LogicMonitor

Making Logs Work for You:

3 Considerations for Moving Past Log Management

Today, log analysis is a fundamental step in achieving full observability for IT Operations. In this guide, we will cover the top three considerations when evaluating a log analysis platform and how these platforms streamline troubleshooting for a variety of IT environments.

Table of Contents

Moving Past Log Management

While the world's data supply continues to grow at astounding rates, less than 1% of that data is analyzed[1]. Large data sets can be a wealth of knowledge for IT Operations teams, answering 'why?' an issue occurred, but the information is often left untapped and unanalyzed. IT teams often speculate about the root cause of problems (manually checking changes after an alert has surfaced), but there is little time to figure it out in real-time. Band-aid solutions are applied, like a reboot or a rollback to a prior version, and the root cause is determined later. But to achieve real-time operational intelligence, teams must utilize a platform that surfaces anomalies and analyzes the most relevant signals automatically. To analyze the data is to understand the root cause of performance issues, enabling teams to reduce troubleshooting time and surface anomalies that would otherwise go undetected.

At the center of all of this is the opportunity to analyze log data. Log data contains the signals of what causes a problem in running software or IT Infrastructure. Still, most teams only have tools that manage logs and require manual intervention to analyze and make sense of those signals correctly. If your teams have to search for these signals in an ad-hoc manner, then they are wasting precious time. If you aren't able to sort through all of your logs due to sheer volume, some teams ignore them altogether. If your monitoring tools are not helping you save valuable time in troubleshooting problems, you have the wrong tools.

Nearly every company in existence is dealing with this challenge because it may not have the tools to filter the crucial signals from an abundance of noise. The hidden anomalies in your logs can help explain why incidents occur and can help prevent future disruptions. Issues will happen, but you can control how quickly you respond or recover. You just need to find a way to get your logs working for you intelligently.

1 https://www.theguardian.com/news/datablog/2012/dec/19/big-data-study-digital-universe-global-volume

The Road to Log Intelligence

Every new device that is added, and every new code release that is pushed, contributes to log overload. These form part of what is called "machine data", which is growing 50x faster(2) than traditional business data. In fact, everything in your stack is continuously writing new events to your log files.

The good news is that log data can be hugely valuable for fast-moving organizations because it contains your applications and infrastructure's behavior patterns. However, discerning which data is relevant can often be too big of a challenge for even the most experienced teams. That is why LogicMonitor believes in taking an algorithmic approach to understand log signals through platforms that provide log intelligence.

Log intelligence can be defined as a method of log analysis that is powered by AI and automation to help teams automatically find the root cause of issues and surface anomalies that exist within your log data. This methodology can help your team proactively prevent problems and reduce the Mean Time to Repair (MTTR) for issues that do arise. Put your logs to work with these core considerations to purchase a log analysis tool and ultimately achieve log intelligence.

Three Considerations for Evaluating A Log Analysis Tool

#1. Automate analysis to reduce troubleshooting time

The sheer volume of log data can be too overwhelming. It makes it impossible for IT teams to efficiently use logs to understand, troubleshoot, and track the changes within their environment. From applications and web servers to network devices, everything in the modern IT infrastructure stack generates data and logs continuously. Reviewing data efficiently to troubleshoot and proactively identify potentially catastrophic incidents is crucial for the IT Operations workflow. Manually searching through log data to find answers can unnecessarily extend troubleshooting times. Some tools allow you to create query-based searches for log data on a recurring basis, but this only accounts for infrastructure and applications that you already use. As your infrastructure and applications scale, you need a system that goes beyond query matching and finds the context within new logs that may otherwise go unsurfaced. Finding a log analysis platform that automates log review and surfaces log data that may be relevant for troubleshooting can save your team valuable time and reduce mean time to repair.

#2. Look for a unified platform to avoid context-switching

Finding useful information in your logs is only half the battle. You need the right information at the right time and in the proper context to effectively prevent or resolve an issue. You may typically start from a metric alert indicating that something is wrong and jump to analyzing logs to understand why that issue occurred. That jump often requires context switching, and each time you switch contexts, you risk losing valuable information and precious time. It would be best if you looked for a log analysis platform that minimizes the need to context switch and integrates the different sources of information you rely on, such as metrics and logs, as seamlessly as possible. A unified solution will help put the full picture of infrastructure performance, and it's underlying issues into focus. In addition to helping you troubleshoot faster, such a solution may also enable intelligent correlation between data sets, whereas siloed platforms may prevent such synergies.

#3. Take an algorithmic approach for proactive operations

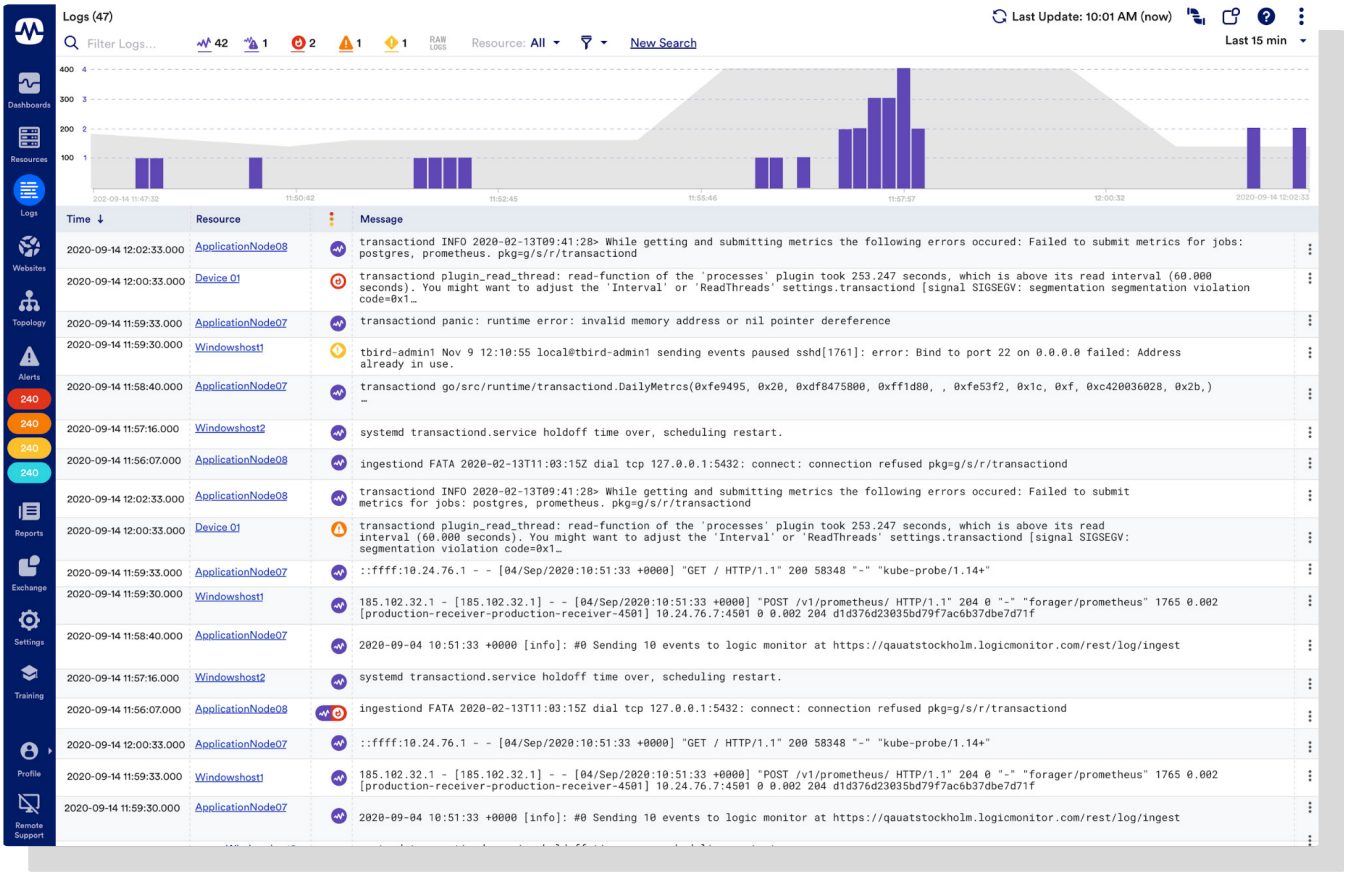
It is essential to understand how any monitoring platform's alerting, and thresholds work. As inefficient as it may sound, many platforms need you to specify the criteria for what constitutes an issue before it will alert for such an event. In most cases, this means that an incident must occur first before thresholds are set, and alert notifications are sent out. As IT infrastructure becomes more complex, the failure landscape is broader. Failure can occur

anywhere from the network, to the cloud, to the applications, to name a few possible failure points. Look for a platform with intelligence that can detect and highlight anomalies in your log data for you, without requiring the overhead of pre-defining static log alert conditions to get any value. Such anomaly detection capabilities will save you time and maximize the chance you will be notified when something needs your attention.

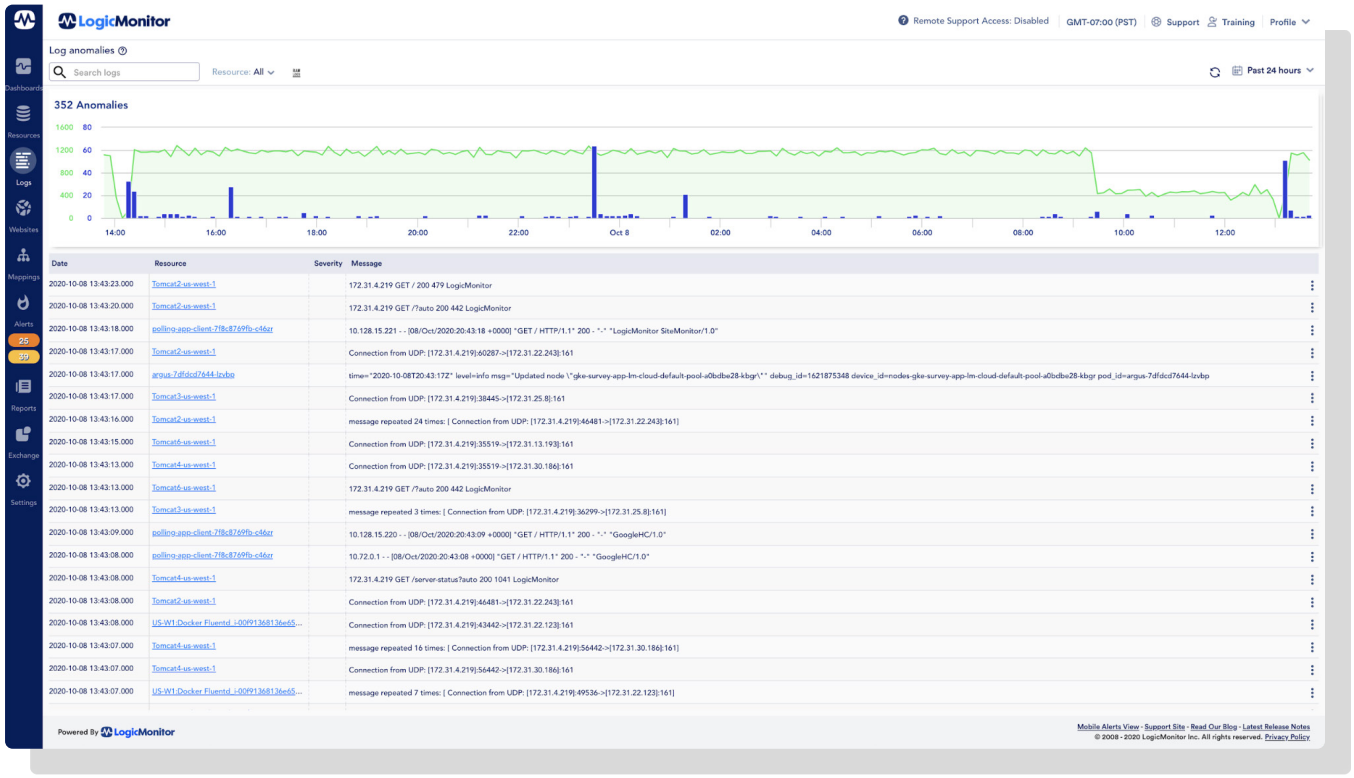
Furthermore, anomaly detection in logs can often catch symptoms or early warnings of issues before the issue occurs. A notification for such a warning allows you to act and prevent the problem from ever occurring in the first place. This algorithmic approach to operations will help your team become proactive rather than reactive.

Putting Your Logs to Work

Based on the considerations listed above, LogicMonitor is proud to show you what the future of log analysis can look like for your organization. LogicMonitor's LM Logs is the essential platform for achieving Log Intelligence, automatically analyzing all of your log data to surface anomalies proactively. This intelligent approach to Log Analysis will help your team go beyond knowing what happened (the issue) to be able to understand why it happened (the root cause).



Built on our AIOps platform, log data is automatically correlated with IT Infrasture metric and topology information. Any anomalies are displayed in the context of alerts to understand why issues occurred. This helps teams troubleshoot quicker, reduce MTTR, and eliminate the need to have multiple monitoring, topology, and log analysis tools. Say goodbye to manual root cause analysis and experience the future of Log Intelligence with LM Logs.



For more information on LM Logs, check out this explainer video or visit our LM Logs Page.

Conclusion

Modern, AI-based log analysis can help you significantly reduce the time spent investigating and troubleshooting incidents. With the many different log analysis platforms available, it can be overwhelming to choose and challenging to know what to look for. In this short guide, we discussed the top three things you should consider when selecting a log analysis platform for your business. Ensuring that you have built-in automation, avoid context switching, and leverage algorithmic intelligence in your log analysis platform will help your team truly become proactive.