OBSERVABILITY WITH LOGS TO ACCELERATE MTTR

Logs play a key role in understanding a system's performance and health and help IT operations (ITOps) teams and site reliability engineers (SREs) identify issues as they emerge and quickly track down the cause of failures. Log analytics involves deriving meaningful insights from log data, which then feeds into observability.

With DevOps and multicloud adoption, logging has become harder than ever. Architecture has evolved into microservices, containers, and orchestration infrastructure deployed on the cloud, across public and private clouds, or in hybrid environments. Not only that, the sheer volume of data generated by these environments is constantly growing, which constitutes a challenge in itself. Long gone are the days when an engineer could simply use a Secure Shell (SSH) to log into a machine and grep a log file. This cannot be done in environments that have hundreds of containers generating TBs of log data a day.

The advanced log management and analytics capabilities of BMC Helix Log Analytics can help by allowing DevOps, ITOps, or SREs to gain the visibility they need and ensure apps are always available and performing optimally, through:

- Log collection
- Log enrichment
- Log analysis
- Alerts and events
- Data visualization

Log collection

BMC Helix Log Analytics data collection uses open-source data collectors to collect logs from different data sources with the intuitive user interface of . It is based on the FluentD collector, which runs in a container and collects logs from docker containers on the host system where the application is deployed, giving flexibility to a system administrator or a DevOps engineer to capture log files so the system can be set up fairly quickly. A user can set up parsing and filtering rules, including custom data patterns for the required information that excludes the data not of interest.

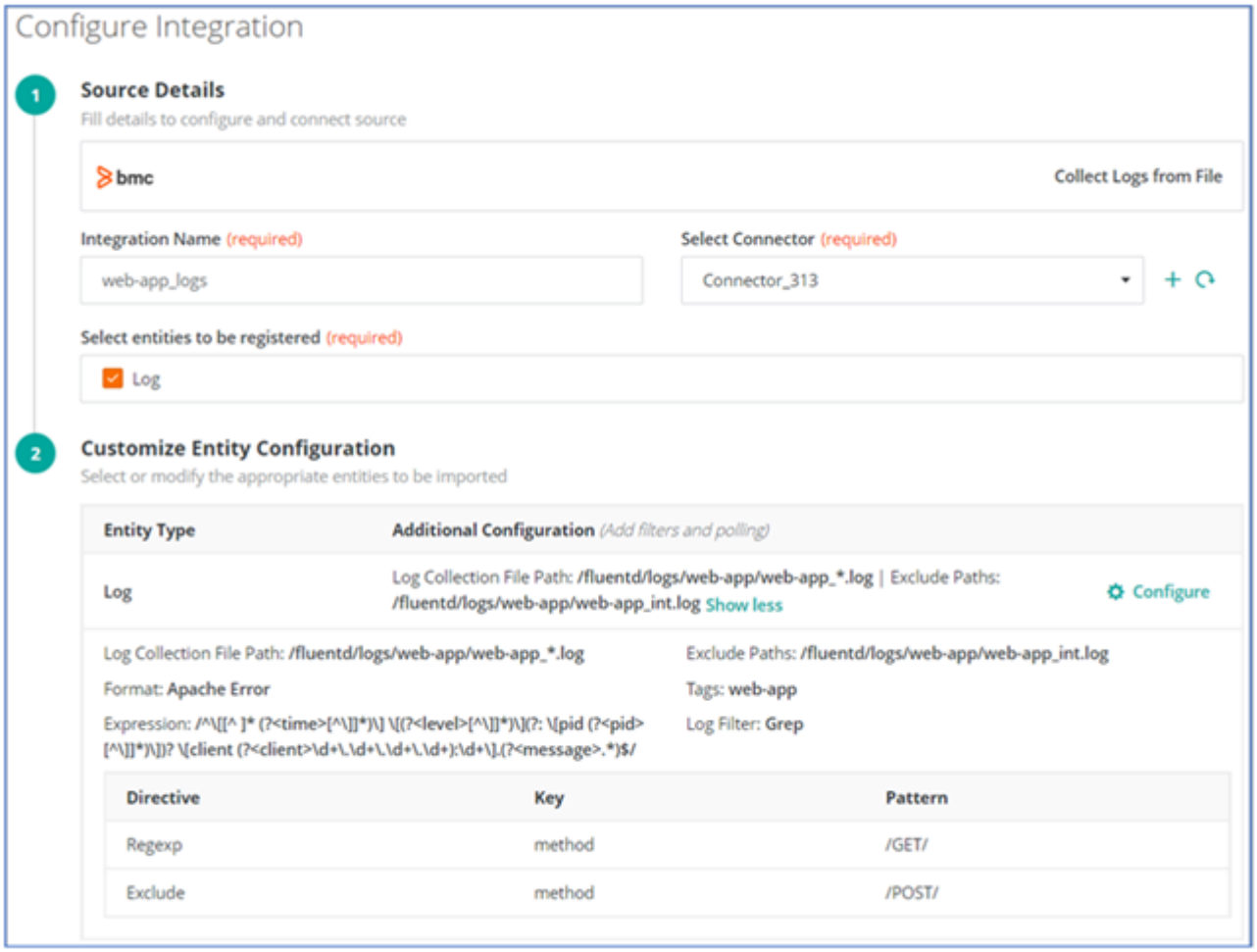

Figure 1. Configuration for collecting log data

Log enrichment

For an ITOps or DevOps engineer troubleshooting issues with logs, problem analysis can be difficult due to the lack of relevant context, which leads to an increase in the mean time to repair (MTTR). For example, if an analyst is attempting to search the logs by a vulnerable host's name, they may not be able to do so if the logs contain only IP addresses but no hostnames. It becomes almost impossible to reconstruct a situation because the volatile, dynamic IP data may change every hour, day, or week, leading to incorrect and misleading summary and detail information.

Log enrichment adds meaningful context to logs for enhanced observability and diagnosis. You can enrich logs by connecting to multiple different enrichment sources like DNS, LDAP, GeoIP, and CSV.

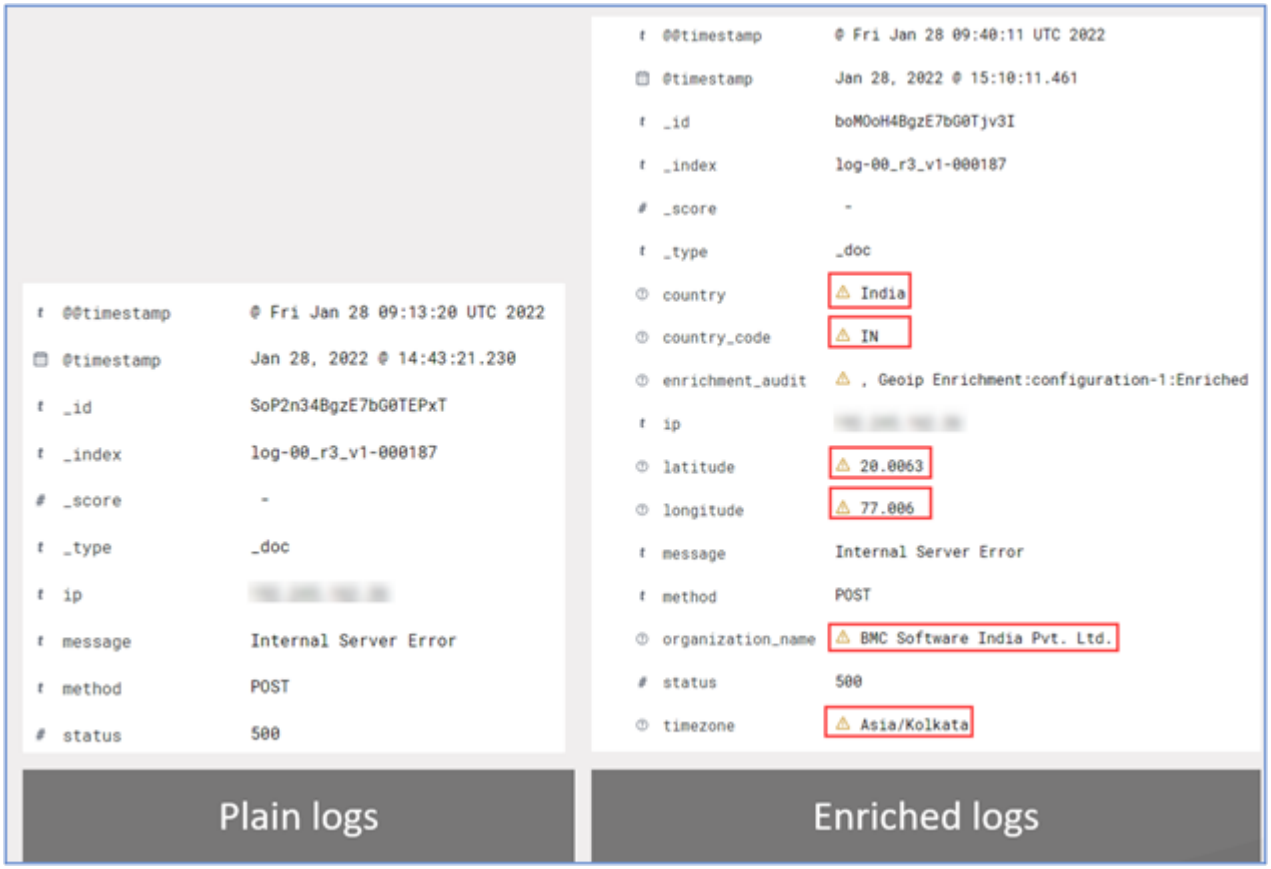

Figure 2. Logs before and after enrichment

Log analysis

The log explorer helps an analyst discover and gain quick insights into their data. The explorer can search and filter the data, get information about the structure of the fields, or query the data for a given time. It can also create a visualization or save the searches and present the findings in a dashboard.

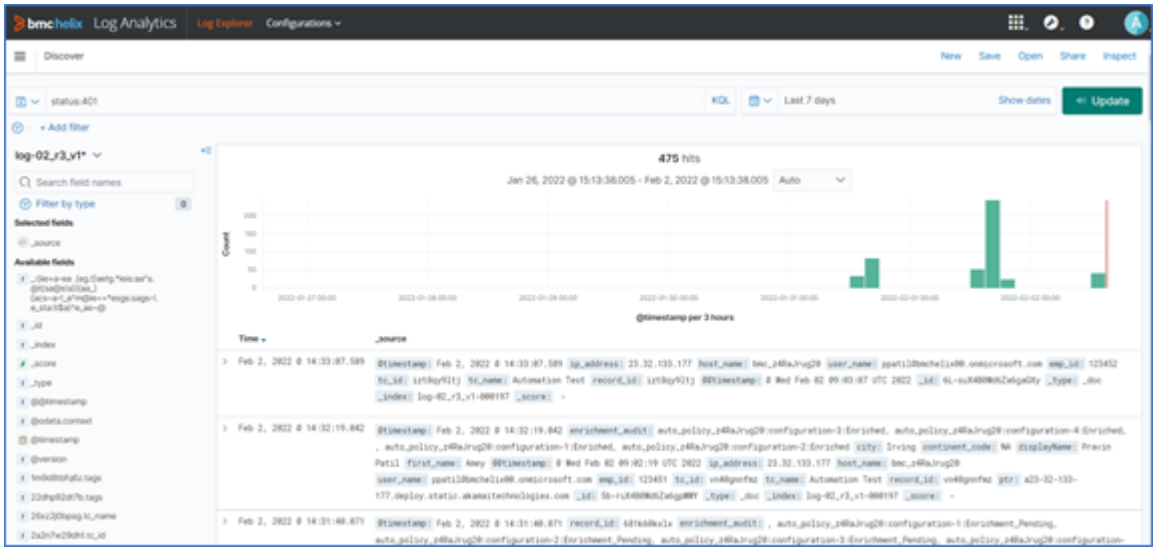

Figure 3. Discover and search logs in log explorer

Alerts and events

Alerts can detect issues quickly without waiting to look at the monitoring dashboard all the time. An administrator can create alerts for complex occurrences between many applications, which allows the ITOps team to take proactive action for the specific, tangible events that are generated.

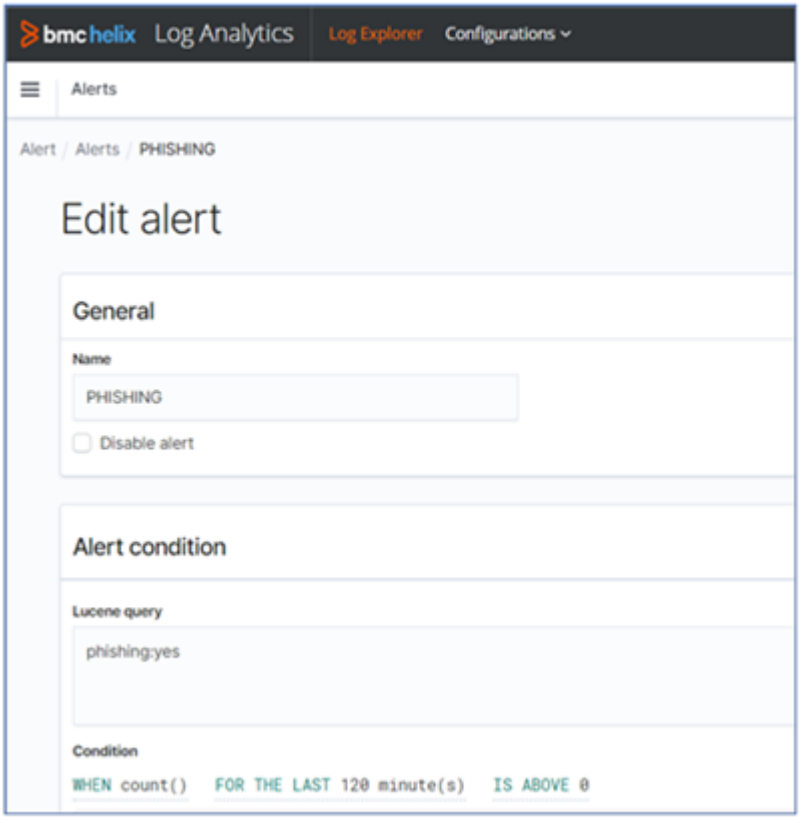

Figure 4. Alert configuration

While managing and analyzing log events, users can perform multiple actions, including notifying the end user via email. All log events are managed in the BMC Helix Operations Management (BHOM) portal and a user can cross-launch into BMC Helix Log Analytics to see the associated logs corresponding to that log event.

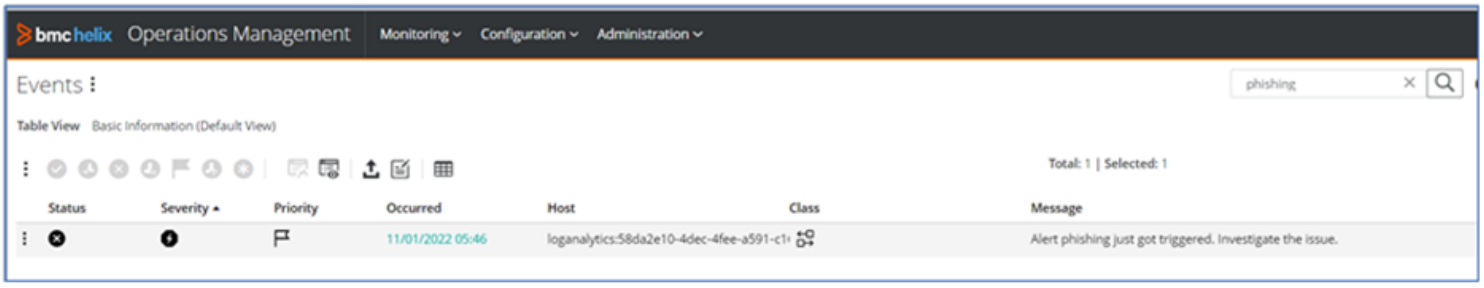

Figure 5. Analysing Log events in BHOM

If you're using BMC Helix Service Monitoring and a host is added in a log event, then it gets auto-correlated with other contextual events for a given service to provide root cause isolation and probable cause analysis. To dive further into the log event, it shows the key details and allows users to cross-launch into BMC Helix Log Analytics to see the associated contextual logs and diagnose the issue.

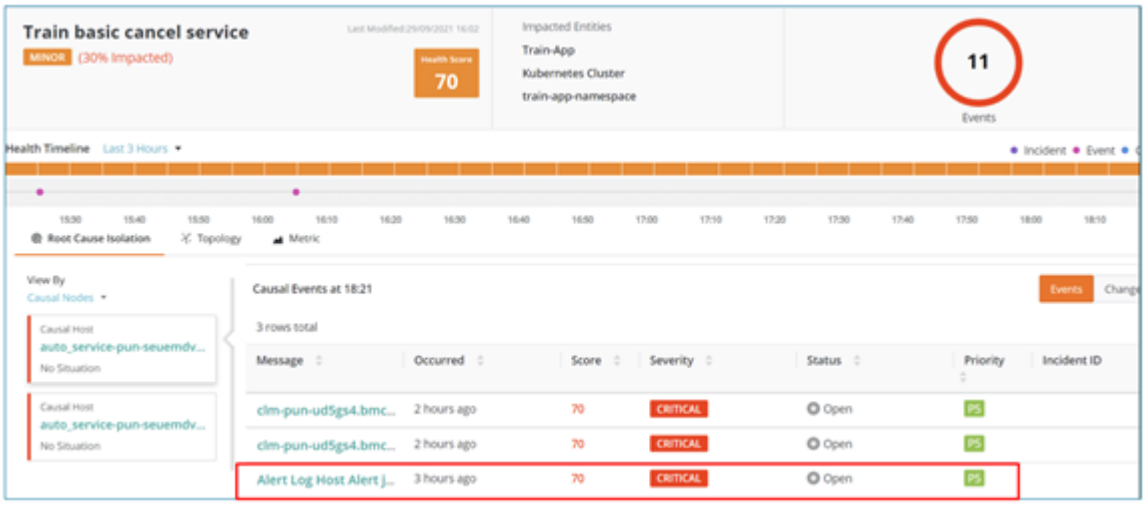

Figure 6. Root Cause Isolation using log events

A log event gets correlated with other events generated from metrics or third-party sources either for the same or different host to form a situation.

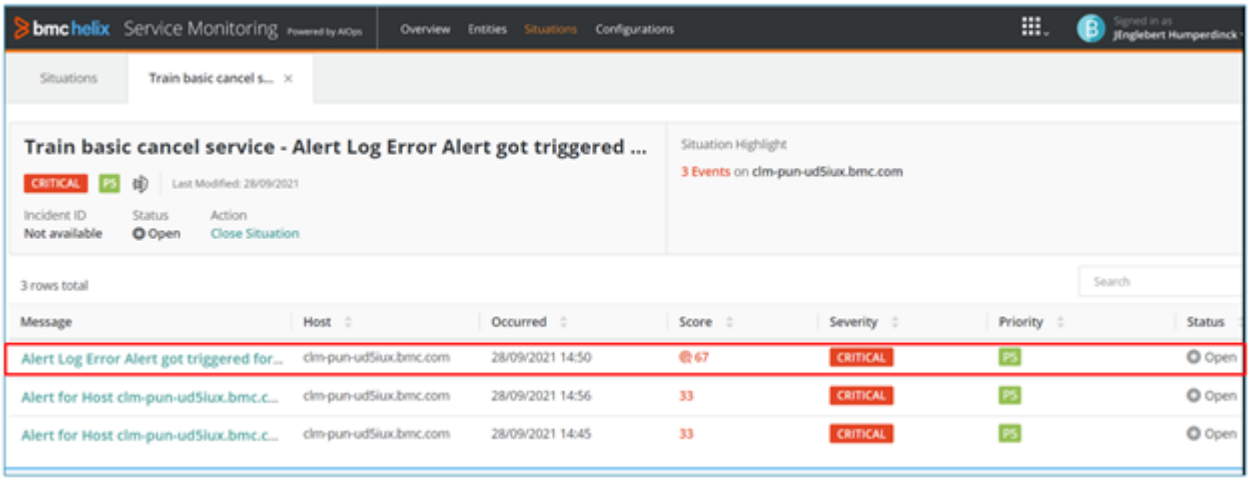

Figure 7. Situations using log events

Data visualization

A user can represent log data graphically by using BMC Helix dashboards to derive valuable insights, analyze issues, and identify trends, which may be useful for capacity and resource planning. All data is stored centrally, so it can be plotted across multiple sources to run cross-analyses and identify correlations.

BMC Helix dashboards provide various options to run queries and apply filters to dashboards so users can interrogate their data. A user can also drill down from the dashboard to specific data points to speed up the process of investigating unusual occurrences and quickly determine whether they're a sign of a real problem.

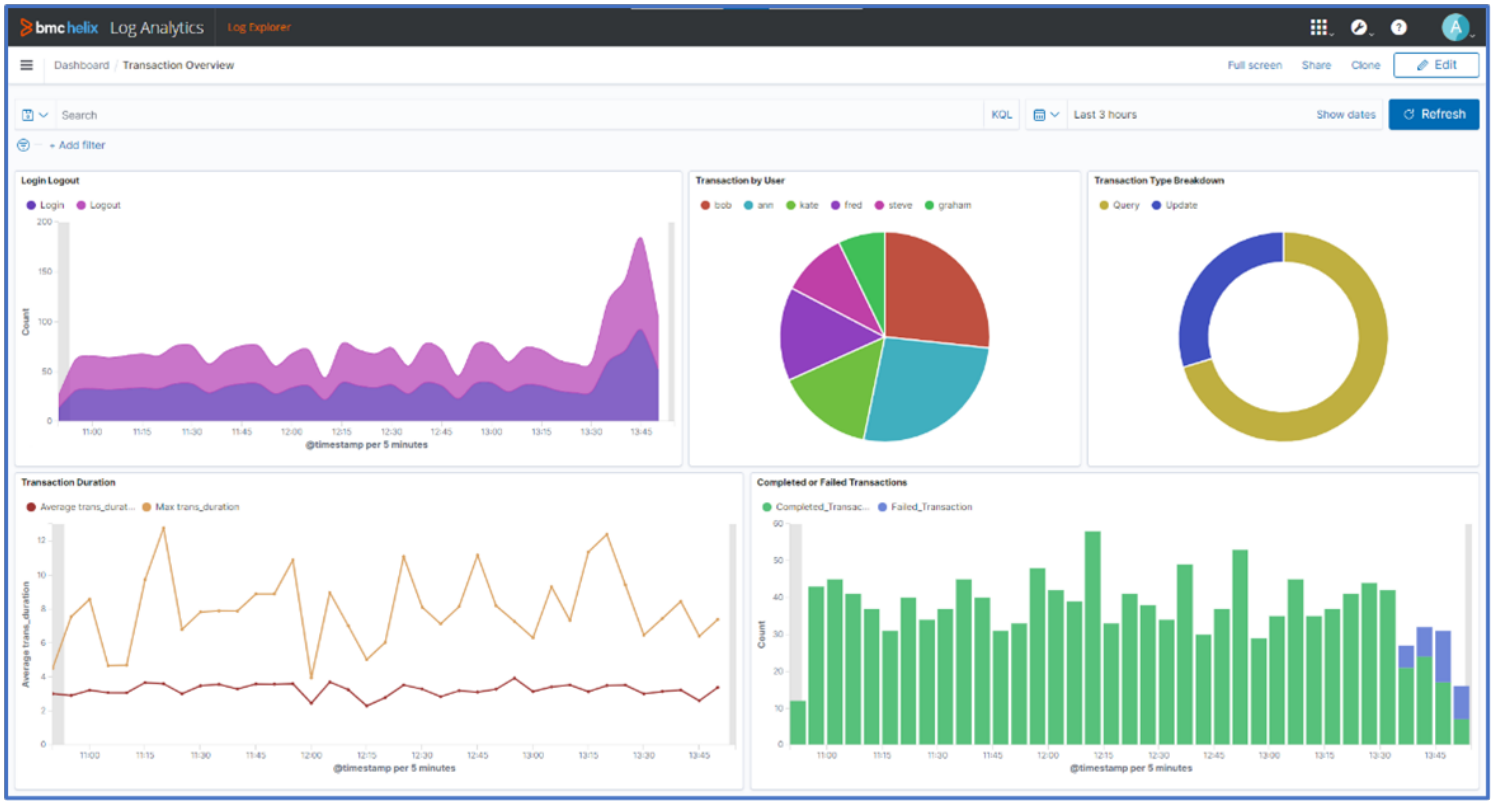

Figure 8. Monitoring using logs dashboard

To conclude, BMC Helix Log Analytics provides a wealth of insights into the usage, health, and performance of your systems, together with a powerful and efficient set of integrated capabilities for detecting and troubleshooting issues. Not only does it simplify and accelerate the process of collating, normalizing, and parsing your log data to make it available for analysis, but it also provides advanced artificial intelligence and machine learning (AI/ML) capabilities for noise reduction and root cause isolation with BMC Helix Service Monitoring powered by AIOps.

BMC Helix Log Analytics leverages ML to keep pace with your systems and data as they evolve and ensures that you get the maximum value from your logs. This in turn helps to free up your ITOps and SRE teams to focus on investigating true positives and making targeted improvements to their platform and infrastructure.

To learn more about BMC Helix and BMC Helix Log Analytics capabilities, watch our overview video here or visit www.bmc.com/helix or our documentation site.

Related blog

- Make Your Data Smarter with Log Enrichment