Brought to you by Moogsoft

Observability with AIOps

for dummies®
A Wiley Brand

Moogsoft Special Edition

Get full observability on modern IT

Automatically identify issues faster

Know what to fix before trouble occurs

Adam Frank

About Moogsoft

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 2012, Moogsoft has more than 140 customers worldwide, including American Airlines, Fannie Mae, Fiserv, HCL, SAP SuccessFactors, and Verizon Media. For more information about Moogsoft, please visit **https://moogsoft.com.**

Observability with AIOps

Moogsoft Special Edition

by Adam Frank

for dummies®
A Wiley Brand

Observability with AIOps For Dummies®, Moogsoft Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

ISBN 978-1-119-73528-1 (pbk); ISBN 978-1-119-73529-8 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Elizabeth Kuball

Development Editor: Colleen Diamond

Executive Editor: Steven Hayes

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Production Editor: Siddique Shaik

Special Help: Will Cappelli, Amer Deeba, Robert Harper, Michele de la Menardiere, Juan Perez, Phil Tee, and Dave Buerger (consulting)

Table of Contents

INTRODUCTION 1
Foolish Assumptions 1
Icons Used in This Book 2
Beyond the Book 2

CHAPTER 1: **Getting How AIOps Benefits DevOps and Site Reliability Engineering** 3
Identifying Challenges for DevOps and Site Reliability Engineering 4
Understanding How AIOps Improves Service Assurance 4
Unlocking True Operational Visibility 5
Attaining 100 Percent Observability 6

CHAPTER 2: **How AIOps Works under the Hood** 7
Considering the AI in AIOps 8
Understanding What Artificial Intelligence Actually Does 8
Considering Algorithm Learning Techniques 9
Machine learning 9
Unsupervised machine learning 9
Supervised machine learning 9
Reinforced learning 10
Seeing How Neural Networks Mimic the Brain 11
Using Deep Learning for New Advances 11
Moving Beyond Rules with AI 12

CHAPTER 3: **Understanding the AIOps Workflow** 13
Visualizing the AIOps Workflow 13
Ingesting and Normalizing Data 14
Context with data enrichment 14
Benefits of AI data analysis 15
Reducing Noise and Detecting Anomalies 15
Reduction by deduplication 16
Enhancing deduplication with entropy 16
Benefits of reducing noise with entropy 17
Correlating Alerts 17
Fine-tuning alert correlation 18
Benefits of correlation 19

Discovering Causality: The Root Causes of Issues 19
How causality identifies root causes of issues 19
Where to look to fix an incident 20
Benefits of root cause analysis 20
Collaborating to Resolve Issues 20
Collaboration capabilities 21
Insight with visualization 21
Benefits of collaboration 22

CHAPTER 4: **Use Cases for DevOps and Site Reliability Engineering** 23
Managing Digital Transformation 23
Enhancing Collaboration and Productivity 25
Streamlining IT Incident Management 26
Automating IT Service Assurance Workflows 27
Reducing Costs 28

CHAPTER 5: **AIOps as a Hub of Integration** 29
Integrating Data Streams 29
Having a Unified View 30
Synchronizing Integrated Data Flows 31
Automating Workflows by Enriching Data 33
Getting the Benefits of Integration 36

CHAPTER 6: **Using Moogsoft Express for DevOps and Site Reliability Engineering** 37
Choosing Moogsoft Express 37
Knowing What Moogsoft Express Can Do 38
Visualizing Your Data with Moogsoft Express 39

CHAPTER 7: **Ten Tips for Getting Started with AIOps** 41

APPENDIX: GLOSSARY 43

Introduction

Artificial intelligence for IT operations (AIOps) is a scalable technology for streamlining the complexities of IT. AIOps helps DevOps and site reliability engineering (SRE) teams quickly identify and fix issues that affect the performance of an organization's apps and vital services.

Observability with AIOps For Dummies helps you understand how AIOps works. This book begins by describing AI, machine learning (ML), and neural network techniques. It shows how using AIOps can streamline the monitoring of operational data from applications, cloud services, networks, and infrastructure. The book ends by showing how you can easily and quickly apply AIOps technology in your organization.

Your operational goal is to automate observability — seeing and understanding everything necessary to ensure the top performance of apps and services. This book tells you how AIOps will get you there. It describes workflows to proactively get early detection of changing conditions so SRE and DevOps teams can detect and resolve incidents *before* they affect customers, partners, or employees. In this book, you find out how to effectively manage the agility that the company needs for improved responsiveness at scale, all from a single view with AIOps.

Foolish Assumptions

This book assumes you know absolutely nothing about AI. It assumes you are not a mathematician or a genius at algorithms. Nor do you need to know how to write an algorithm. You should, however, want to become familiar with what AIOps algorithms can do and their benefits for DevOps and SRE teams. If that's your motivation, step right up — you've come to the right place!

We assume that readers of this book are familiar with typical requirements and workflows for DevOps or SRE teams. Don't worry if you know about only one of these — AIOps automatically brings related benefits to these symbiotically linked domains.

Finally, we assume that you have basic familiarity with the interplay of applications, cloud services, networks, and IT infrastructure — particularly the benefits of monitoring operational activity in all these domains as fundamental for ensuring apps and services assurance.

Icons Used in This Book

Throughout this book's margins are special icons that call attention to important information. Here's what they mean:

TIP

The Tip icon gives you hints for a successful implementation of AIOps.

REMEMBER

Hold on to anything marked with the Remember icon as you plan and proceed on the AIOps journey.

TECHNICAL STUFF

No doubt about it: AI and its mathematical substructure may stretch the boundaries of familiarity for many of us! When we get a bit technical, we mark that information with the Technical Stuff icon. You can skip material marked with this icon without missing anything essential to the topic at hand.

WARNING

Anyone who works in DevOps or SRE expects that things in IT can blow up. This icon reminds you when something *can* be trouble and how to avert a disaster. Heed its advice, grasshopper!

Beyond the Book

The 48 pages of *Observability with AIOps For Dummies* are just enough space to get started on the ins and outs of AIOps. When you're ready for more, visit `https://moogsoft.com/resources` to find content that can further your understanding of AIOps. See the Glossary for definitions of AIOps-related terms used in this book.

IN THIS CHAPTER

- Recognizing the challenges presented by a growing digital economy
- Getting how IT modernization requires AIOps to improve service assurance
- Seeing how observability with AIOps unlocks true operational visibility

Chapter 1
Getting How AIOps Benefits DevOps and Site Reliability Engineering

In a growing digital economy that tolerates no downtime, DevOps and site reliability engineering (SRE) teams maintain increasingly large and complex infrastructure environments. These environments continue to grow in complexity as organizations strive to digitally transform nearly every aspect of their businesses, including how they engage with customers.

Today's DevOps and SRE teams must balance achieving faster, continuous development with maintaining increasingly diverse architectures, more applications, and elaborate infrastructure. AIOps is the secret sauce that helps these processes work smoothly.

Identifying Challenges for DevOps and Site Reliability Engineering

DevOps and SRE teams work to ensure that apps are continuously available. The cost of failure in this objective can be hefty. If a service failure crashes an app, it can hurt sales, damage an organization's brand, and disappoint customers. So, keeping apps running continuously is a prime objective for these teams.

In addition to keeping apps continuously running, DevOps and SRE teams must accommodate new ways of building and managing software that allow for continuous integration and delivery. Because today's digital economy is unforgiving of downtime, software updates must be implemented seamlessly, without interrupting service.

All these factors tremendously stress modern DevOps and SRE teams. Traditional systems management tools are proving woefully insufficient. AIOps presents a modern solution to these new challenges.

Understanding How AIOps Improves Service Assurance

IT modernization naturally brings new solutions to the table, which replace technology that no longer works. By introducing technologies such as AIOps to automate and improve service assurance, DevOps and SRE tasks can be streamlined. As you can imagine, in a fast-growing digital economy, any technology that streamlines DevOps and SRE tasks is likely to be your organization's new best friend.

AIOps improves service assurance by streamlining the following DevOps and SRE tasks:

- Rapid incident resolution (helps avoid service outages)
- Meeting service level agreements (SLAs) and service level objectives (SLOs)
- Managing error budgets
- Accelerating the digital transformation of a business

CASE STUDY: KEYBANK

KeyBank is a regional bank based in Cleveland, Ohio. As the 28th largest bank in the United States, KeyBank has customers that span retail, small business, corporate, and investment clients.

Problems: The complexity of working with more than 21 monitoring systems slowed mean time to repair (MTTR) and ability to identify the root cause of problems; caused poor mobile satisfaction scores; and produced poor branch workstation performance metrics.

Moogsoft Solution: Cloud-based AIOps for use by DevOps and SRE teams replaced on-premises legacy system with two days for setup; network operations center (NOC) training took one hour.

Integrations: Amazon CloudWatch; Elastic; ServiceNow; and WatchIT.

Results:

- Noise reduction stable at over 99.8 percent; reduced MTTR significantly.
- Streamlined incident detection, cause identification, and resolution; improved outage prevention and continuous service assurance; increased agility, automation, and collaboration in DevOps; much better return on investment (ROI).

For details, see `www.moogsoft.com/blog/aiops/keybank-aiops-success-story`.

REMEMBER

By using AI techniques, AIOps enables DevOps and SRE teams to quickly receive, understand, and prioritize the significant events that are most likely to cause downtime, affect the customer experience, or lead to missed SLAs and SLOs.

Unlocking True Operational Visibility

Observability is a buzzword in some DevOps and SRE circles. The ability to see what's going on in apps and supporting services is often equated with getting a river of metrics, traces, and log events. Although getting data is an important part of achieving visibility, getting value requires additional context with AIOps.

For example, knowing that the CPU usage on a server is at 94 percent means nothing if you don't know whether this level indicates normal functioning or a potential problem. And you must know much more, including the following:

- **What was it like yesterday?** Understanding performance over time provides a comprehensive picture; examining data from a single moment in time provides an incomplete picture and flawed conclusions.
- **What was it while doing something different?** Understanding server loads by task helps weight performance levels so that you can determine which tasks correlate to server loads that are an issue.
- **Is the server unique?** Is the server the only one supporting the app, or is the server part of a server farm?

REMEMBER

AIOps analyzes traditional metrics, traces, logs, and changes to provide a *complete* operational view for service assurance. Leveraging the contextual intelligence provided by AIOps is the means to unlock true operational visibility.

Attaining 100 Percent Observability

To ensure 100 percent observability and attain its enormous value, AIOps automates the following:

- Applies AI and machine learning algorithms to all data
- Detects anomalies and eliminates noise
- Correlates relevant metric anomalies, traces, changes, and log events triggered by incidents
- Surfaces incidents with contextual data
- Identifies probable root causes
- Helps DevOps and SRE teams resolve issues faster and prevents them from happening again in the future

REMEMBER

By providing contextual intelligence, AIOps helps DevOps and SRE teams achieve true visibility for services assurance.

IN THIS CHAPTER

- **Looking at artificial intelligence**
- **Identifying what artificial intelligence does**
- **Considering algorithm learning techniques**
- **Understanding how neural networks mimic the brain**
- **Marveling at the new advances brought by deep learning**
- **Moving beyond rules with artificial intelligence**

Chapter 2
How AIOps Works under the Hood

Artificial intelligence (AI) is technology used to create machines that imitate intelligent human behavior. To common Netflix-soaked humanoids, AI is a bigger-than-life "thing" that is taking over the world — and their jobs. They may associate HAL, the supercomputer in the movie *2001: A Space Odyssey*, with the same type of general AI that some data scientists have promised for half a century. Rest assured; it will be *quite* a while — possibly decades or centuries — before machines achieve general AI. Meanwhile, less flashy forms of AI, such as artificial intelligence for IT operations (AIOps), are taking over in other domains.

This book mostly describes what the *AI* in AIOps can do for DevOps and site reliability engineering (SRE) teams, but getting the gist of what's going on under the hood is also useful. For that, don your dummy's hat, because the next section turns to the very basics of AI.

Considering the AI in AIOps

AI is more than smart computers that threaten the world with domination. AI-driven "human" behavior is everywhere. It's in helpful digital assistants that you're familiar with, like Siri and Alexa. AI powers self-driving cars and unmanned aerial vehicles that fly themselves. It's also in robotics, image analysis, and bots that make you want to buy stuff or ask someone you've never heard of to be your friend.

But these are things that you can eventually see, hear, smell, taste, and touch. The power of AI that delivers these fruits with machines finds root in a single nonsentient word: *mathematics.*

TECHNICAL STUFF

AI data scientists love math, even more so than the joy many people felt when they were free to forget all the math ever learned in high school and college. At the risk of stirring bad memories, four types of math pertain to AI that are especially useful for AIOps:

- **Statistics:** These mathematical tools allow you to ask questions about and learn from the frequency of observed data. Statistics are the essence of machine-based learning.
- **Probability:** These tools help you predict the likelihood of future events. They're also crucial for machine learning (ML) because probability predictions help manage the uncertainty from incomplete data or evolving analytical models.
- **Multivariate calculus:** Other tools help analyze relationships between functions and related inputs. They're useful for models that learn by themselves without prescribed rules or supervised learning.
- **Linear algebra:** Think "lifeblood of machine learning," and you'll immediately grok the importance of linear algebra. It helps with behavior simulation, seeing how data clusters show significance, and injecting more confidence into predictions.

Understanding What Artificial Intelligence Actually Does

AI puts math to work by executing algorithms. The idea of an algorithm actually is quite simple. *Algorithm* is just a fancy word that means mathematical instructions a computer can follow. So, when AIOps executes an algorithm, the algorithm instructs the computer system to perform operations that automate DevOps and SRE processes.

The next section covers some of the learning techniques used by modern algorithms that drive AI innovation.

Considering Algorithm Learning Techniques

A hallmark of modern algorithms is the ability to quickly examine massive quantities of data and learn stuff from the numbers. Much of this occurs automatically without much or even any intervention by humans. Algorithms may use one or more of the following typical AI learning techniques.

Machine learning

ML is the science of getting computers to perform tasks without requiring explicit programming. In the early days of AI, it relied on prescriptive expert systems to work out what actions to take, an "if this happens, then do that" approach. New approaches to ML are moving beyond the limitations of rules. Rules-based IT management systems are on their way out, being kicked out with a swift boot, thanks to ML.

Unsupervised machine learning

Algorithms using unsupervised ML are generally simpler. They aim to find patterns within a set of given data. Being unsupervised, the training is typically longer in duration, and results may not provide the granularity required by a specific use case.

Supervised machine learning

Supervised ML allows algorithms to learn by example. The idea is to provide the system with specific examples of what's "bad" and what's "good" — this issue caused the app to crash the network, and this issue did not crash the network, for example. Training by example enables targeted insight by the system and yields more accuracy required for a use case. Supervised ML is transforming many domains such as AIOps, natural language processing, autonomous vehicles, optical character recognition, medical imaging, and more.

Reinforced learning

AI is all about automation. Humans play an important role in making algorithms smarter. Reinforced learning is a fancy way to describe feedback by users. In AIOps, for example, a system should include provision for accepting comments by DevOps and SRE teams as they resolve issues. Unlike kids who rarely hear helpful advice from parents, the AIOps system always hears every helpful hint you make — and remembers it forever!

HOW AI ALGORITHMS HELP AIOPS

Under the hood, AI algorithms allow AIOps to aggregate data, discover information, detect anomalies, enable automated workflows, and accelerate diagnostics for DevOps and SRE teams.

When applied to a domain like AIOps, a set of different specialized algorithms is narrowly focused on specific tasks. Different algorithms can

- Pick out significant alerts from a noisy event stream.
- Identify correlations between alerts from different sources.
- Assemble the correct team of human specialists to resolve an incident.
- Propose probable root causes and possible solutions.
- Learn from feedback in order to improve continuously over time.

Clustering and correlation is the most complex and crucial step for AIOps, requiring multiple different approaches. A combination of historical pattern matching and real-time identification helps IT ops teams to identify both recurring and net-new issues. Raw monitoring events may be enriched by reference to an external data source, where available. This enrichment helps to deliver better correlation, as well as service impact information.

Seeing How Neural Networks Mimic the Brain

As a branch of supervised ML, neural networks are software systems that try to mimic (often crudely) the way a human brain works. It's an old concept that recently got legs thanks to the advent of big data and the ubiquity of compute and network resources. Here's how it works:

- **Human-like structure:** A neural network is made up of artificial neurons, with each neuron connected to other neurons.
- **Automated configuration:** As different training examples are presented to the network along with their respective outputs, the network works out which neurons it needs to activate in order to achieve the desired output.
- **Automated operation:** With automated configuration, the system enables a structure to automatically make decisions on how to handle any type of data and process it through the system.

Using Deep Learning for New Advances

Deep learning is a very specific and phenomenally exciting field within neural networks. Data scientists are especially keen on deep learning as a way to enable ML — much like ML enables AI. Human readers: Your job is to recall the acronyms!

Think of a deep network as a larger and more complex network enabling interactions between the individual nodes or neurons. Deep learning employs multiple "layers" with complex, sophisticated interactions within each layer and between layers. The essential task of deep learning is to identify patterns and solve problems automatically.

REMEMBER

Deep learning is at the leading edge of ML research, and some of the advances in it have resulted in technologies such as automatic language translation, automatic caption generation for images, automatic text generation, and even creating plays in the style of Shakespeare. If deep learning can write like Shakespeare, it surely can handle AIOps issues for DevOps and SRE teams! “To be a fault, or not to be. That is the question!”

Moving Beyond Rules with AI

WARNING

This brief warm-up on AIOps under the hood is about how AI algorithms are able to automatically process massive amounts of data from your IT environment. DevOps and SRE teams, take note: Only AI can do this! Legacy systems that rely on rules for managing IT can’t handle operational issues of modern systems that daily pump out millions and billions of metrics, traces, logs, and changes.

Here are four reasons why AI algorithms are better for you:

- **Brittle rules frustrate DevOps and SRE teams.** Rules are easy to create, but you can never create enough to address every situational option. They bring the illusion of simplicity but have exponential complexity and do not address unpredictable events.
- **Rules are expensive.** Constant maintenance of rules costs big money and time. In return, rules have hidden complexity and can hinder detection and remediation.
- **Rules have tiny scope.** They only work in simple environments and are unpredictable with complexity — especially in large IT environments. Rules are unable to scale for modern systems.
- **Rules are undecidable.** Rules cannot guarantee to find root causes of failure. Random failures are confusing to rules and confound remediation.

REMEMBER

By using an approach with AI algorithms, DevOps and SRE teams finally get automated observability and control of service continuity and performance.

IN THIS CHAPTER

- » **Mapping the AIOps workflow graphically**
- » **Improving data analysis**
- » **Reducing noise and detecting anomalies**
- » **Identifying data patterns across systems**
- » **Identifying root causes of issues**
- » **Resolving issues**

Chapter 3 Understanding the AIOps Workflow

Most of the steps of the artificial intelligence for IT operations (AIOps) workflow are performed automatically by the AIOps solution. The functions are completed for you so that DevOps and site reliability engineering (SRE) teams can focus on fixing the things that matter most and then take the rest of the week off to hang out and relax — er, refocus freed-up time on higher-value tasks.

Visualizing the AIOps Workflow

As the AIOps workflow progresses, AIOps-specific algorithms and applications work to ensure effective continuous service assurance. Figure 3-1 illustrates the steps of the AIOps workflow.

The remaining sections of this chapter describe each step of the AIOps workflow in detail.

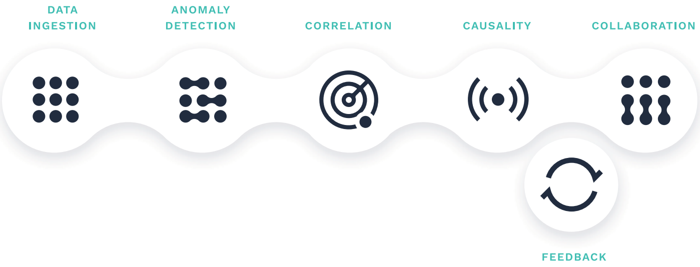


FIGURE 3-1: The AIOps workflow.

Ingesting and Normalizing Data

The first step in the AIOps workflow is ingesting and normalizing the source data generated by your infrastructure, applications, and monitoring tools, including log events, metrics, traces, changes, and alerts. Simultaneously, AI and machine learning (ML) are applied in real time to learn the normal operating behaviors of your services.

REMEMBER

A major advantage of AIOps is the ability to ingest different types of data across siloed technology stacks and use algorithms to filter and organize the data. The goal is to reduce event noise and minimize incident volumes.

DevOps and SRE teams gain complete observability across the production environment with the aggregation of event data, log files, streaming metrics, traces, and changes across cloud and on-premises applications, services, and infrastructure.

Context with data enrichment

A robust AIOps solution integrates with critical information systems such as configuration management database systems (CMDBs), asset management databases, and discovery systems. These multidomain data sources add key information such as location, department, business criticality, service relationships, and owner. By providing this context within the alerts, the solution provides situational awareness, helping DevOps and SRE teams understand interdependencies and relationships so that they may resolve incidents quickly.

The AIOps solution also uses the data to "enrich itself" without using external intelligence feeds. Examples include parsing the data for keywords or pieces of information to populate other fields, or combining values in fields to equate to a value in another field. This is the power of using algorithms to make your team smarter!

TECHNICAL STUFF

Cross-domain data enrichment optimizes several processes:

- **Operational:** Functionally modifies behavior within AIOps to drive processes such as clustering, ideally performed upon alert creation.
- **Diagnostic:** Assists operators to investigate incidents and can be performed at either the alert level or the incident level. Examples include updates to custom information and incident discussion threads.
- **Informational:** Assists DevOps and SRE teams with informational updates to the incident description, services, and processes for ease of use and situational awareness.

Benefits of AI data analysis

AI data analysis provides the following benefits:

- 360-degree visibility across technology stacks is provided from a central system of engagement.
- Event noise is reduced by up to 99 percent.
- Data is enriched for context and situational awareness.

Reducing Noise and Detecting Anomalies

In a modern IT environment, the velocity and volume of operational data makes finding an anomaly that matters akin to finding the proverbial needle in a haystack. The solution? Make the haystack smaller, and the search for anomalies becomes easier.

In an IT environment, the "haystack" is the large volume of data. This haystack of data is the *noise.* The object you seek is the needle, or *signal.* Visibility of the signal depends on reduction of noise. Aha! A math problem! The task is now more approachable.

Reduction by deduplication

For many years, the concept of noise reduction began and ended with deduplication. Every time a repeat event was encountered, the system incremented a counter on the parent alert and discarded the repeated event. In this way, hundreds of ping-fail alerts, for example, collapsed into a single alert. Simple and effective, but insufficient for managing modern systems.

Enhancing deduplication with entropy

Entropy is an algorithmically determined numerical value that rates the importance of an event within the context of the rest of the system. The higher an alert's entropy, the greater its importance; importance declines as entropy moves lower. High-entropy events are the needles, the things to examine first. Low-entropy events can be safely ignored; these events are the noise that creates a giant haystack of grief.

REMEMBER

Even a basic entropy threshold means large proportions of the inbound events can be ignored, because they don't contain useful information. For purposes of remediation, you may safely ignore anything without high entropy.

In practical terms, if your team has deduplication only for noise reduction, you'll still see thousands of alerts every day. Experience and other information held inherently within your organization can help identify alerts of no consequence that can be ignored — such as the process heartbeat messages, the polled and unthresholded utilization messages, and the temporary connectivity failures. None of these alerts needs remedial action; they contain little useful information and have low entropy.

But can these low-entropy alerts be distinguished from important, actionable events? For example, the failure of a disk array on your database cluster requires action.

The underlying concept of an alert entropy is a simple and incredibly powerful model for noise reduction. Alert entropy is far more powerful and sophisticated than the legacy process of deduplication, and far more relevant to modern IT operations (see Figure 3-2).

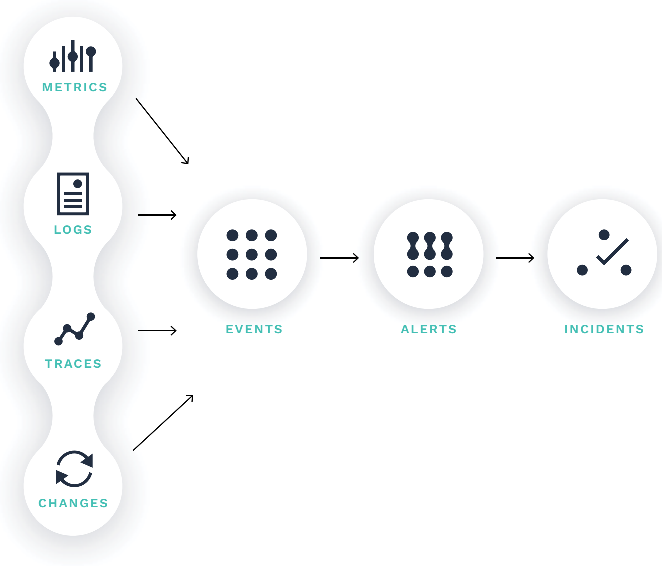


FIGURE 3-2: Discovering all the important events in your observability data is essential for actionable alerts and contextual correlation.

Benefits of reducing noise with entropy

TIP

Using entropy to reduce noise provides the following benefits:

- The haystack is quickly reduced so that isolating alerts that matter is easier.
- Geometrically improved accuracy of detection is produced.
- DevOps and SRE teams can focus on alerts relevant to solving real issues.

Correlating Alerts

In the quest for meaningful observability, you'll find correlation to be one of the most important elements for AIOps. *Correlation* makes connections between data from multiple data sources from different parts of the IT ecosphere. *Alert correlation* allows you to see patterns across the systems that make up technology stacks to ensure applications and microservices are at peak performance. An AIOps solution's correlation algorithms analyze alerts to identify clusters of similarity across service-affecting incidents, problems, or changes.

REMEMBER

The result of correlation and aggregation is a massive reduction in the number of alerts or notifications bombarding IT operations, network operations centers, and DevOps teams. Correlation can reduce the number of tickets received by DevOps and SRE teams by two-thirds or more, and it simultaneously teaches the algorithms to improve accuracy in guiding faster remediation, especially for recurring incidents.

Fine-tuning alert correlation

An AIOps solution with visualization capability helps DevOps and SRE teams identify similarities of alerts within an incident, as shown in Figure 3-3. Using the tool's rich view into the AIOps algorithms, teams can adjust and train algorithms to focus on the data sets that deliver the most insight for resolving incidents.

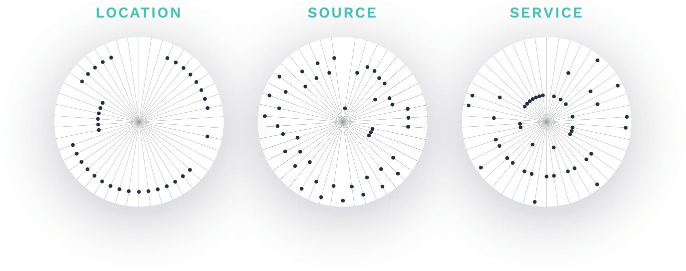


FIGURE 3-3: An AIOps solution should provide transparency into the ML algorithms and patterns used for correlation (such as location, source, and service).

TECHNICAL STUFF

An AIOps solution uses several ML algorithms to cluster alerts into incidents. The clusters are made more precise through definitions that contain identifying characteristics such as the following:

- Event arrival times
- Network topological proximity
- Contextual similarity

These algorithms cluster alerts based on underlying metadata and with enrichment information that adds to the contextual relevance, presents operations teams with situational awareness, and recommends probable root cause.

Benefits of correlation

REMEMBER

The benefits of correlations include the following:

- Shared context enables faster incident, problem, and change management.
- Typically, DevOps and SRE teams deal with 99 percent fewer incidents.
- Faster mean time to detect (MTTD) occurs.
- Faster mean time to resolve (MTTR) occurs.

Discovering Causality: The Root Causes of Issues

Causality algorithms identify changes in critical nodes in physical or logical topologies to assess and understand the impacts of alerts. They also help DevOps and SRE teams to understand which events have the highest probability to be the root cause, guiding teams to the best starting point for troubleshooting and remediation.

How causality identifies root causes of issues

TECHNICAL STUFF

Providers of AIOps solutions may have different approaches to causality. For example, Moogsoft probable root cause functionality uses supervised ML techniques in a neural network to look at the workflow of operators and learn from the feedback they provide to the system. The ML approach of classification allows the Moogsoft AIOps Platform to categorize an object by its metadata or attributes. The neural network uses alert attributes in combination with operator feedback to analyze real-time data sets and predict which alerts are the most causal.

Where to look to fix an incident

TIP

Algorithms for probable root cause identify the alerts and changes most likely to have caused the incident. If DevOps or SRE teams currently follow a process of elimination, or a mean time to innocence (MTTI) model, they'll find the algorithmic approach to be a major leap in technology. Through supervised and unsupervised ML, probable root cause quickly analyzes the patterns, previous incidents and timeline, proximity and linguistic aspects of alerts, and changes to present the most likely causes. Of particular value is the ability for probable root cause to identify changing conditions in service delivery *before* customers feel pain. This is how AIOps provides focus for teams to triage a few alerts versus hundreds, saving time and resources across the organization.

REMEMBER

Probable root cause can speed the time to resolution with an AIOps solution that automates algorithmically delivered workflows. Automation is invaluable, especially for triaging complex incidents.

Benefits of root cause analysis

REMEMBER

The AIOps algorithmic approach to root cause analysis provides the following benefits:

- DevOps and SRE teams can determine where to begin troubleshooting and diagnosis immediately upon opening an incident by looking at the probable root cause alerts and changes.
- Teams can resolve incidents quickly by examining probable root cause alerts and changes.
- Teams can focus time and resources on fixing the most likely root cause for a more efficient operating model.

Collaborating to Resolve Issues

Collaboration is the process of teams working together to quickly triage and remediate incidents. AIOps algorithms should be able to compare current and past incidents. By assigning each incident a similarity percentage, DevOps and SRE teams can view and apply captured knowledge and resolution steps to solve IT problems more quickly. Teams can also identify recurring problems, as algorithms provide the insight needed to prevent damaging effects to business services before they occur. Goodbye, exceeded error budgets!

Collaboration capabilities

Collaboration across teams is the fastest way to resolve complex multiservice incidents. When a high-priority incident occurs, subject matter experts (SMEs) from multiple teams must collaborate to find solutions. AIOps solutions for large enterprises should include an integrated *Situation Room* (a virtual room for SMEs and other stakeholders to collaborate and quickly resolve incidents).

TIP

An AIOps solution for small to medium-size enterprises may also enable collaboration via prebuilt integrations and generic mechanisms for posting incidents to and collaborating in the third-party products. Think ChatOps, PagerDuty, Slack, and other notification and escalation tools. Moogsoft's solution for small to medium-size enterprises, called Express, provides more than 100 prebuilt integrations (see Chapter 5). Moogsoft Express can also act as a plug-in to its companion large-enterprise solution, Moogsoft Enterprise.

Insight with visualization

A solution's algorithm-created topological data shows a dynamic visual representation of connections between resources affected by an incident. This capability is enabled when an incident affects more than one node and AIOps has topological data for those nodes. Zoom in and out, select one of multiple topologies, or click and drag the nodes to rearrange the view. Red signifies a "critical" incident requiring immediate investigation.

TIP

Likewise, an AIOps timeline provides faster MTTR. No more chasing alerts in silos! A timeline offers a powerful graphical view showing the progression of an incident. Operators see a breakdown of the incident's associated alerts in the order they occurred alongside key activity markers. This helps identify probable root cause by showing how an incident developed and indicates the hot spots where there are higher volumes of more severe alerts.

Benefits of collaboration

REMEMBER

Collaboration with AIOps offers the following benefits:

- It eliminates the frequent “all-hands-on-deck” clumsy meeting room gatherings and conference calls.
- Agility comes from automating your workflow and integrating with tools and systems that your organization has invested in for many years, such as incident management or runbook automation tools.
- Workflows are transformed for every operator who is responsible for elements of an incident. They immediately have all the information they need to do their job, available with a few clicks of a mouse.

Naturally, a recurring final step to AIOps workflow entails the “post-mortem,” in which DevOps and SRE teams review the causes and events of incidents to better understand and implement a permanent fix and prevent similar problems in the future.

IN THIS CHAPTER

- » Understanding the role of AIOps in digital transformation
- » Improving collaboration and productivity across teams
- » Managing service incidents more effectively
- » Ensuring optimal IT service assurance
- » Reducing costs to bolster cash flow

Chapter 4 Use Cases for DevOps and Site Reliability Engineering

With the flexibility of artificial intelligence (AI), artificial intelligence for IT operations (AIOps) can fulfill a broad range of IT use cases, with new use cases being discovered at a fast pace. This chapter covers five typical DevOps and site reliability engineering (SRE) use cases. It also shares stories from companies that are using AIOps for very successful outcomes.

Managing Digital Transformation

Each DevOps and SRE professional is personally involved in the digital transformation sweeping through businesses, governments, and other organizations around the world. Digital transformation takes many forms as entities strengthen their online presence, enable frictionless digital transactions, implement autonomous communications, and deploy many more initiatives changing the way they operate.

CASE STUDY: SAP SUCCESSFACTORS

SAP SuccessFactors is one of the world's largest providers of cloud human capital management (HCM) software.

Problems:

- Cloud transformation triggered exponential growth in transactions — 100,000 alerts per day were being manually analyzed and correlated.
- End users identified 80 percent of incidents; internal silos constantly produced duplicated efforts by ops teams.

Moogsoft Solution:

AIOps event correlation across multiple domains, bidirectional integration with ServiceNow, and increased collaboration across teams.

Integrations:

Dynatrace, Splunk, SolarWinds, Pingdom, Zabbit, Jira, Azure, and ServiceNow.

Results:

Improved customer satisfaction; 99.6 percent reduction in event noise; 40 percent reduction in mean time to detect (MTTD); and automated correlation.

Jim Reed, Chief Technology Officer of SAP SuccessFactors says, "We matured the operational staff from just looking at incidents and flashing lights to looking at situations and coming out of that and saying here is what happened, here's how we fixed and here's what we know going forward to make sure it doesn't happen again."

For details, see `www.moogsoft.com/case-study/sap-successfactors`.

With transformation comes a deluge of data from ever-changing IT environments. For this use case, AIOps helps teams make effective use of the data. No longer must teams suffer from alert fatigue and confusion when determining what broke and how to fix it. AIOps uses data to concisely inform teams on how to ensure the uptime and availability of the company's online presence and digital footprint.

REMEMBER

Digital transformations often entail major shifts in technology, such as migrating from legacy mainframe and distributed systems to container-based and service-oriented architectures, or moving from on-premises to virtualized public and private cloud architectures. All these transformations generate massive amounts of data and bring huge complexity for IT — the perfect use case for AIOps!

Enhancing Collaboration and Productivity

Simplifying and automating workflows to enhance collaboration and productivity are an important AIOps use case. With AIOps, alert fatigue and siloed efforts that thwart collaboration are things of the past. Teams are more productive when guided toward the root causes of issues. AIOps shows teams incidents while the incidents are forming but before they trigger an outage. AIOps provides proactive insights that enable teams to prevent incidents from occurring at all!

AIOps workflows for DevOps and SRE teams eliminate the need to manually swivel between multiple dashboards or communications channels. The collaboration tools built into an AIOps solution or integrated via third-party apps place the insights that DevOps and SRE teams need at their fingertips.

REMEMBER

The key collaboration and productivity benefits of AIOps include

- An end to alert fatigue
- Increased system visibility — an end to data silos
- Automated routine tasks
- Faster decision making
- Improved team collaboration
- Support for the constant change of continuous integration/continuous delivery (CI/CD)

Streamlining IT Incident Management

As a meat-and-potatoes activity for DevOps and SRE teams, incident management can consume many hours of a workday. For some, this can also mean worknights and work weekends. AIOps provides a better way to manage service incidents by automating tasks to ensure the following:

- Faster issue detection
- Probable root cause identification
- Faster MTTR
- Reduced escalations
- Improved incident workflows

CASE STUDY: FANNIE MAE

Fannie Mae is a U.S. government-sponsored enterprise that makes home mortgages available to low- and moderate-income borrowers.

Problems:

- Siloed incident management and alert processing resulted in operational inefficiencies, poor customer experience, and high cost.
- Five million alerts per month across a complex environment led to alert fatigue and visibility gaps.

Moogsoft Solution:

Tool rationalization, AI/ML anomaly correlation with historical analysis, identification of recurring issues, automated actions, and IT service management (ITSM) integration.

Integrations:

ServiceNow, Dynatrace, ExtraHop, xMatters, and IBM NetCool (migration).

Results:

Improved customer satisfaction, cut incidents by a third, reduced MTTR by 25 percent to 75 percent, and improved teamwork.

According to Jay Rudrachar, Director of Enterprise Monitoring, Analytics and Reporting, at Fannie Mae, "What our operations team is seeing is, they have additional bandwidth to focus on real problems, and also spend more time on identifying the underlying root cause to permanently fix the problem."

For details, see `www.moogsoft.com/blog/aiops/fannie-mae-aiops-best-practices`.

Automating IT Service Assurance Workflows

Service assurance is a catchall term with origins in the telecommunications business. In that domain, service assurance means applying policies and processes to enable services offered over networks for an optimal subscriber experience. When a customer subscribes, the contract stipulates the provider will ensure predefined levels of service quality (hence, the term *service level agreement* [SLA]).

Over time, other IT domains have adopted this term. Modern subthemes for IT service assurance may include the following:

- Observability
- Monitoring
- Alarm and event management
- Incident management
- Problem management
- Change management

REMEMBER

AIOps happens to sit at the center of these subthemes. Alert readers will immediately grasp the primary use case for IT service assurance: automation! By automating IT service assurance workflows, your organization may accomplish the following:

- Mitigate the impacts of system outages and downtime.
- Meet customer SLAs.
- Reduce ticket and notification volume.
- Fix poor reliability and availability of critical applications and services.

Reducing Costs

Cost reduction is an eternal theme in business and a frequent motivation to try new technology for pudgy use cases that need to go on a financial diet. The savings may result from operational efficiencies spawned by automation. When automation so permits, AIOps may enable reallocation of staff. It may also lead to rationalizing and consolidating tools that are no longer required for service assurance.

Also consider the promise of AIOps substantially reducing the risk of service outages. Reduction of risk means preservation of cash flow. Nothing gets The Management more excited than cash flow (or more upset than when cash flow dribbles to a halt). DevOps and SRE teams are typically blamed for these outages.

REMEMBER

High points to remember for the cost reduction use case include the following:

- Reduced staff overhead
- Stemmed losses from outages and downtime
- Controlled cost of incident, problem, and change management

IN THIS CHAPTER

- » **Integrating all types of data**
- » **Seeing everything in one place with a unified view**
- » **Keeping teams in sync with synchronized dataflows**
- » **Enriching data to create automated workflows**
- » **Recognizing the benefits of integration**

Chapter 5
AIOps as a Hub of Integration

Artificial intelligence for IT operations (AIOps) solutions seamlessly integrate data from all IT sources, including the systems your organization has invested in over the years. AIOps uses algorithms to reduce noise and reveal the most relevant information required by DevOps and site reliability engineering (SRE) teams to speed incident response times. Using deep contextual insights, AIOps substantially reduces the number of incidents DevOps and SRE teams deal with, which facilitates rapid remediation of issues and diminishes or eliminates system downtime.

This chapter covers four ways that integrations are turning AIOps into the modern hub for service assurance.

Integrating Data Streams

An effective AIOps solution automatically applies intelligence to all data streams to help DevOps and SRE teams proactively identify and resolve incidents before they affect business services.

Effective AIOps solutions receive, analyze, and manage monitoring and observability data from any system or device using standard integrations. They also may use simple application programming interfaces (APIs) for do-it-yourself (DIY) integrations and workflows.

REMEMBER

Integration capabilities for an effective AIOps solution should include

- **Ingestion of data at scale:** Integrations should easily connect all your monitoring and observability data, tools, and systems for scalable ingestion of data streams of any size.
- **Noise reduction:** AIOps should leverage ingested data to understand the significance and relevance to effectively reduce noise and surface only actionable alerts.
- **Intelligent correlation:** The solution should use AIOps algorithms to discover patterns and relationships in your data, effectively correlating results.
- **Root cause identification:** Finding and fixing the problem faster is what AIOps is about, and integrations are a crucial pillar for determining root cause.

Having a Unified View

Effective AIOps solutions provide a unified view for monitoring, observability, and change data. With the complete visibility and context provided by a unified view, AIOps can best help you efficiently investigate issues, reduce downtime, and ensure your business services remain continuously available.

TIP

Because AIOps lets you view everything in one place, you can finally get control of the much-dreaded trouble tickets. Everyone will agree that "death to tickets" is a welcome result of AIOps!

Synchronizing Integrated Data Flows

Integrations must include existing workflow processes, as shown in Figure 5-1. Because alerts are pre-correlated with context and better insight, AIOps can determine which alerts matter for an incident, and team members get fewer alerts. Bidirectional integration of data sources ensures better-quality information and keeps DevOps and SRE team members in sync.

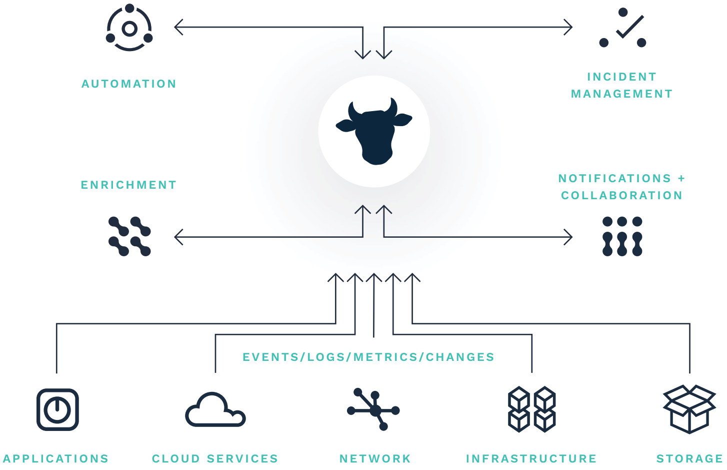


FIGURE 5-1: Integrating data sources with existing workflow processes.

Synchronization of integrated data flows also helps engage teams faster for informed collaboration with peers and other subject matter experts. This includes integration of DevOps and SRE team feedback from previous incidents that are related to new incidents.

REMEMBER

With synchronization, AIOps ensures that quality information is automatically delivered to the right people, enabling faster remediation and continuous service assurance.

PREBUILT INTEGRATIONS TO LEVERAGE TOOLS YOU ALREADY USE

Prebuilt integrations let you snap in tools that are already tested and trusted by DevOps and SRE teams. Following are examples from more than 100 prebuilt integrations included with the Moogsoft AIOps Platform. Integrations provide built-in intelligence to automatically collect and algorithmically analyze metrics directly at the source.

Monitoring and Observability

- Amazon Web Services (AWS)
- Apache Kafka
- Catchpoint
- Cisco AppDynamics
- Datadog
- Dynatrace
- ExtraHop
- Fluentd
- Google Cloud Platform
- Grafana
- Kubernetes
- Microsoft Azure
- MongoDB
- Nagios
- New Relic
- Prometheus
- Sensu
- SolarWinds
- Splunk
- Sumo Logic
- VMware
- Zabbix
- Zenoss

Notification and Collaboration

- Atlassian Opsgenie
- Microsoft Teams
- PagerDuty
- Slack
- xMatters

Automation

- Ansible
- Chef
- eyeShare
- Jenkins
- Puppet
- Resolve Systems

Ticketing

- Atlassian Jira
- BMC Remedy
- Cherwell
- ServiceNow

Automating Workflows by Enriching Data

TIP

AIOps algorithms fulfill enrichment by analyzing internal operational data, as well as data integrated from third-party tools. A robust solution easily draws requisite data from your existing configuration, topology, and system of information repositories. These data are a baseline for enriching operational information inputs with your organization's key data assets and aiding DevOps and SRE teams in effective decision making.

CASE STUDY: GODADDY

GoDaddy, the world's largest domain name registrar, has invested in the latest agile data center technologies, including the adoption of AWS as its primary infrastructure platform. It needed a next-gen event management solution.

Challenges:

- Lack of data integrations prevented monitoring new technology stacks.
- Customers detected issues before SRE teams did.
- Legacy systems wouldn't scale with rapid growth.
- AWS operations added silos of support.

Solutions and Results:

- GoDaddy implemented Moogsoft AIOps.
- Teams stayed agile throughout the migration.
- The solution provided team and resource stability while scaling events.
- Customer help desk calls fell 66 percent; workloads were cut by 99 percent.

For more information, see `www.moogsoft.com/resources/aiops/case-study/godaddy-migrates-aws`.

DevOps and SRE teams learn to trust automation when it provides the probable root cause context and intelligence required to trigger correct automation workflows. Providing DevOps and SRE teams with authoritative visual information, such as asset topology maps and incident timelines, helps them know where to begin triage and remediation.

AIOps removes the complexity of determining where and how to begin fixing issues. DevOps and SRE teams can proactively ensure continuous service assurance for the on-demand customer experience that consumers have come to expect.

DIY BY BUILDING YOUR OWN INTEGRATIONS

Being self-reliant is handy, so look for an AIOps solution that allows you to easily build your own custom integrations — just in case a tool your team loves is so old or obscure that there's no prebuilt connector. Moogsoft includes the following capabilities to make DIY integration fast and easy:

- **API:** Call, retrieve data, update data, and call actions in Moogsoft AIOps.
- **Stats API:** Retrieve statistics from Moogsoft AIOps for reporting and dashboards.
- **Bot:** Create bots to perform automated tasks and expose functions.
- **Custom polling:** Accept API calls and parse the responses into Moogsoft AIOps events.
- **Webhook:** Send events from a webhook client to Moogsoft AIOps.

CASE STUDY: FISERV

Fiserv is a global provider of financial services technology to banks, credit unions, securities broker dealers, leasing and finance companies, and retailers.

Problems:

An alert volume of 3 million per year hampered MTTR, so much so that customers grew dissatisfied with service quality.

Moogsoft Solution:

AIOps event correlation across multiple domains (application performance, synthetics, logs, and network monitoring) and a knowledge base for similar corrective actions (probable root cause and next steps).

Integrations:

IBM NetCool (migration), AppDynamics, CA Spectrum, BMC Remedy, Splunk, Amazon Web Services (AWS), and Mir3.

Results:

Customer satisfaction improvement, 75 percent reduction in Level 1 and 2 tickets, 85 percent MTTR reduction, and penalty avoidance.

Tony Wages, IT Architect at Fiserv, says, “We had an incredible volume of alerts and we needed a way instead of working individual alerts. We wanted to be able to correlate alerts into a single problem, which in AIOps is a situation. That way our staff would be more efficient. We wanted the correlation and the noise reduction — our two key parameters.”

For more information, watch the video at `https://youtu.be/5TKRrPFZ9S4`.

Getting the Benefits of Integration

REMEMBER

Integration provides the following benefits:

- You can customize your workflows for faster time-to-value by plugging in prebuilt or custom integrations.
- You can engage the right individuals and teams faster, provide better-quality information, and keep everyone in sync through bidirectional integration of automated ticketing, notification, and collaboration systems.
- You can draw from your existing configuration, topology, and system-of-record repositories to enrich alerts and incidents by leveraging AIOps as a hub of integration. This way, your organization's key data assets assist in effective analytics and decision making.

IN THIS CHAPTER

- Knowing why cloud-first organizations choose Moogsoft Express
- Understanding the capabilities of Moogsoft Express
- Gaining instant insights with data analysis and visualization tools

Chapter 6

Using Moogsoft Express for DevOps and Site Reliability Engineering

Moogsoft Express is the observability with AIOps solution for DevOps and SRE teams. It improves the reliability of mission-critical services and applications that digitally transform and power your organization. The solution is designed to help DevOps and SRE teams automate observability and obtain deep insights across your dynamic and ephemeral infrastructure and applications.

Choosing Moogsoft Express

Moogsoft Express is the only offering that democratizes AIOps while including native monitoring and observability capabilities. Simple to deploy and easy to use, Moogsoft Express allows DevOps and SRE teams to keep their continuous integration/continuous delivery (CI/CD) software pipelines humming, detect application performance problems, and honor customer service level agreements (SLAs) and service level objectives (SLOs).

REMEMBER

Here are key highlights that make Moogsoft Express the AIOps and observability solution of choice for cloud-first organizations, and DevOps and SRE teams:

- **Born in the cloud.** It all starts with a cloud-native and application programing interface (API)–first architecture. Thanks to its software-as-a-service (SaaS) deployment and subscription licensing model, organizations don't have to provision hardware — Moogsoft takes care of that. Designed for smaller teams, it's priced accordingly and features all the functionality they need in a package that's easy to adopt.
- **Automates streaming of metrics.** The Moogsoft Express Collector enables real-time collection, analysis, and streaming of metrics with a lightweight agent that runs on any operating system. It discovers time-series metrics data from any source and performs localized anomaly detection. The Collector learns the normal operating behavior of the metrics directly at the data source.
- **Provides comprehensive functionality.** The solution's comprehensive feature set is powered by the same patented AI and machine learning (ML) algorithms of Moogsoft's industry-leading AIOps platform, which is trusted by more than 140 customers. Moogsoft Express has out-of-the-box support for many common DevOps and SRE tools and data sources for optimal insights and quick resolution of issues.

Knowing What Moogsoft Express Can Do

With Moogsoft Express, DevOps and SRE teams can finally gain insight into and streamline the management of their operational data, putting an end to alert overload and lengthy outages. Moogsoft Express provides full visibility over potentially serious incidents and helps teams promptly and proactively address them.

REMEMBER

Moogsoft Express is a complete AIOps solution. Here are some of its best features:

- **Ingests and enriches observability data.** Moogsoft Express automatically ingests logs and metrics to identify anomalies and surface events, along with events, traces, and alerts from monitoring tools and systems.

- **Reduces noise to detect anomalies.** Moogsoft Express automatically applies statistical calculations and noise-reduction algorithms to detect anomalies and surface significant alerts for triage and remediation.
- **Correlates alerts.** Using Moogsoft's robust correlation algorithms, Moogsoft Express automatically correlates alerts into meaningful and actionable incidents.
- **Discovers causality.** Moogsoft Express automatically identifies the probable root cause — the most likely alerts to have caused an incident. It finds the needle in the haystack.
- **Enables collaboration.** Moogsoft Express has prebuilt integrations with popular tools, as well as flexible and simple APIs to build hundreds of integrations.

Visualizing Your Data with Moogsoft Express

Moogsoft Express automatically learns the normal behavior of your metrics and then flags anomalies as they occur. Snapshots of anomalous activity are available within each incident involving metrics. Live interactive graphs are easy to inspect and manipulate within the powerful Moogsoft Express metrics interface.

REMEMBER

Visualization tools provide instant insights, literally showing DevOps and SRE teams where to address remediation of situations for continuous service assurance. Moogsoft Express aggregates metrics and events across your full stack. The solution provides full visibility into your applications in order to monitor, troubleshoot, and optimize their performance across all your systems.

TIP

As a business grows, it can add Moogsoft Express licenses for different teams. For more advanced collaboration and customization features, it can deploy Moogsoft's Enterprise product, knowing both solutions interoperate seamlessly.

TEST-DRIVING AIOPS WITH A FREE TRIAL

You can get full access to Moogsoft Express, the cloud-native observability with AIOps solution for DevOps and SRE teams. Moogsoft Express helps you resolve incidents faster and deliver continuous service assurance for all digital services. Begin your free cloud trial now, and watch Moogsoft Express get to work on your data right away. Go to `https://moogsoft.com/express` to register.

Chapter 7

Ten Tips for Getting Started with AIOps

Congratulations! You're ready to dip your toes into artificial intelligence for IT operations (AIOps) and try a simple proof-of-concept (POC) project. This POC project will show your team how a modern AIOps approach dramatically improves your DevOps and site reliability engineering (SRE) teams' ability to achieve continuous service assurance.

TIP

Here are ten tips you can use to get started with AIOps:

- **Read this book.** Read *Observability with AIOps For Dummies* and share it with your team. Get familiar with its themes — they'll guide you on a successful AIOps journey!
- **Start a free trial of Moogsoft Express.** The Moogsoft Express solution helps you implement these tips for getting started with AIOps. Get a free cloud trial by going to `https://moogsoft.com/express` to register.
- **Pick target apps and services.** Identify one or two applications and services that will be the test bed for your observability with AIOps POC of data gathering, analytics, and monitoring.

- **Identify data sources.** Connect the data sources for the target applications and services. Moogsoft Express can help you with this by automatically discovering and connecting to some of the data sources.
- **Identify enrichment sources.** Get more context and useful information from your data by enriching it with additional third-party sources using Moogsoft Express integrations. Moogsoft Express can also help surface useful information within the data itself.
- **Enable workflows with tools.** Establish connections between Moogsoft Express and your existing third-party tools, such as Slack and Jira, to automate workflows and bidirectional transfer of data and notifications.
- **Observe the initial results.** Moogsoft Express will analyze your data and determine normal operating behaviors. Observe the results and become familiar with how Moogsoft Express presents what's normal versus anomalous operating behavior.
- **Socialize intentions and plans.** While conducting the POC, tell your coworkers and teammates what your intentions and plans are for using Moogsoft Express in live-fire operations. Everyone will quickly recognize that automated capabilities will dramatically make their lives easier!
- **Reassess the results against your plan.** Review the results of how Moogsoft Express helped your team resolve incidents. Make sure the results align with your original goals and expectations. You can refine and tune settings to achieve optimal results at any time.
- **Share your experiences.** Let all stakeholders know the results of the POC. Be sure to associate successful incident resolutions with tangible business benefits that prevented an outage or improved the customer experience. Observability with AIOps will become the trusted anchor for your continuous service assurance.

Appendix
Glossary

The following sections define general AIOps and Moogsoft AIOps–specific terms.

General AIOps Terminology

AI: *See* artificial intelligence (AI).

AIOps: *See* artificial intelligence for IT operations (AIOps).

algorithm: A process and/or rule set used by a computer to solve problems for a specific use case.

artificial intelligence (AI): Use of computer systems to automate and accelerate tasks normally requiring human intelligence.

artificial intelligence for IT operations (AIOps): A modern approach to managing events with real-time artificial intelligence and machine learning techniques using neural networks to detect and resolve anomalies anywhere in an enterprise IT environment. *See also* machine learning (ML).

incident: A negative scenario of impacted service requiring detection and investigation by DevOps and site reliability engineering (SRE) teams. Similar to Moogsoft's term, *situation* (see the next section).

machine learning (ML): A type of AI that can automatically learn and improve in predicting outcomes from computational experience and other data inputs.

ML: *See* machine learning (ML).

neural network: A computer system modeled on the human brain and nervous system to learn from examples without requiring programming of task-specific rules.

Moogsoft AIOps–specific terminology

alert: One or more similar events or instances of new data, detected by a monitoring tool and passed into Moogsoft AIOps.

event: A message from a monitored system indicating a change in state, including log files and status indicators from third-party monitoring tools.

operator: Person with responsibility for operating or monitoring the operations of a computer-based system or digital services.

situation: A group of alerts clustered by factors such as time, language, topology, and similarity; Moogsoft's term for an *incident* (see the preceding section).

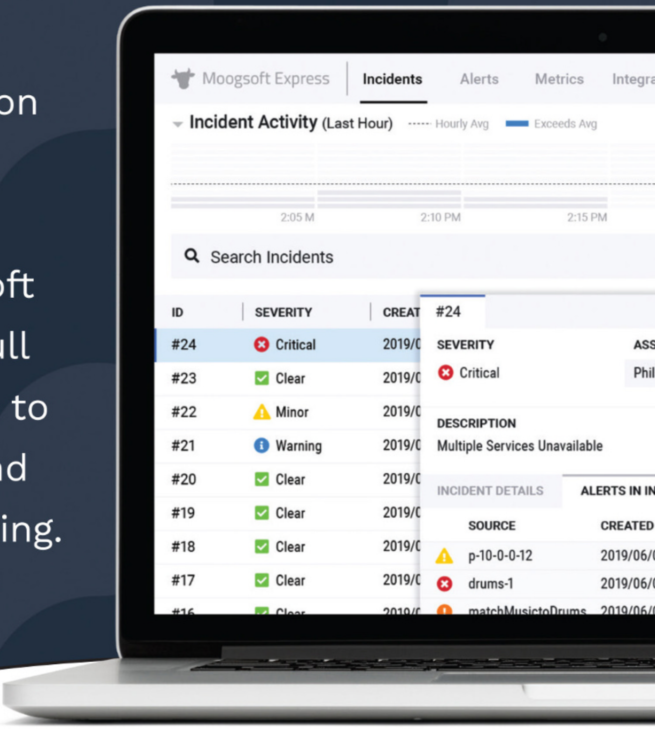
Situation Room: A virtual war room for operators from multiple teams to collaborate while finding resolution to a situation. *See also* operator *and* situation.

team: A list of responsible operators shown by service or applications in one view, such as those pertaining to a line of business. *See also* operator.

moogsoft®

Develop More and Operate Less with Moogsoft Express

The AIOps and observability solution for DevOps and SREs in cloud-first companies, Moogsoft Express provides full event management to keep CI/CD agile and your business growing.


Moogsoft Express | Incidents | Alerts | Metrics | Integra

Incident Activity (Last Hour) ----- Hourly Avg ▬ Exceeds Avg

Search Incidents

ID	SEVERITY	CREAT
#24	Critical	2019/(
#23	Clear	2019/(
#22	Minor	2019/(
#21	Warning	2019/(
#20	Clear	2019/(
#19	Clear	2019/(
#18	Clear	2019/(
#17	Clear	2019/(
#16	Clear	2019/(

#24

SEVERITY: Critical

ASS: Phil

DESCRIPTION
Multiple Services Unavailable

INCIDENT DETAILS | ALERTS IN IN

SOURCE	CREATED
p-10-0-0-12	2019/06/(
drums-1	2019/06/(
matchMusictoDrums	2019/06/(

Learn More at www.moogsoft.com/express

Get total observability with AIOps

In a digital economy that tolerates no downtime, today's DevOps and site reliability engineering (SRE) teams face infrastructure environments that are larger and more complex than ever. These environments will continue to grow in complexity as businesses strive to digitally transform nearly every aspect of their organizations and how they engage with customers. Artificial intelligence for IT operations (AIOps) is the modern way to help teams get continuous observability on modern IT.

Inside...

- Learn how AIOps enables observability
- See how AIOps works under the hood
- Use AIOps workflow for observability
- Explore five use cases for AIOps
- Use AIOps as a hub for modern IT operations
- Get Moogsoft Express for observability
- Find ten tips for getting started with AIOps

moogsoft®

Adam Frank is an AIOps engineering and IT operations aficionado with more than 15 years of hands-on experience in digital transformation. His imagination and passion for creating AIOps solutions are helping DevOps and SRE teams around the world to build continuous service assurance.

Go to Dummies.com™
for videos, step-by-step photos,
how-to articles, or to shop!

ISBN: 978-1-119-73528-1
Not For Resale

9 781119 735281

for dummies®
A Wiley Brand