# Log Management Challenges in Modern IT Environments

Modern IT environments have presented many difficult-to-overcome challenges to organizations in recent times. One such challenge is gaining visibility into the systems. One may argue that due to **cloud computing** and limitless storage, it is now very easy to overcome some of the conventional challenges regarding visibility.

However, the architecture has changed into infrastructure scheduling and microservices. Hardware and software programs are now more complex, with their own set of challenges. These complexities have affected handling of **event log management**, which now requires specific tools and strategies to solve the visibility challenges.

## What Consists of an Effective Log Management Solution?

Your log management software must be able to:

* Back cloud-native log analysis for cloud services, containers and container orchestration
* Support storage that can be automatically scaled
* Support process engine that can transform **log data** as required
* Back log analysis with machine learning and anomaly detection
* Retain event log data with archivable and configurable storage
* Integrate log management system with notification tools like email or Slack
* Provide pre-built dashboards and support custom dashboards allowing for integration with cloud services

## The Challenges Facing Log Management

There is no doubt that log management is a very important issue, considering the need for adequate **log management tools** that can cater to the security and compliance requirements. Let us have a look at some of the common challenges faced by traditional log monitoring solutions.

**High Log Volume**

Going by the definition of log by National Institute of Standards and Technology (NIST) which states that “a log is a record of the events occurring within an organization’s systems and networks”, we can infer that everything creates log data. Firewalls, security software, computer systems and even operation systems generate **windows system event logs**.

For an organization to comply with security, the **log analyzer** must audit every log in an appropriate manner. Managing this large volume of log data, particularly in a big network, creates heavy burden on the IT resources. Hence, old school log monitoring tools are not as effective as ideally, they should be.

**Variety in Formats**

Every log comes from a different source. Thus, each source has a different format for generating and reporting logs to the **log monitoring tools** for analysis. To address this issue, many event log monitoring solutions have a common log format, but it’s not possible for all logs to comply with the same format.

Hence, even with the implementation of common log format, there is no guarantee that all your incoming **log data** will have the format similar to what is being currently analyzed. This in turn needs more effort and time to find out key information and interpret it as needed.

**Parsing Information Properly**

This leads to the next common challenge, parsing information within every log properly. When analyzing a **system event log**, it is necessary to do everything as accurately as possible. This means that information should be parsed line by line. There are various solutions to do this, but parsing log management information properly needs manual administration.

Moreover, if key information is missing, it is required to manually track it down and determine why it was absent from the logs initially. These issues make **information parsing** a big challenge for IT administrators, since they need to establish the rules by first knowing what they need to look for.

**Speed**

Another challenge of conventional log management is speed. Considering the huge amount of information collected from log server for analysis and storage, and the need to properly parse that information manually, effective **log management** requires more time. Either it’s fast or well-presented, but not both. It’s a challenge to maintain a correct balance between both.

## What is Centralized Logging Concept?

## For modern IT environments, log management should include log analysis, aggregation, storage and processing. These characteristics must be based on the principles of cloud computing i.e. scalability, resiliency, high availability, and automation, together leading to a centralized log management process.

## Analysis – querying the data to dissect it and creating dashboards and visualizations on top of it

## Aggregation – collecting and shipping logs from various data sources

## Storage – storing data for long periods of time to allow for log monitoring and trend analysis

## Processing – transforming log messages into knowledgeable data for easy analysis

## Alerting – getting notified of a real-time event

## Future of Log Management Solutions

## Log management has already seen many innovations time and again to combat these challenges. With time, the solutions are improving, with Security Information and Event Management (SIEM) dominating the sector because of highly effective and efficient management of these challenges related to event log management.

## SIEM is a solution that gathers log data from multiple sources in an IT environment, aggregates, analyzes and presents them in a manner that is easy to observe and store. SIEM solutions cater to many difficulties that exist in log management. They also enable IT staff to have a clear understanding of information security.

## Though information security will always depend mainly on the human factor, SIEM solutions are heading in the right direction. Many compliance standards such as ISO 27001 and Payment Card Industry Data Security Standard (PCI DSS) require you to include an SIEM solution to regulate information security.

## This is because where log management issues may cause your information security to weaken, an SIEM solution will help reinforce security in your environment and engage your resources optimally to deal with all other important tasks. Thus, it’s easier to manage and cater to security and log management simultaneously.

## Summing it Up

## It’s imperative that in order to manage a full-scale log management solution, considerable planning is required. Carefully chalk out your plan, look at potential solutions and then make a knowledgeable decision. VirtualMetric provides comprehensive package of powerful log monitoring to help you ensure the infrastructure reliability, conduct security auditing, and comply with security standards.

## As part of our Analytics Suite, benefit from our Log Analytics module, which helps you collect and analyze logs from various sources, and presents them on a user-friendly dashboard. You can also discover SIEM capabilities along with change tracking for log server inventory. Get in touch with VirtualMetric today for a free trial.