Log monitoring can be a tedious process. When you have logs, you generate numerous log files in the log database that you need to track. Though a **log file parser** can help you search through multiple or large logs easily, it’s typically one of those processes which we only look at once it stops working.

The windows system logs contain operating system logs as well as logs from applications such as **Internet Information Services** (IIS) and SQL server. These windows system event logs use structured format, which makes them easy for search from their event log location and faster to analyze. Let’s look at some important aspects of log monitoring.

**What is a Log?**

A log is a comprehensive list of events that happen within your system, website, server access or user events. **Event log monitoring** can help you track many things. A log analysis can help prevent vulnerabilities, improve services and raise alerts for potential bottlenecks. Log data can be a valuable asset to track and prevent problems.

**All Logs are Different**

Typically, event log types are chronologically appended for easy use. But not all logs are same, with every log type representing different event, such as authorization logs, debug logs, system logs, application event logs, audit logs, IIS logs and **Active Directory logs**. Hence, different log monitoring reports are generated for each log.

**Which Log Monitoring Reports You Must Have?**

Log monitoring is not an easy task for system administrators to manage, and this is why Windows server 2008 introduced **Windows event log forwarding** to make it easier for administrators to centralize client event logs and server. This made it more manageable to monitor all event logs without connecting to individual servers.

Let’s look at ten most important **event log management** and monitoring reports that every business must get with the help of [log management tools](https://www.virtualmetric.com/windows-monitoring).

1. **Firewall Log Monitoring**

Deploying security tools such as firewalls alone cannot secure your network completely. Rather, it’s the security data extracted from log monitoring tools which should be analyzed and reported for ensuring network security. A **firewall log analyzer** can reveal valuable information about the nature of incoming and outgoing traffic and security threat attempts to the administrators.

1. **Infrastructure Log Monitoring**

Infrastructure log monitoring is vital for managing policies, equipment, processes and all other resources affecting the enterprise’s IT foundation. To minimize downtime and increase efficiency, IT teams gather and interpret data of each component. **Infrastructure log analysis** tools also help to monitor Windows event logs or Linux log files.

1. **Server Log Monitoring**

A log management software can generate **server log monitoring** report, which helps you continuously detect and monitor server activities and alert administrators on potential issues or threats before a server problem arises. It helps you assess internal security policies and establish compliance with auditors. The reports generated can also help plan expansion of server capacity.

1. **Storage Monitoring**

Storage monitoring provides solution to evaluate **storage infrastructure** in real-time. A storage monitoring log tool helps to assess the slowdown happening on physical disks and the storage capacity requirements to ensure that there are enough resources for optimal performance, performance of controllers, device ports and physical disks.

1. **Login-Logoff Monitoring**

As more organizations are now allowing remote work and flexible working hours, it’s become more important for them to monitor and manage working hours of employees. The **log chart** can not only track employee login-logoff times, but also keep a record of lock and unlock activities to accurately assess employees time spent on their computer.

A good monitoring report can give an insight into employee attendance, productivity times, overtime threshold and suspicious access times stored in windows log files location. Such reports can give you a better understanding of a user’s connection time and provide detailed, accurate data required by the administration or management for **log aggregation** and decision making.

1. **Application Performance Monitoring**

Application Performance Monitoring or APM detects problems and patterns in an application. It tracks an application’s availability and performance at user’s end. For instance, an IIS log analyzer can tell us about IIS log file location, **IIS advanced login option**, and IIS error logs, etc.

The IIS log viewer or **IIS log reader reports** help optimize resource usage to drive a business towards growth. Application monitoring has become easy with log aggregation tools that can produce a real-time insight of application performance and security. The goal of APM reports is to provide insight into quality of experience delivered to end-users.

1. **Virtual Machine Monitoring**

As businesses are moving towards virtual IT spaces, virtual machine log monitoring reports have become an essential part of log management. It helps in network security by gathering, analyzing and archiving logs. **VM monitoring** also aids in managing virtualized tools, which is a very complex task.

Virtual Machine monitoring also helps to track VM resource health and usage, resolve problems in resource allocation, identify root causes of VM downtime and conduct **resource planning and management of VMs**. A VM monitoring report can provide metrics such as top memory and CPU consumers, network consumers along with health history of every virtual machine.

1. **Network Traffic Monitoring**

Network traffic monitoring is a difficult task that is very demanding if handled manually or with free tools. An effective **network traffic monitoring tool** can help network administrators maintain smooth operation of the network by monitoring performance and traffic throughout the network. It can also verify that no security breach occurs within the network.

1. **Database Monitoring**

Database monitoring tracks your database performance and resources to create and maintain highly available and high-performance **application infrastructure**. For instance, log monitoring SQL log server, Oracle and MySQL database reports include query, session and replication details, scheduled jobs and database performance. Data from all categories is analyzed to prevent or minimize slowdown and database outage.

1. **Service Monitoring**

Modern applications come with multiple services to support them. **Service monitoring** can keep an eye on your IT services and generate reports that help identify and monitor application and customer-defined services and find related issues. Effective monitoring tools will check the services in a hierarchical manner such hard disk capacity, CPU usage, and so on.

**Virtual Metric’s Log Management System**

[Virtual Metric’s Log Management and Monitoring](https://www.virtualmetric.com/windows-monitoring) software records logs and creates multiple reports for easy error tracking. It can also perform event log monitoring on **different operating systems** such as Windows, Linux and other UNIX systems. You can generate all the above-mentioned log monitoring reports and get a detailed insight into your system’s behavior.

With our log monitoring solution, you can collect, analyze and consolidate systems, network and Windows events along with performance and availability data. Get our free trial [here](https://www.virtualmetric.com/trial) for a complete log monitoring tool that provides you detailed analysis for better decision-making and optimal functioning of your systems.