions uses AI models—representing the IT infrastructure systems and their behavior under varying load patterns—that have trained and learned patterns of log metrics data over time. When the AI model determines a pattern of performance issues in the log metrics data, it replicates the future behavior of the infrastructure systems and predicts a likely future outcome based on recent historical events. In the case of root cause analysis, the AI models can be trained to analyze situational events from the infrastructure system and nodes, and predict

the future impact on metrics such as mean time to identify (MTTI) or mean time to resolve (MTTR).

The AI-enabled root cause isolation works differently from traditional automation and analytics in the following ways:

- The AI tool provides a list of most likely incidents as well as the most relevant root causes applicable to the events scenario.
- The AI model then determines the most likely set of nodes that map to the most probable root cause incidents.
- The model then finds a list of causes or situational events as well as automated triggers or change requests that help reduce the probability of service outages to specific root nodes.
- Additional useful information can include the health trajectory of individual nodes and services. Next, tools can leverage this information to create intuitive dashboards and reports that allow for decision making at various levels of the organization, including long-term strategic actions on technology investments, updates, and modifications.
- The AI system can be programmed to act autonomously on actions such as dynamical workload management and isolating nodes to contain damages.
- The key difference from traditional automation tools is that the rules for action do not have to be hardcoded or informed explicitly. Instead, the AI tool can be trained from historical events around the optimal system behavior and trigger actions to address any deviation when specific performance thresholds are exceeded.
- These triggers can also be replaced with insights, guidance, or change requests that can be manually reviewed and approved based on the organizational policies.

While the insights and subsequent control actions are not predefined in an AIOps solution, the tool uses a predefined knowledge graph and business service models for every underlying technology. The knowledge graph connects different nodes and identifies the relationships between these nodes and subsequently, the hardware components, IT services, and application components. Between the graph nodes to each so-called edge of the graph, the AI tool assigns weights or an importance value.

Based on the training of the model and the patterns of observed data, these weight values are updated autonomous, with different patterns of incidents ranked on the knowledge graph. Therefore, when a specific event and its corresponding series of events or traffic patterns are observed, the AI model is able to rank the nodes corresponding to the highest importance value or weights as a relevant criteria.

With this capability, AIOps teams can focus their efforts on innovation and service improvement instead of firefighting IT incidents that occur with little notice and can potentially cause a lasting impact. It is important to understand that the performance of AI models inherently depends on the data quality used to train them. If the data is sufficiently rich in terms of representing relationships between nodes and business service models and is available for processing in real time, the AI tool can help organizations identify and contain damages that might impact specific root cause nodes. It is also important to align cross-functional teams operating in silos and give them access to exhaustive log metrics data and proposed controlled action triggers.

In conclusion, AI-enabled root cause isolation is a powerful tool for incident management. Organizations can quickly identify and contain damage from IT outages or incidents, thus reducing risk and minimizing disruption to business operations.