AFFINITI **N**ETWORK **A**SSURE

AIOps and How It Will Transform IT Operations for the Next 10 Years

The model couldn’t keep up with the real world, so this is what we need to do instead

IT Operations people tend to be, by and large, a cautious bunch. The unstated Rule One of the profession is “if it ain’t broke, don’t touch it”. There are very good reasons for this caution; nobody wants to be hauled up in front of management to explain why the website is down, especially if the reason is tied to upgrading or refactoring something that was working fine or at least acceptably beforehand.

This caution can however make IT Operations as a group slow to recognize change and adapt to its consequences.

For all the focus on deployment, the hand-off from development groups, and the automation of the attendant tasks, the bulk of IT Operations work is in keeping services running that are already provisioned. The services themselves, and the infrastructure that they run on, are all fully instrumented (or at least, they are supposed to be) – but the data generated by that instrumentation cause their own set of problems. Monitoring a handful of servers and applications is one thing, but with monitoring scaled out to thousands of systems, operators are liable to drown in a sea of red alerts.

The Journey from ITOA to AIOps

Enter analytics, or specifically, IT Operations Analytics – ITOA, to its friends. This category included a number of techniques used to discover complex patterns in high volumes of often "noisy" IT system availability and performance data (to quote Gartner's definition). This worked well, for a time, but the analytics techniques used tended to be fairly static and brittle, and did not deal gracefully with changes to the underlying IT infrastructure.

As long as operations teams could update their models fast enough to keep ahead of the rate of change, all was well. However, over the last decade the introduction of virtualization, first of compute and then of network components, and the rise of self-service provisioning and cloud computing, coupled with new approaches to application release (Agile, DevOps, CI/CD) has caused the rate of change to accelerate vertically, with no sign of a slowdown. A new approach is required.

What should IT Operations Analytics look like in a dynamic world, where the real-world changes far faster than the model can keep up, and operations teams are deluged with ever more events? An equally dynamic approach to analysis is required, and a new category of tools is emerging to satisfy that need. Gartner have characterized this new field as Algorithmic IT Operations, or AIOps.

The positioning of AIOps is at the intersection of monitoring, service desk, and automation. The idea is to take inputs from all the existing monitoring tools, and apply algorithmic techniques to sift them and analyze them to deliver valuable insights to Operations – in other words, create fewer and higher-quality tickets in the service desk, with the aim of delivering an early warning of developing problems, rather than documenting a failure that has already occurred. Those tickets can also be connected to orchestration or run-book automation tools to enable rapid resolution of issues as they are identified.

The key is the use of dynamic, real-time algorithmic techniques instead of static models to perform the analysis, avoiding the continuous labor that would otherwise be required to update the rules and filters in response to changes in the environment.

The practical application of AIOps boils down to four key features:

Alert De-Duplication

A big problem in IT Operations is the problem that generates too many alerts, whether repeating alerts in one channel, or similar alerts in many different channels. In the worst cases, this can develop into a full-blown alert storm. One of the major goals of AIOps is to identify those duplicates – but crucially, without needing to define them ahead of time, and without discarding useful information.

Event Correlation

Once the significant needles have been sifted out of the huge monitoring haystack, there is still a risk of wasted effort if they are only considered individually. Many approaches to identifying relationship require the configuration of the infrastructure and the application to be known and documented beforehand – but in an environment where the infrastructure may be changing or even moving around autonomously, on top of the pre-existing problems of different teams making changes, it is not feasible to have that perfect model. AIOps proposes to use algorithms to identify correlations automatically, purely based on the event stream itself, avoiding duplicate effort by disconnected teams and wasted time in the critical early phases of incident detection and diagnosis.

Situation Workflow & Remediation

Of course detection and diagnosis is only half the battle; IT Operations need to solve the problems that have been identified. AIOps enables different teams to work effectively together, with events from each functional area correlated together algorithmically. This collaboration avoids unnecessary reassignments and escalations, enabling fluid communication and faster resolution of incidents.

Knowledge Recycle

Problem solved, everyone moves on to the next one! Not so fast: what if happens again? The traditional approach is for the whole incident to be reviewed and documented in some sort of knowledge base or FAQ system, so that if the same type of incident recurs, everyone will be able to refer back to the documentation. The problem is that this work is time-consuming and not particularly exciting, so it only tends to be carried out for the major incidents. For lower-severity incidents, everything that was learned in the investigation and resolution stays in people's heads or their inboxes, part of the "dark matter" of organizational knowledge. AIOps instead proposes to capture the collaboration process itself and make that knowledge available automatically if similar events recur in the future – without anyone needing to write out a KB article.

How Does AIOps Improve IT Operations?

The result of doing all of this is improvement in a few key IT Operations metrics.

First of all, there is faster detection and diagnosis of problems – ideally enabling IT Operations to detect problems before end users are even aware, or at least before the impact is too widespread.

By getting this reduction in Mean Time To Detect, or MTTD, the overall incident duration is already significantly shorter – but it can be further reduced by also accelerating the Mean Time To Resolve, or MTTR. This is achieved through more effective collaboration between different teams and avoiding wasted effort.

In general, this makes for a reduction in the overall number and duration of incidents, which in turn makes for a much better experience for all of the other people who rely on the quality of IT Operations.

Ultimately, ITOA was about letting IT Operations deal with IT as it was: static, relatively slow to change. AIOps is about enabling IT Operations to deal with IT as it is and as it will be: dynamic, rapidly evolving. This is the key to supporting the new needs of IT's users, as the business climate goes through its own, parallel transition to a faster and faster rate of change and evolution. If IT is to keep up, static models will not work; algorithms are the only way to deal with the requirements that business will continue to place on IT.

Network Performance Monitoring and Diagnostics + IT Operations Analytics + Network Operations Center = **A**ffiniti **N**etwork **A**ssure

Contact us today at 512-334-4101 if you would like to learn more!