moogsoft®

The Virtual NOC Is Here to Stay: AIOps Is Its Beating Heart

May 2020

WHITE PAPER

Introduction

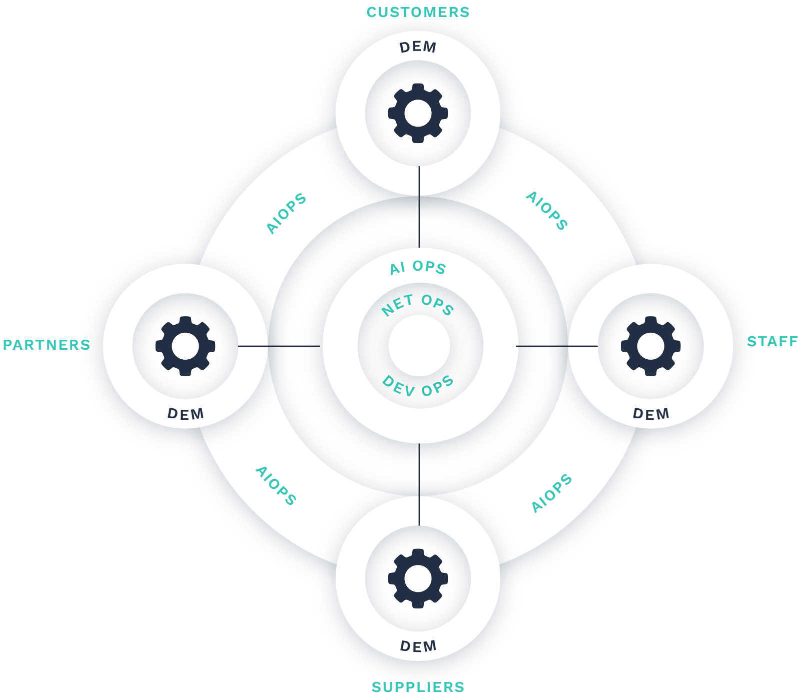
The sudden shift to remote work caused by the global pandemic has forced IT Ops and DevOps pros to quickly adjust in multiple ways to maintain the uptime and stability of critical digital services.

Amidst this crisis, AIOps has emerged as a lifeline, as it facilitates remote collaboration, streamlines incident management, and accelerates detection and resolution. For that reason, AIOps has become the foundation of virtual NOCs (network operations centers) that Ops teams forced to telework must create to communicate and collaborate effectively.

However, far from a temporary phenomenon, the virtual NOC will be a permanent fixture and key element of IT organizations, one of many IT trends whose maturity the current crisis has accelerated.

Given the present and future importance of virtual NOCs for service assurance, and the role AIOps plays in them, we've created this white paper to offer guidance and best practices on key topics, including:

- The multiple ways the sudden, global shift to remote work has impacted Ops teams
- The limitations and inefficiencies of the physical NOC, and why it's now obsolete
- The advantages of virtual NOCs, and why AIOps is a key component
- The comprehensive and unique capabilities Moogsoft AIOps offers for virtual NOCs



AIOps holds the virtual NOC together and powers Ops teams' digital experience management (DEM)

The "New Normal" for Ops

Having been forced to vacate their offices and on-premises NOCs, IT Ops and DevOps pros must still effectively communicate and collaborate while working from home. On top of that, traffic and usage patterns on their IT infrastructures have changed, putting stress on systems and topologies at all stack layers.

As staff, partners, suppliers and clients connect from dispersed endpoints, Ops teams must adapt architectures and management processes to address both temporary and permanent shifts in consumption of their enterprise IT services.

Moreover, due to illness and the economic downturn, Ops staff sizes will fluctuate, intensifying the importance of automating processes. Thus, service assurance has become more challenging, as Ops teams adapt to telework, while scrambling to adjust their IT environment.

Simultaneously, the pressure on preventing outages has increased, because the shutdown of physical channels has made digital services, transactions and interactions even more crucial.

All of these complications brought about by the pandemic pile on top of all the challenges that Ops teams have encountered in recent years. As IT environments have become more distributed, dynamic and componentized, they generate higher quantities and variety of data, making them harder to monitor.

In response, Ops teams have acquired a growing number of point, domain-specific monitoring tools that use rigid, history-based rules and models, meaning they can't anticipate and respond to unknown issues and anomalies. Also, these heterogeneous tools don't always interoperate, and are often deployed in a haphazard way. This creates workflow fragmentation and data silos.

As a result, Ops teams have realized they need an overarching technology that acts as an orchestrating layer that synthesizes the observations from all these tools, providing a holistic, continuous view of an IT environment's status.

The Twilight of the Physical NOC

The trend towards facilitating remote collaboration within IT organizations has been ongoing for years, and for good reason. IT teams are never all assembled in the same location all the time: People occasionally telework, while entire groups work out of satellite offices, often in different time zones and different countries.

Ops teams lagged behind in this trend. Preferring to work on site, they've historically had a certain resistance to automating processes and streamlining workflows, trusting more in their perceived effectiveness of in-person interactions.

But the reality is that being on site doesn't ensure efficiency for Ops staff. Team members can still be siloed and struggle collaborating because they use different tools that don't interoperate nor share data.

It's also well known that all-hands war rooms are rarely effective: Everyone is looking at their own laptops with their limited slice of data, and trying to shift and assign blame, causing costly delays in detecting, diagnosing and fixing issues.

In short, being in the same room in and of itself is of little help to Ops pros struggling to make sense of the vast amount, variety and complexity of monitoring data generated by modern IT environments.

As the pandemic has shown, Ops teams can't be dependent on on-site work environments for ensuring service availability. As forward-looking Ops teams have already done in recent years, they must transform processes and adopt technology that allows them to continue working — from anywhere. These Ops teams have found AIOps to be a game changer.

The benefits of embracing AIOps to build a virtual NOC boil down to this: Being able to ensure the uptime and availability of key digital services, regardless of where Ops team members are physically located.

The Dawn of the Virtual NOC

In recent years, AIOps has been tapped by thousands of IT Ops and DevOps teams in global enterprises to tame their growing IT operational complexity and prevent costly outages. Now, in this dawning era of the virtual NOC, AIOps has taken a major leap, going from being a successful next-gen technology to being the key for continuous assurance of critical services.

In other words, AIOps is the fabric that holds together the virtual NOC and helps Ops teams by facilitating remote collaboration, and by streamlining and automating event management. Specifically, as new, quickly-evolving types of incidents sprout up, AIOps allows Ops teams to detect and analyze new anomalies which can cause outages rapidly and stealthily. It does this in a way that legacy rules-based tools can't deliver.

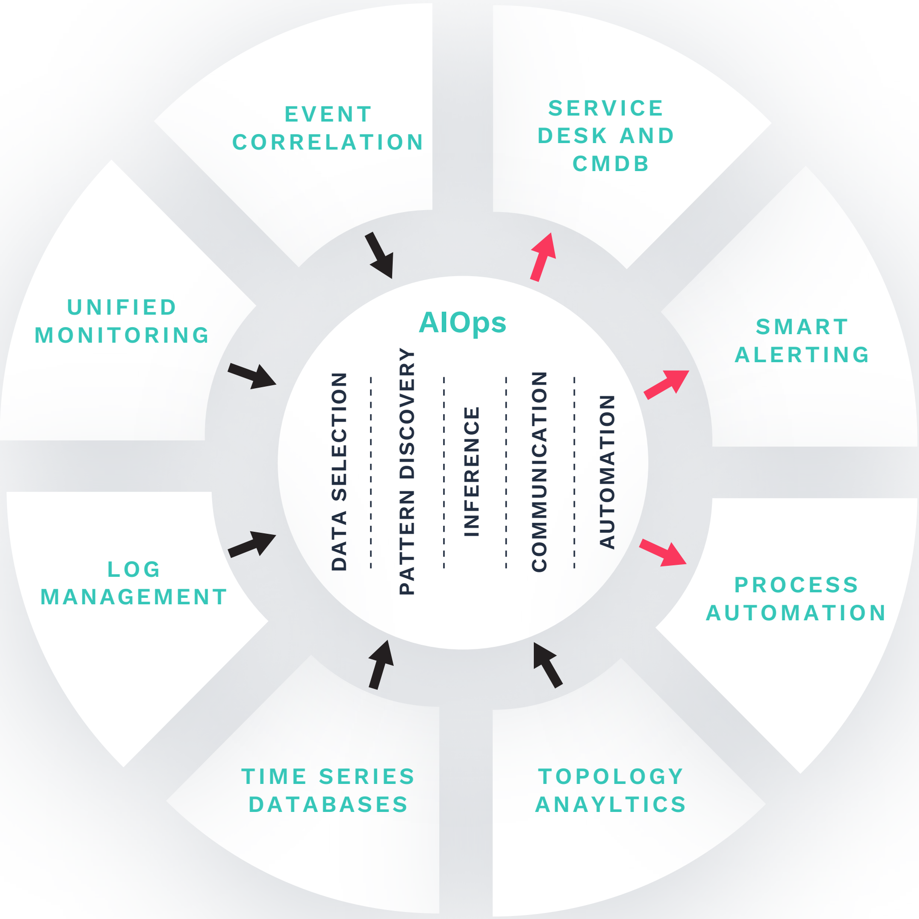
Optimizing the problem-resolution workflow so that it can be performed faster, more precisely, and with fewer manual processes is crucial for Ops teams that find themselves displaced from their office and working from home. They don't have to spend time and energy sifting through massive amounts of monitoring data, hoping to find the handful of needles — alerts — in the haystack, and then figuring out how they're related, and which one is causing the problem.

With AIOps, they can be efficient with their time, focusing on the truly valuable work of solving the issues. The heavy lifting, laborintensive work of ingesting, analyzing and correlating alerts, and of identifying probable root causes, is done for them.

This way, they systematically and efficiently stay on top of all ITSM workflows and processes, such as the management of configurations, changes, releases, availability and capacity, and ensure they are all running optimally, drastically reducing the risk of service disruptions, degradations and full-blown outages.

However, AIOps isn't one technology, and not all AIOps solutions in the market are created equal. To support the key functions of a virtual NOC, the underlying AIOps platform must address five very specific and essential algorithmic dimensions:

- data selection and normalization, for selecting and surfacing the most relevant information out of the "noisy" stream of IT data



The five algorithmic dimensions an AIOps platform must have to anchor a virtual NOC

- pattern discovery, for correlating and finding relationships between events across the tool stack
- inference, for identifying root causes and recurring issues
- communication / collaboration, for identifying and notifying the appropriate operators and teams
- automation, for automating processes for remediation

In a real-world virtual NOC, this is how such an AIOps platform supports the workflow of an Ops team, augmenting its capabilities through algorithmic analysis and automation.

The AIOps platform ingests vast amounts of all types of monitoring data from all sources in the IT environment — applications, networks, infrastructure, cloud instances and more. Using entropy algorithms, it removes noise and duplication, and selects truly relevant data. It then correlates and groups this data using various criteria, like text, time and topology.

PHYSICAL NOC		**VIRTUAL NOC**
Many Screens	→	UI-Embedded Consoles
Central Location	→	Virtual Room
Manual Detection	→	Probable Root Cause
War Room & Bridge Call	→	Bidirectional Collaboration
Manual Processes	→	Automated Workflows
Slow to Resolve	→	Streamlined Remediation

These are the key benefits of switching from a physical NOC to a virtual NOC

Next, it discovers patterns, and infers which data items signify causes. It then communicates the analysis results to a virtual collaborative environment, whose members will oversee automated repair responses.

For Ops teams, this means benefitting by going:

- From individual screens with fragmented data, to shared, UI-embedded consoles with comprehensive data, insights and context;
- From working in a central location where not everyone can be present, to collaborating in a virtual room where everyone can gather from anywhere, ensuring the right people with the right skills are engaged in solving the problem;
- From error-prone manual detection of issues, to algorithmically analyzed and precise root cause diagnosis;
- From chaotic and contentious all-hands meetings, to a virtual collaborative environment where everyone has access to the same data and is focused on problem resolution;
- From slow manual processes and resolution delays, to automated workflows and streamlined remediation

A virtual NOC underpinned by an AIOps platform gives Ops teams the flexibility, speed, and agility they need to quickly detect, identify and resolve issues before business-critical digital services are impacted and customers are affected. An AIOps-fueled virtual NOC allows Ops teams to work from anywhere, and to monitor and manage highly dynamic and complex IT environments — during normal times and during a global crisis that upends all aspects of life and work.

In summary, AIOps acts as the brain and central nervous system of the virtual NOC, coordinating and bringing together all processes, data and tools involved in the IT operations workflow.

The Economic Value of an AIOps-Supported Virtual NOC

The financial benefits a business derives from creating a virtual NOC founded on AIOps technology go way beyond reducing costs. This is not to say AIOps doesn’t significantly help cut costs in multiple ways. For example, it automates manual processes, freeing up staff for higher-value work, and replaces existing products, eliminating their maintenance and licensing.

But AIOps goes much further, because its impact can be often directly traced to business benefits, especially as organizations become more and more dependent on digitization for all their operations. This has intensified even more during the current pandemic, as more transactions and interactions have shifted to the digital channels.

For example, AIOps helps prevent disruptions of critical digital services, and accelerates detection and resolution. In that way, an AIOps optimizes revenue generation, because when apps malfunction or crash, sales are lost. It also plays a direct part in customer experience, satisfaction and retention, as well as in brand reputation protection, all of which are directly related to business performance and profitability.

And it does all of this in an optimal way, at a speed and with a precision that's unmatched by manual processes and by legacy tools, even those that have been retrofitted and sprinkled with a little bit of AI.

Thus, the significant economic value of AIOps comes from its deployment as a platform that provides all five algorithmic dimensions described in the previous section. It's only through that type of application of AIOps that modern IT systems — highly modular, distributed, dynamic, and, at a component level, ephemeral — can be properly monitored and managed, and service assurance attained.

Take the real-world example of a large financial services institution, which cut its MTTR (mean time to resolution) by a whopping 85%, down to 100 minutes, and slashed its Level 1/2 tickets by 75%, its Level 3 tickets by 15%, and its Level 4 tickets by 50%. The financial benefit to the business: Tens of millions of dollars.

This was achieved via a multi-pronged strategy encompassing several key use cases, including:

- A dramatic improvement in the clustering of alerts around incidents. The company went from a very limited, inefficient process, to an AIOps-driven ingestion and correlation process that consolidated alerts into unique, contextually-rich incidents and a massive reduction of tickets.
- An integration with the ITSM / CMDB system. This drastically simplified and accelerated ticketing, leading to faster, more effective routing, prioritizing, handling and resolution of incidents.
- Automated knowledge capture and recycling. The company went from not being able to access historical knowledge on how prior incidents were resolved, to having the knowledge capture and recycling process totally automated. Now, operators are automatically notified of resolved past incidents that are similar to the one being worked on, and they have all the past resolution documentation at their fingertips, leading to exponentially faster MTTR.

This global financial services company reaped those benefits with their deployment of the Moogsoft AIOps platform. Read on to learn more about it.

The Moogsoft AIOps Platform: The Virtual NOC Engine

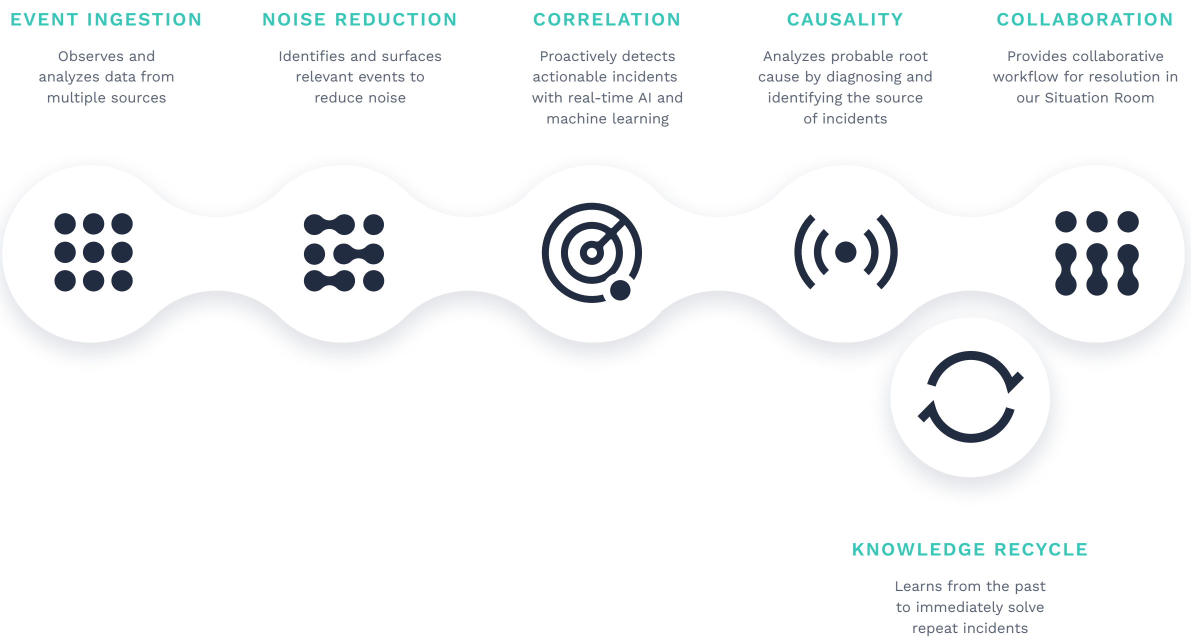
Moogsoft AIOps, a unified, collaborative platform for end-to-end incident management, incorporates AIOps' five dimensions, empowering IT Ops and DevOps teams to provide service assurance from virtual NOCs — during this crisis and beyond.

By adding a critical layer of intelligence between performance monitoring and ITSM systems, Moogsoft AIOps streamlines, automates and accelerates incident detection, diagnosis, and resolution.

With 50+ patented algorithms, it ingests IT data of all types from all tools and sharply reduces event noise. It then correlates and groups important alerts, and pinpoints root causes by tapping its stored collection of incident resolutions.

Finally, it facilitates cross-team collaboration via its unique Situation Room, a virtual war room where everyone involved in solving a problem can gather to communicate and work together accessing the same information from a single dashboard with all required context.

As such, Moogsoft AIOps has provided for years the necessary capabilities to support Ops teams in virtual NOCs. A raft



EVENT INGESTION

Observes and analyzes data from multiple sources

NOISE REDUCTION

Identifies and surfaces relevant events to reduce noise

CORRELATION

Proactively detects actionable incidents with real-time AI and machine learning

CAUSALITY

Analyzes probable root cause by diagnosing and identifying the source of incidents

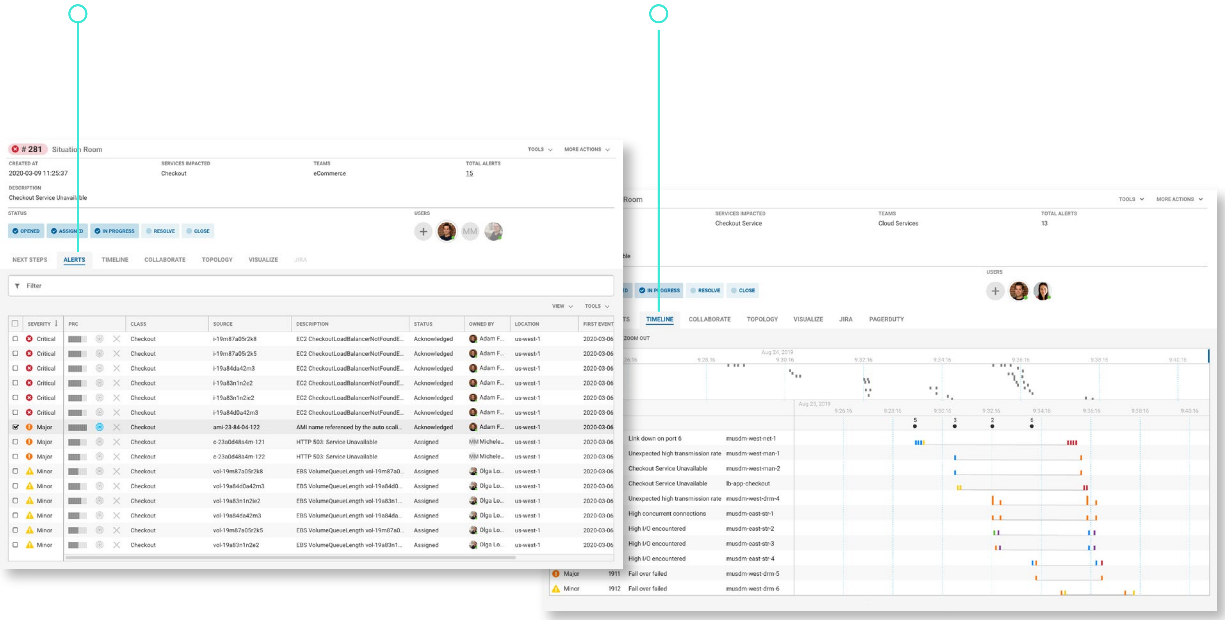
COLLABORATION

Provides collaborative workflow for resolution in our Situation Room

KNOWLEDGE RECYCLE

Learns from the past to immediately solve repeat incidents

The Moogsoft platform's implementation of the five algorithmic dimensions of AIOps



View all related alerts with root cause identifying the source so everyone is in sync and on the same page

See how the incident unfolds so you and your teams can focus troubleshooting where it's needed

CREATED AT 2020-03-09 11:25:37 · SERVICES IMPACTED Checkout · TEAMS eCommerce · TOTAL ALERTS 15

DESCRIPTION Checkout Service Unavailable

☐	SEVERITY	PRC	CLASS	SOURCE	DESCRIPTION	STATUS	OWNED BY	LOCATION	FIRST EVENT
☐	Critical		Checkout	i-19m87a05r2k8	EC2 CheckoutLoadBalancerNotFoundE...	Acknowledged	Adam F...	us-west-1	2020-03-06
☐	Critical		Checkout	i-19m87a05r2k5	EC2 CheckoutLoadBalancerNotFoundE...	Acknowledged	Adam F...	us-west-1	2020-03-06
☐	Critical		Checkout	i-19a84da42m3	EC2 CheckoutLoadBalancerNotFoundE...	Acknowledged	Adam F...	us-west-1	2020-03-06
☐	Critical		Checkout	i-19a83n1n2e2	EC2 CheckoutLoadBalancerNotFoundE...	Acknowledged	Adam F...	us-west-1	2020-03-06
☐	Critical		Checkout	i-19a83n1n2ie2	EC2 CheckoutLoadBalancerNotFoundE...	Acknowledged	Adam F...	us-west-1	2020-03-06
☐	Critical		Checkout	i-19a84d0a42m3	EC2 CheckoutLoadBalancerNotFoundE...	Acknowledged	Adam F...	us-west-1	2020-03-06
☑	Major		Checkout	ami-23-84-04-122	AMI name referenced by the auto scali...	Acknowledged	Adam F...	us-west-1	2020-03-06
☐	Major		Checkout	c-23a0d48a4m-121	HTTP 503: Service Unavailable	Assigned	MM Michele...	us-west-1	2020-03-06
☐	Major		Checkout	c-23a0d48a4m-122	HTTP 503: Service Unavailable	Assigned	MM Michele...	us-west-1	2020-03-06
☐	Minor		Checkout	vol-19m87a05r2k8	EBS VolumeQueueLength vol-19m87a0...	Assigned	Olga Lo...	us-west-1	2020-03-06
☐	Minor		Checkout	vol-19a84d0a42m3	EBS VolumeQueueLength vol-19a84d0...	Assigned	Olga Lo...	us-west-1	2020-03-06
☐	Minor		Checkout	vol-19a83n1n2ie2	EBS VolumeQueueLength vol-19a83n1...	Assigned	Olga Lo...	us-west-1	2020-03-06
☐	Minor		Checkout	vol-19a84da42m3	EBS VolumeQueueLength vol-19a84da...	Assigned	Olga Lo...	us-west-1	2020-03-06
☐	Minor		Checkout	vol-19m87a05r2k5	EBS VolumeQueueLength vol-19m87a0...	Assigned	Olga Lo...	us-west-1	2020-03-06
☐	Minor		Checkout	vol-19a83n1n2e2	EBS VolumeQueueLength vol-19a83n1...	Assigned	Olga Lo...	us-west-1	2020-03-06

SERVICES IMPACTED Checkout Service · TEAMS Cloud Services · TOTAL ALERTS 13

		Link down on port 6	musdm-west-net-1
		Unexpected high transmission rate	musdm-west-man-1
		Checkout Service Unavailable	musdm-west-man-2
		Checkout Service Unavailable	lb-app-checkout
		Unexpected high transmission rate	musdm-west-drm-4
		High concurrent connections	musdm-east-str-1
		High I/O encountered	musdm-east-str-2
		High I/O encountered	musdm-east-str-3
		High I/O encountered	musdm-east-str-4
Major	1911	Fail over failed	musdm-west-drm-5
Minor	1912	Fail over failed	musdm-west-drm-6

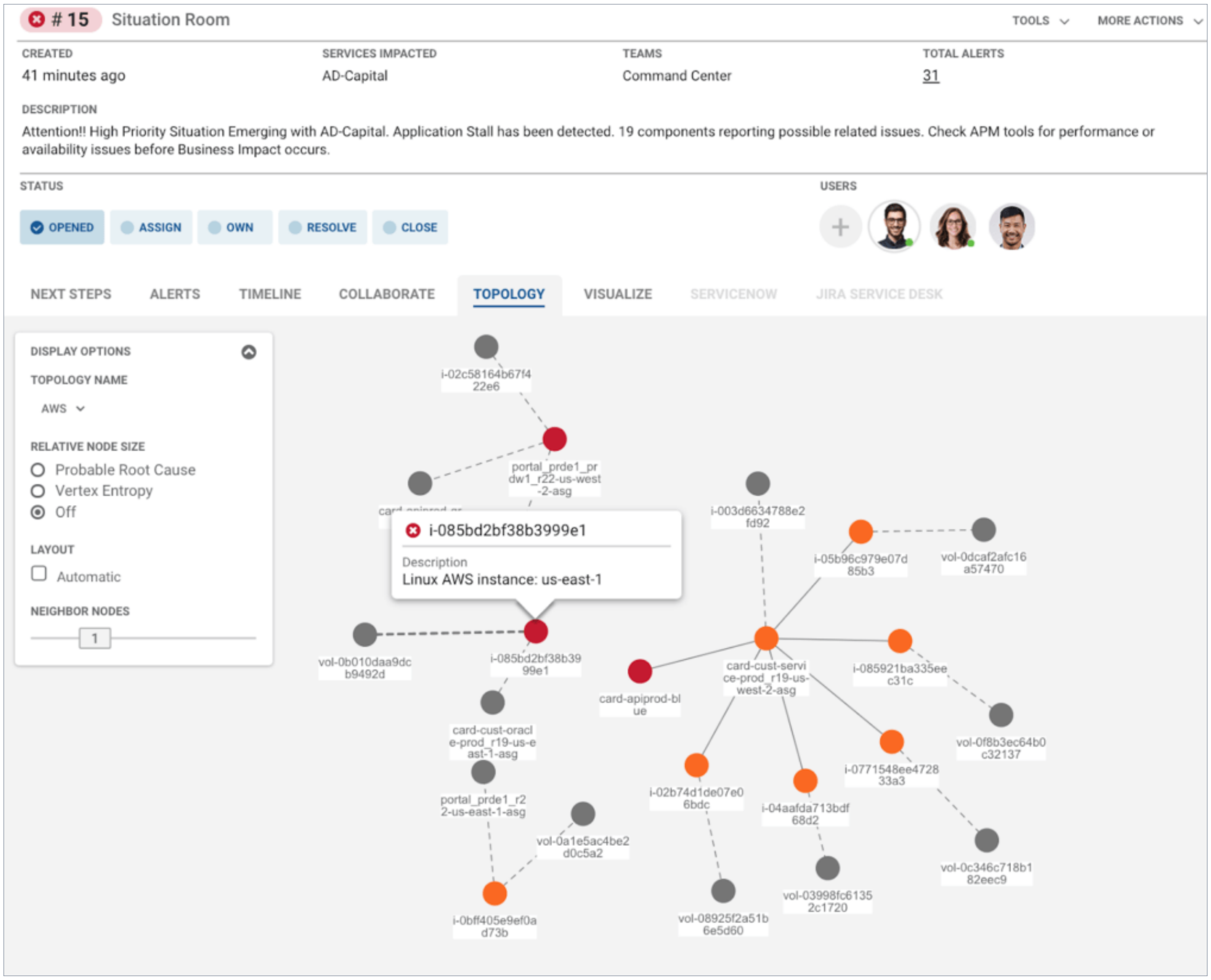
A snapshot of the collaborative event resolution workflow of the Moogsoft AIOps Situation Room

of groundbreaking and unique new features added to the platform in May strengthen its capabilities even more.

A major new feature is the Dynamic Topology Builder, which boosts the platform's already strong capabilities for probable root cause analysis, putting Moogsoft AIOps in an entirely different level from all other competitors.

The Dynamic Topology Builder provides the virtual NOC with greater level of visibility into the correlation process, based on logical, virtual and physical topological relationships. It allows Ops teams to immediately gain expanded insights into incidents in real time, and visualize the probable root cause and potential impact associated with current and neighboring services.

This type of topology capability is critical for remote Ops teams because it graphically illustrates algorithmic processes and results in a way that brings visibility and understanding to people who aren't necessarily data scientists and mathematicians. By helping Ops teams visualize problems and solutions with the Dynamic Topology Builder, Moogsoft boosts their capacity to think and make decisions.



15 Situation Room

CREATED: 41 minutes ago

SERVICES IMPACTED: AD-Capital

TEAMS: Command Center

TOTAL ALERTS: 31

DESCRIPTION

Attention!! High Priority Situation Emerging with AD-Capital. Application Stall has been detected. 19 components reporting possible related issues. Check APM tools for performance or availability issues before Business Impact occurs.

STATUS: OPENED

DISPLAY OPTIONS

TOPOLOGY NAME: AWS

RELATIVE NODE SIZE

○ Probable Root Cause
○ Vertex Entropy
● Off

LAYOUT

□ Automatic

NEIGHBOR NODES: 1

i-085bd2bf38b3999e1

Description

Linux AWS instance: us-east-1

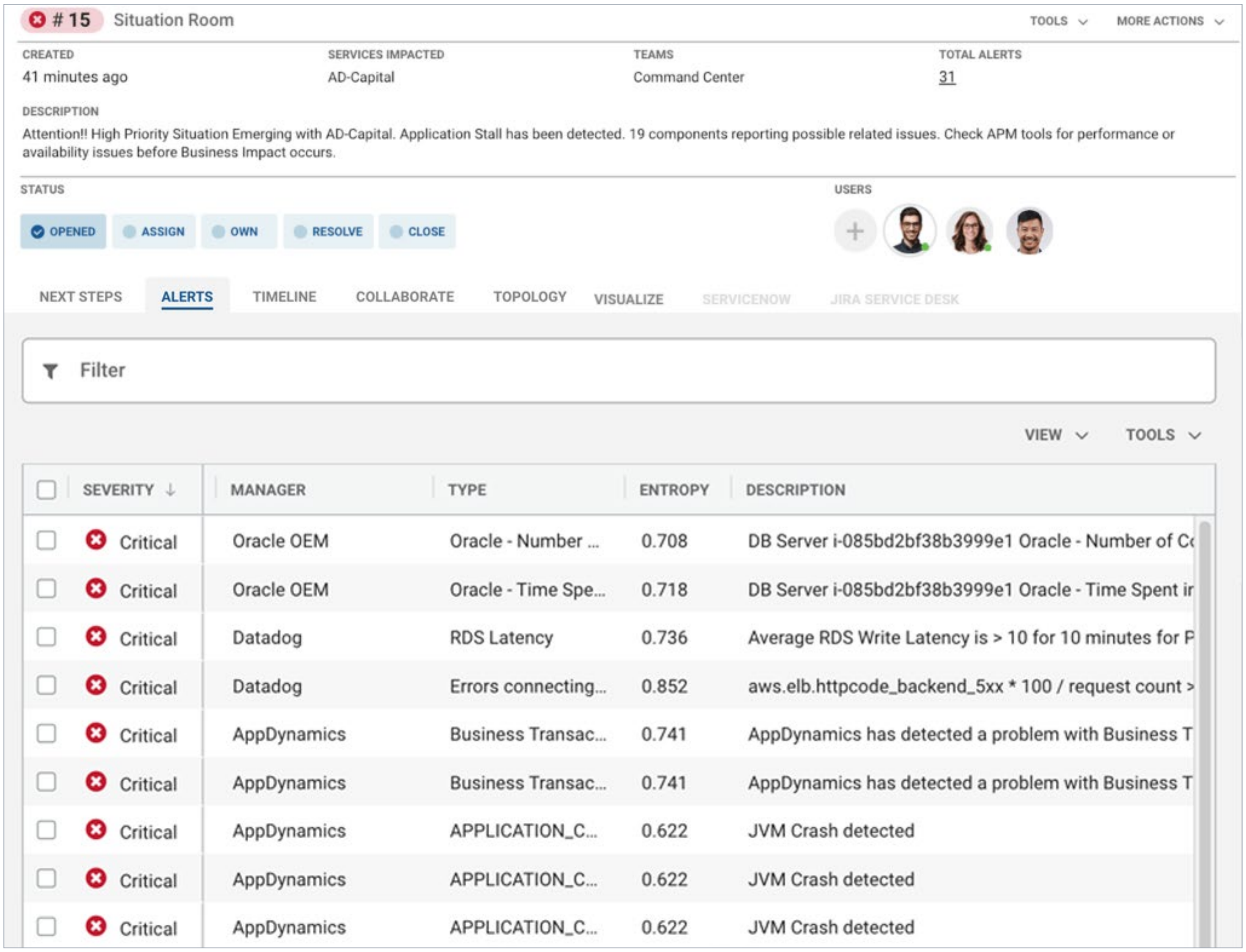
Nodes in the Dynamic Topology Builder representing AWS EC2 Instances and related services

Here we highlight several other important features released with Moogsoft Enterprise 8.0.

Alert Analyzer

The Alert Analyzer uses Moogsoft's patented Entropy algorithm to automatically tame the flood of noisy events and alerts before they overload the Ops teams working in virtual NOCs. It gives them an intuitive user interface (UI) to visually configure, identify anomalies within, and fine tune the platform's alert processing.

Each ingested event or alert is assigned a value between 0 and 1 to indicate its importance. The Alert Analyzer offers a dynamic graph to display the alert and the entropy value distribution, providing transparency for users to more precisely view the important alerts.



CREATED	SERVICES IMPACTED	TEAMS	TOTAL ALERTS
41 minutes ago	AD-Capital	Command Center	31

DESCRIPTION

Attention!! High Priority Situation Emerging with AD-Capital. Application Stall has been detected. 19 components reporting possible related issues. Check APM tools for performance or availability issues before Business Impact occurs.

STATUS

● OPENED ○ ASSIGN ○ OWN ○ RESOLVE ○ CLOSE

□	SEVERITY ↓	MANAGER	TYPE	ENTROPY	DESCRIPTION
□	Critical	Oracle OEM	Oracle - Number ...	0.708	DB Server i-085bd2bf38b3999e1 Oracle - Number of Co
□	Critical	Oracle OEM	Oracle - Time Spe...	0.718	DB Server i-085bd2bf38b3999e1 Oracle - Time Spent ir
□	Critical	Datadog	RDS Latency	0.736	Average RDS Write Latency is > 10 for 10 minutes for P
□	Critical	Datadog	Errors connecting...	0.852	aws.elb.httpcode_backend_5xx * 100 / request count >
□	Critical	AppDynamics	Business Transac...	0.741	AppDynamics has detected a problem with Business T
□	Critical	AppDynamics	Business Transac...	0.741	AppDynamics has detected a problem with Business T
□	Critical	AppDynamics	APPLICATION_C...	0.622	JVM Crash detected
□	Critical	AppDynamics	APPLICATION_C...	0.622	JVM Crash detected
□	Critical	AppDynamics	APPLICATION_C...	0.622	JVM Crash detected

Each alert is analyzed and scored by Moogsoft's patented Entropy algorithm

The key here is to eliminate the noisy, non-actionable alerts without being forced to write a unique rule for each alert type and associated action. This automation of event and alert analysis happens before correlation. That way, there's more context and similar alerts across multiple technology domains being correlated, accelerating mean time to resolution for incident management.

Enhanced Workflow Engine

This new version of Workflow Engine (WE) enables customers to configure workflows and drive outcomes through an intuitive UI for each of the WE modules:

- Ingest: delivers user control for advanced configuration of the event flow.
- Enrich: enables customers to quickly enhance incoming data streams with external data sources including CMDB data directly from ServiceNow.

- Automate: delivers new functionality with Ansible and Puppet to drive advanced remediation solutions.
- Ticket: allows bi-directional integration into tools such as ServiceNow, Remedy and Cherwell.
- Collaborate: easily configure PagerDuty, xMatters and Slack for users to directly communicate with the Situation Room team members.

Enhanced Correlation and Versioning of ML Configurations

Version 8.0 delivers new platform functionality for transparency and control over the deployment of ML algorithms. New versioning, rollback and history capabilities allow customers to audit new deployments, enabling them to add, track, delete and change ML algorithms where necessary.

New Integrations

New out-of-the-box integrations — including with AWS Firelens to ingest EC2 log files and with Opsgenie for on-call management — are easily deployed via the UI and accelerate customers' time to value.

In addition, a new joint solution based on a bidirectional integration with PagerDuty for alert notification engages DevOps engineers in seconds, pointing them in the right direction with contextual and proactive insights to resolve incidents early and quickly.

Real World Examples of Virtual NOCs

Already, there are global enterprises leveraging Moogsoft AIOps for virtual NOCs.

- JetBlue's NOC staff in the US and India are now working from home to monitor, troubleshoot and resolve issues, ingesting data from AppDynamics, Extrahop, Nagios and SolarWinds. The Moogsoft AIOps Situation Room has been the key feature.
- After a major railway company sent all employees to work from home, its executives were complaining of intermittent home-office connectivity problems. The IT team was seeing uncharacteristic usage patterns, and could not diagnose the problem. Using Moogsoft AIOps, they were able to quickly identify and fix the issue, restoring the productivity of the affected users.
- A major global online company is using Moogsoft to monitor their Zoom conferencing across data centers in the US, Europe and APAC for global employees. The client is also monitoring three different wireless systems so it can pinpoint the source of problems due to infrastructure. The Ops team using Moogsoft is located in the U.S. and India.
- A large enterprise used the Moogsoft AIOps Situation Room to manage an issue affecting their VPN, a crucial

functionality with its workforce now dispersed globally and connecting to its network from their homes. The organization was able to detect, identify, diagnose and fix the problem quickly, thanks to the visibility provided by Moogsoft AIOps, which assesses network services as a coherent whole, looking at all layers of the OSI (Open Systems Interconnection) stack simultaneously.

Conclusion

With AIOps, Ops teams working from anywhere can build a virtual NOC and regain visibility and control over the scale and complexity of their modern IT environments, and ensure the uptime and reliability of digital services.

AIOps lays the foundation for a virtual NOC by automating the analysis of the oceans of noisy IT data, and by facilitating remote collaboration of Ops teams working from home — or anywhere.

With an AIOps-powered virtual NOC, Ops teams put themselves in a position to provide continuous service assurance at all times, regardless of where their team members are located, and whether a major crisis has created global disruptions.

For more information visit:
moogsoft.com/vNOC

Moogsoft is a pioneer and leading provider of AIOps solutions that help IT teams work faster and smarter. With patented AI analyzing billions of events daily across the world's most complex IT environments, the Moogsoft AIOps platform helps the world's top enterprises avoid outages, automate service assurance, and accelerate digital transformation initiatives. Founded in 2011, Moogsoft has more than 130 customers worldwide including SAP SuccessFactors, American Airlines, Fannie Mae, Verizon Media Group, and HCL Technologies. It has established strategic partnerships with leading managed service providers and outsourcing organizations including AWS, Cisco, HCL Technologies, TCS, and Wipro.

www.moogsoft.com

moogsoft®

MOOGSOFT | 1265 BATTERY ST., SAN FRANCISCO, CA 94111