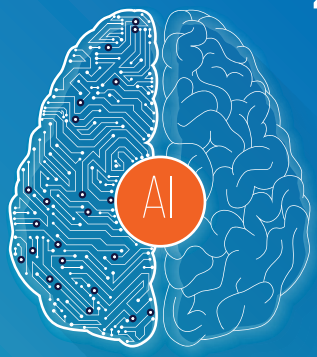
AIOps and Monitoring

— The Best of Both Worlds



Enterprises have spent the last 10 years trying to transform their businesses by powering them with applications. But when something breaks, they're typically left figuring it out by looking at siloed tools, usually operated by siloed teams — and then they're often stuck in a room arguing about whose information is right. These enterprises have too many tools, too many events and alerts, and more disjointed pieces of information than they know what to do with.

Event correlation is an insightful way to find that needle in a haystack or to become aware of a needle no one previously knew even existed. Event correlation is a technique for making sense of a large number of events and pinpointing the actionable events in that mass of information. This is accomplished by identifying and analyzing relationships between events. This is what AIOps vendors claim to do, ostensibly by employing artificial intelligence techniques, although most are just using statistical analytics. Customers are led to believe that they can just add an AIOps tool on top of their existing mix of monitoring tools without having to address the issue of disjointed monitoring tools.

The Statistical Event Correlation Approach (The AIOps Way)

AIOps tools use statistical analytics along with user-defined rules to bubble up and prioritize incidents. These statistical methods rely on indicators such as time (Did multiple events occur simultaneously?), network proximity (Are two disruptions located on the same subnet?), and number of like qualities (Did a particular word show up in many events?).

These tools can be really great at spotting a pattern. Given a set of whitelisted and blacklisted events, they can perform brute-force pattern matching to classify new incoming events as good or bad. They can also detect these patterns themselves, but for this, they need long training times and large sets of data. But there are two challenges with this approach.

- **Noise reduction via statistical correlation**
- Doesn't understand service context or model
- Doesn't always have access to raw data or events

Informational Entropy

Soft, Fuzzy Matching

- **User-defined rules engine**
- Dependent on users to define the rules

- **Depends on an operator's ability to tag occurrences correctly**
- Only works for issues that have already occurred — will not extrapolate to new scenarios
- Updates and changes to environment and tools reset understanding of what is "good" or "bad"

Blacklisting

Whitelisting

Textual Similarity

- **Linguistic matches within event data**
- Events do not carry the full-context raw data

Network Proximity

- **Infer relationships based on topology links**
- Proximity doesn't determine relationship

- **A visual representation of events**
- Same drawbacks as previous methods

Graph Entropy

Time Occurence

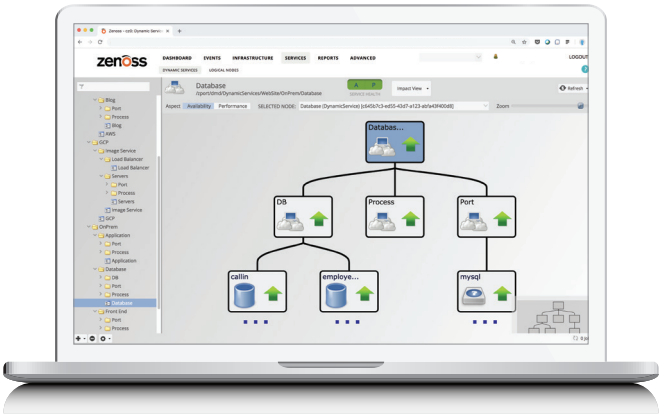
- **Correlates based on concurrent activity**
- Unrelated things may occur at the same time
- Related things may not occur at the same time

The first is that these AIOps tools have no domain knowledge and don't inherently understand the IT elements themselves, which can lead to them surfacing too many false positives to be useful. They commonly flag issues that are obviously not related. For example, it's obvious a printer and a website aren't related even though they generated events at the same time. But the AIOps approach probably does not know this. As a result, to be deployed effectively, AIOps tools require not only teams of data scientists, but teams of data scientists who are domain experts on IT infrastructure.

The other challenge is that AIOps tools are designed to troubleshoot business-impacting incidents after they have occurred. They only recognize issues they've seen before, and, furthermore, those issues must have the exact same signature. Around 70 percent of IT incidents are completely new and haven't occurred in the past. So, relying on past behavior, by definition, means not only that outages must occur, but that identical outages must occur before they can be recognized by AIOps tools. How many outages can an organization afford to endure before the AIOps tool learns how to recognize them?

The Intelligent, Domain-Based Correlation Approach

This approach involves modernizing the monitoring approach for the entire information technology stack. The key is selecting a platform with an ability to perform event correlation based on a native, deep understanding of the IT infrastructure components and dependencies. One that is domain-aware as well as IT service-aware — one that knows how the infrastructure works in order to determine logical relationships. Understanding how these individual monitored elements support a critical service at any given point in time helps to prioritize the most important issues to investigate and resolve first.



An intelligent IT operations management platform like Zenoss Cloud helps IT Ops and DevOps teams understand IT service risks in real time and reduce noise by bubbling up service-impacting events (with prioritized root-cause analysis to ease resolution). Zenoss has inherent domain understanding of all IT systems and how they work. Zenoss knows that a failing fan in a converged infrastructure server will affect the performance of specific applications and that a printer error is not going to take down infrastructure for an e-commerce website even if it is on the same subnet. Zenoss knows that an issue on a backup server could affect the mobile app it supports, even if it isn't at peak use and customers aren't yet affected.

The Best of Both Worlds

Before organizations slap yet another tool on top of their glut of monitoring tools, they should stop and think about what problems they are trying to solve. Companies that have hope an AIOps solution is the easy way out inevitably end up realizing that this approach is terribly flawed.

The right approach is to tune the monitoring approach first. Monitoring is your first line of defense, and ensuring that you have a unified view with quality insights is key. You can then augment that with an AIOps tool on a broader set of data to further refine root-cause analysis capabilities. Here are some tips on how organizations should leverage each type of tool to get the best of both worlds. Zenoss software provides:

- **Unified monitoring of performance and availability across hybrid IT environments**
- **Amalgamating event data from your other monitoring tools (In other words, your "monitor of monitors")**
- **Infrastructure-related insights that are timely, actionable, and enriched with contextual data for resolution**
- **Automated alerts and ticketing for infrastructure-related, service-impacting events**

To learn more about how Zenoss can add rich context to AIOps events and gain insights into your IT services, visit our website at **www.zenoss.com.**