Are We There Yet? Autonomous Networking and the Rise of AIOps

Paving the way for virtual engineers, augmented operations, and automation on a self-managing network

John E. Burke
CIO and Principal Research Analyst
Nemertes Research

Q1 2020

Table of Contents

Executive Summary

Digital transformation demands a continuously available, high-performing network and drives ever more business-critical activity to the network. Yet most organizations aren't increasing the size of their network teams. So, IT must increase use of automation as a "force multiplier" for staff.

IT needs automation to help understand *what is going on in the network*, and also automation to *act in response to changes* in the network. IT teams are often leery of tools that take action automatically in response to events in the environment, often preferring systems that keep them in the loop. Being given a button to push and the choice of whether to push it keeps control squarely in the hands of staff, and prevents machine-speed mistakes—resulting from a lack of contextual understanding—that expand damage rather than healing it.

AIOps is the application of AI and analytics techniques to the problems of network management. AIOps tools have the potential to act on behalf of IT staff more flexibly, reliably, and correctly than previous generations of tools because they can apply contextual understanding to decisions about what is happening and what to do about it.

Artificial learning and reasoning coupled with self-modification provide the equivalent of digital twins of the network administrators and engineers able to watch, warn about, act on, and improve the network as a driver of business value.

IT professionals should:

- Assess their, and their networks', readiness. Can the network give an AIOps tool the information feeds and architectural support it needs to be effective?
- Assess the kind of AIOps tool—standalone, or built into a management portal for key infrastructure or network services—that will work best for their network given the ways in which it can support integration (e.g. via SDN and SD-WAN controllers, or device APIs, or CLIs, etc.), and where their greatest staffing and performance challenges lie
    - If working with a service provider, how well is that provider's infrastructure tailored to provide the AIOps tool all the data it needs, and the ability to act effectively on the enterprise's behalf? How long has the tool been in production use, and how many years of operational data have gone into its training?
- Start slowly, and early: use AIOps for visibility first, and expect to take time to teach it their context before looking to it for automated responses (hence the importance of starting early)
- Use the analysis AIOps provides to fine tune their own operations playbooks before attempting to automate them
- Learn to trust: Lay out a timeline for moving from "show me the button to push" to "tell me you just fixed something" with a rising level of importance over time (and plans how to fall back a level if a step pushes past the tool's abilities).

Why IT Needs to Stop Managing the Network

Digital transformation affects all aspects of enterprise operations, from factory floor to back office, from retail shop to warehouse. New initiatives, whether customer-facing or focused on staff and internal operations, will only continue to increase the number, variety, and criticality of functions entirely reliant on the network. To support digital transformation, the enterprise needs a continuously available, high-performing network.

Yet most organizations aren't increasing the size of their network teams. Despite the steady increase in on-premises, cloud, and hybrid use cases to support and the exploding number of devices to connect, IT is being asked to deal with the network as yet another "do more with less" situation.

Given no additional staff, IT has no choice but to increase the effectiveness and efficiency of the existing staff. That, in turn, means finding a way to give network teams additional leverage on the challenges they face. The solution? Automation, which serves as a "force multiplier" for staff.

There are two distinct types of automation IT needs to address different aspects of the scaling problem. First, IT needs help understanding *what is going on in the network*. Second, IT needs help *acting in response to changes* in network behavior, context, and load.

AI: Automating the Understanding

Artificial Intelligence (AI) assists in solving the first problem; understanding the network. Humans unaided cannot digest all the information the network can generate about itself, let alone make sense of it in real time. Even a midsized enterprise network can generate terabytes of monitoring data in a day, which means that an unaided human cannot hope to

- understand what constitutes "normal" activity
- sift out the potential performance or security-affecting events
- see the relationships of different events to each other.

Without these different flavors of understanding, it can be difficult for network teams to know how best to react to performance problems and service failures. It is also difficult to see how to act proactively, to prevent recurrence or head off similar issues.

Applying AI techniques such as machine learning and machine reasoning to streams of network-monitoring data can allow an AI-powered network management tool to

- handle network baselining
- use adaptive, self-modifying pattern recognition to spot and correlate anomalies
- predict events that might hurt performance
- drive immediate corrective action
- suggest longer-term mitigations and changes for service improvement.

Closing the Loop: Moving from Understanding to Acting

The second challenge is automating appropriate action, based on the understanding generated by AI.

Automation can come in the form of anything from an admin's own ad-hoc system scripting to complex workflows built in a management console. And though all aspects of IT are increasingly dependent on it, IT has a love/hate relationship with automation. Previous attempts to deeply automate operations failed to live up to IT expectations and enterprise needs. Tools either lacked the ability to act widely enough to really ease IT's burden, or, lacking anything resembling an understanding of context and normalcy, ended up doing widespread damage thanks to speed of execution.

As a result, IT teams are most comfortable with automation that is completely embedded in a system (think RAID drive), with ad-hoc scripting, and with "show me the button" automation—tools that generate alerts and provide a suggested response that can be activated by clicking an OK. Deciding when to run a script, or being given a button to push and the choice of whether to push it, keeps control squarely in the hands of staff, and prevents machine-speed mistakes from expanding damage rather than healing it.

AIOps: A New Generation of Automation

AIOps is the application of AI and analytics techniques to the problems of network management. AIOps tools have the potential to act on behalf of IT staff more flexibly, reliably, and correctly than previous generations of tools. They learn more about the network than previous generations of tools were able to, thanks both to fuller monitoring of data streams from more diverse sources, and to radically improved abilities to parse, understand, and correlate information across data streams.

As with previous generations of tools, AIOps tools can "show the button," keeping IT in the critical path of action. Or they can take action themselves (or trigger action via other tools) if IT lets them. The key differences compared to older generations of tools are

- AIOps tools can maintain a dynamic picture of what constitutes "normal" network performance and behavior, which necessarily changes over time
- AIOps tools can learn from IT teams as they solve problems, and automate the application of those solutions to future situations as appropriate.

That is, because they undertake the automation of understanding, they will be able to be more effective in automating actions.

Advancing Toward the Self-Driving Network

This pair of AI-powered abilities—to track an evolving picture of "normal" and to learn how to solve problems automatically within that context—bring with them the promise of an autonomous network. They also highlight an important fact: the self-driving, autonomous network doesn't just happen with the installation of new software or hardware. Creating

such a network requires an iterative process of learning, feedback, and adaptation, a close collaboration between staff and software that transfers knowledge (both ways, ultimately) of network characteristics and performance as well as network context and meaning.

An AIOps tool may come "out of the box" knowing what some kinds of network behavior mean (when a switch port ceases to pass traffic, for example) but will need to learn others (e.g. what a spike in HTTP traffic in December means). It may know some kinds of action to take (e.g. alerting IT staff to a hardware failure, creating a service desk ticket to track the resolution, etc.) but need to be taught others (e.g. to change the priority of some classes of traffic at specific times of year).

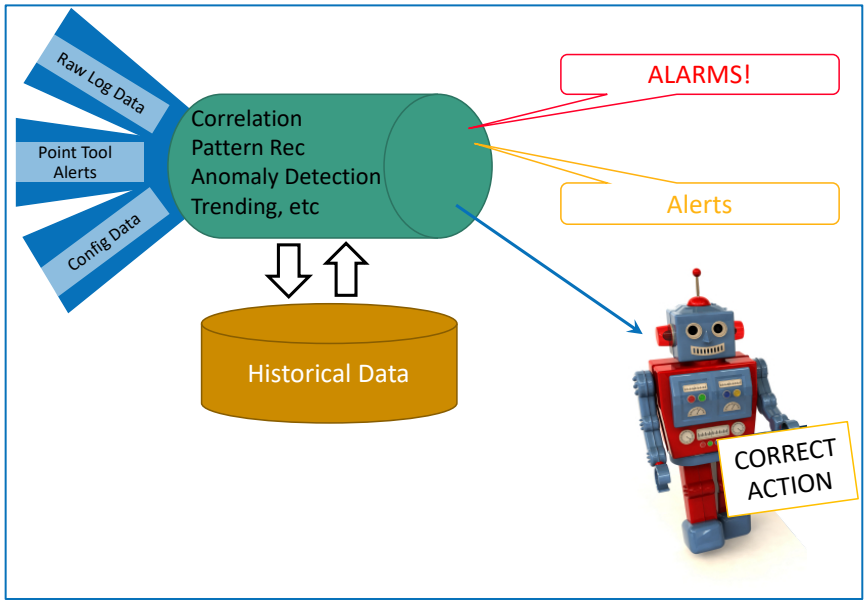

Figure 1: AIOps—Data Floods to Actionable Information...and Correct Action

This training period allows a true AIOps tool to become steadily more effective while at the same time allowing the IT team to build trust. The process of moving from "show me the problem" to "show me the button" to "here's what I just did on your behalf" can proceed in step with the tools' ability to take more, and more effective, action.

The AIOps market is still relatively young, of course, and the ability of AIOps tools to learn and act varies significantly. Much of the focus is still on the "understanding" side of the automation coin, and the ability to ingest vast amounts of data from diverse sources and correlate across them, though some solutions focus more on process automation.

Tools tend to be standalone, and need to be integrated with the other monitoring solutions and data sources they will rely on. However, when a network service provider is building AIOps technology into its management portals, most of that integration is built in, behind the scenes, keeping that work of IT's plate.

Help Wanted: Virtual Assistant

However, chronic short staffing and widespread challenges filling open positions are increasing the incentives to improve tools "act" capabilities. IT needs the same kind of leverage on the problems of network management that virtual assistants, chatbots, and

robotic process automation have brought to contact centers and other business activities. The creation of network virtual advisers and assistants, acting as digital twins for network engineers whether taking up mundane management tasks or providing expert guidance on design and problem solving, will be the key transformation true AIOps ultimately brings to networks.

Both network infrastructure companies and network service providers are seeing the inexorable logic behind this drive to autonomous operation. They are adding AIOps functionality to their own management tools and portals in an effort to build an enduring value proposition: that they can deliver not just a network capable of doing what the enterprise needs, but one that can be managed and supported sustainably over time.

The complexity of the network and of the management environment affect the use of AIOps: An enterprise or service provider with a relatively homogeneous environment, or one architected on open standards to accommodate centralized intelligence and action, will have an easier time providing an AIOps tool the information it needs to be truly effective.

What AIOps Needs

To be successful IT teams deploying an AIOps tool need to ensure they can deliver to it the data it needs, adequate computational capacity, and the levers necessary to automate operations.

Data, Data, Data

To succeed, even a current AIOps tool focused more on understanding than action needs data about the network. It should be able to ingest and use configuration data as well as performance monitoring feeds from all the underlay components of the network. It should also be able to take feeds from other management tools, such as Software Defined Network (SDN) controllers and monitoring software. The complexity of the network and of the management environment affect the use of AIOps: an enterprise or service provider with a relatively homogeneous environment, or one architected around open standards to accommodate centralized intelligence and action, will have an easier time providing an AIOps tool the information it needs to be truly effective. Environments with more generations of technology, more diverse infrastructures from more vendors, and requiring more protocols for integration and action will have a harder time realizing and delivering the value of AIOps.

Power to Process

To make use of the data streams, AIOps tools need serious analytical capacity behind them. Whether provided in data center resource pools or in a service provider cloud infrastructure, AIOps is hungry for compute power to drive event correlation, real-time alerting and response. Beyond that, it also needs powerful analytical capacity to deliver the many, overlapping layers of non-real-time analysis IT needs, such as application usage, application performance per each user, overall and detailed network health, and equipment health and lifecycle management.

Levers and Strings

And, where AIOps is not built directly into the core of network management, it needs access to the means to act. It needs there to be an SDN and SD-WAN controller, through which it can drive changes in configuration. Or it needs comprehensive APIs for the network underlay as well as any overlaid applications and services, or equivalent means of automating both modifications to intelligence gathering—the AI needs to be able to tweak the streams of data being sent to it—and modifications to packet handling.

What IT Should Look for AIOps to Deliver

IT teams should look for several specific kinds of value from AIOps tools: improved understanding of the network and its performance with respect to enterprise needs; proactive assistance in focusing on what is important, and in improving operations over time; support of operational processes; and the ability to work across the whole network ecosystem.

Understanding

AIOps will help IT teams understand their networks better, in two ways. First, it will restore a level of understanding of the network that IT had many years ago, when networks were smaller, simpler, and changed less often. IT teams could understand what their networks would and could do. But networks have become vastly more complex and dynamic, and connect to orders of magnitude more devices. AIOps tools can take in endless data streams describing the state of this entangled mass and turn it into actionable and comprehensible intelligence—a human-understandable picture of what is going on.

AIOps should deliver:

- Deeper understanding
- Proactive focus
- Root cause analysis
- Process support
- Process integration

Secondly, AIOps will deliver new levels of understanding, things IT was never able to do well in the past (if at all). AIOps tools, through analytics as well as the breadth of scope of the information they assess, will uncover previously unavailable kinds of performance visibility. They will allow IT to see, in near real time as well as with trending over time and predictions for the future, how well the network is doing in delivering a given app, or serving a specific user, site, or device, and in any combination needed.

Practically speaking, an AIOps tool, once receiving network operations data, should begin seeing patterns in that data and reporting them to the network admins, who can then train the AI to understand context:

- "I see thousands of managed nodes coming on the network every day between the hours of 7AM and 9AM, Monday through Friday. I see thousands of unmanaged nodes come on at the same time. Most drop off the network again between 4PM and 7PM."
  Admins can identify this as normal behavior.

- "I see remote sites using both MPLS and Internet connectivity, except sites LA-1, Chi-12, and NYC-30, which are using only their Internet links."
  Admins can tag the former as normal and the latter as anomalous—and begin troubleshooting immediately, expecting an alert the next time such a situation is detected.

By focusing attention not just on symptoms but on actual causes, AIOps tools conserve IT's most precious resource: the attention of the staff.

Proactive Focus and Root Cause Analysis

One of the biggest ways AIOps tools help IT teams tackle network problems is by applying intelligent filtering to alerts and alarms. Network teams, like security teams, suffer from an abundance of alarms and alerts coming in from every layer of the infrastructure and monitoring ecosystem. False positives are alerts raised in response to things that may look like network problems but are not in fact, or that simply repeat an alert that has already been delivered.

By correlating across data streams and applying human-like reasoning to an array of alerts from various layers of the infrastructure, AIOps tools help eliminate false positives. They can discard thousands of alerts that are repetitious and consolidate hundreds or thousands of alerts from different components into a single one pointing at the root cause of the whole constellation of related problems.

By alerting IT only when it needs to be alerted and focusing attention not just on symptoms but on actual causes, AIOps tools conserve IT's most precious resource: the attention of the staff.

Taking proactive data analysis a step further, AIOps tools can engage in diagnostic modeling: look at actual behaviors, at the underlying infrastructure, and at trends in use, and suggest ways to make the network better at its job:

- What changes could improve reliability, such as adding one more Internet link to WAN sites with specific connectivity problems
- What changes could improve security?
- How should WAN traffic be routed to deliver optimal performance or to optimize costs? When should capacity be added?
- Which configuration modifications will boost performance, or eliminate problems?

Moreover, mature AIOps tools, especially those built and operated by network service providers, will be able to do some of this out of the box, based on knowledge accumulated from other networks and network and security teams.

AIOps tools can drive improvements in customer satisfaction while also reducing the number of trouble tickets IT gets. Performance against all service delivery metrics should improve.

Process Support and Integration

AIOps tools should also be able to fit into operational processes. They should literally integrate, via API at least, into ticketing systems, for example, so that they can create and update tickets for real incidents. They should also integrate functionally. For example, they should play a key role in incident response processes, starting with providing the alerts that trigger a response plan. Beyond that, their ability to assist in root cause analysis and to provide guidance on remedial action should put them at the center of incident response.

More broadly, their ability to learn and automate repetitive actions will give them a central role in other support processes as well. If network engineers have written a bit of ad-hoc automation, AIOps tools should be able to absorb it, and to provide intelligent support for it (e.g. knowing how to re-execute a set of actions against network nodes unreachable at the time of initial execution).

To do everything it can for the organization, an AIOps tool must be able to integrate with or into the core network management and security platforms for all three primary pieces of the network: WAN, campus, and data center.

What AIOps Can Do for the Business of IT

By reducing the time it takes to solve problems, as well as by helping IT avoid problems in the first place through proactive configuration tuning, AIOps tools can drive improvements in customer satisfaction while also reducing the number of trouble tickets IT gets. Performance against all service delivery metrics should improve.

At the same time, AIOps will help IT raise its profile organizationally, and shift its focus from tactical support of network services (bound always by low-level operations and attention to components) to strategic support of business initiatives. Improved visibility into service delivery, and the ability to truly map network performance to business value, will make AIOps tools central to IT's support of transformational technology deployments and business initiatives. Ultimately, being able to wield such tools to automate tactical response to strategic problems should create an upward career path for network engineers.

Conclusions and Recommendations

AIOps tools, though in their early days, are on the path to transforming IT's relationship to the network infrastructure by harnessing the tools of AI and analytics to automate huge new swathes of network operations. Through the application of artificial reasoning and the ability to learn and self-modify, such tools will be able to provide the equivalent of digital twins of the network administrators and engineers—helpers, teachers, and ever-vigilant watchdogs, able to intelligently watch, efficiently warn about, effectively act on, and proactively improve the network as a driver of business value.

IT Professionals should:

- Assess their, and their networks', readiness: can the network give an AIOps tool the kinds of information feeds and architectural support it needs to be effective?
- Asses the kind of AIOps tool—standalone, or built into a management portal for key infrastructure or network services—that will work best for their network given the ways in which it can support integration (e.g. via SDN and SD-WAN controllers, or device APIs, or CLIs, etc.), and where their greatest staffing and performance challenges lie
    - If working with a service provider, how well is that provider's own infrastructure tailored to provide the AIOps tool all the data it needs, and the ability to act effectively on the enterprise's behalf? How long has the tool been in production use, and how many years of operational data have gone into its training?
- Start slowly, and early: use AIOps for visibility first, and expect to take time to teach it their context before looking to it for automated responses (hence the importance of starting early)
- Use the analysis AIOps provides to fine tune their own operations playbooks before attempting to automate them
- Learn to trust: Lay out a timeline for moving from "show me the button to push" to "tell me you just fixed something" with a rising level of importance over time (and plans how to fall back a level if a step pushes past the tool's abilities).