Log File

sumologic.com/glossary/log-file

What is a Log File?

Enterprise organizations are increasingly choosing to deploy new applications and migrate existing ones to both private and public cloud computing environments. Cloud computing, especially in the public cloud, provides significant benefits that include cost savings through economies of scale, streamlined processes and simplified management with fewer administrative tasks.

As organizations depend on the cloud for more of their critical applications and services, there is a growing need to maintain network transparency and visibility, also called observability. Observability in the context of cloud computing depends on two factors: the presence of data outputs that accurately reflect activities and behaviors on the network, and the ability to aggregate and analyze that data.

Log files are the primary data source for network observability. A **log file** is a computer-generated data file that contains information about usage patterns, activities, and operations within an operating system, application, server or another device. IT organizations can implement security event monitoring (SEM), security information management (SIM), security information and event management (SIEM), or another analytics tool to aggregate and analyze log files from throughout a cloud computing environment.

Log File Categories for Common Operating Systems

Log files are automatically computer-generated whenever an event with a specific classification takes place on the network. The reason log files exist is that software and hardware developers find it easier to troubleshoot and debug their creations when they access a textual record of the events that the system is producing. Each of the leading operating systems is uniquely configured to generate and categorize event logs in response to specific types of events.

Windows Event Logs

The windows operating system can generate an event log in response to activity on any of its hardware or software components. Network security and operations analysts can use specialized software tools to aggregate and analyze these logs, detect patterns and trends, and respond to incidents or potential user issues. Windows is pre-configured to classify events in six categories:

- **Application Logs** - an application log is created when an event takes place inside an application. These logs help code developers understand and measure how applications are behaving during development and prior to release.

- **Directory Service Logs** - a computer that is configured to respond to security authentication requests within a Windows Server domain (known as a domain controller) may generate directory service logs. These logs record user privilege changes, authentication operations, and requests and other operations that take place in Windows Active Directory.
- **DNS Server Logs** - a Domain Name System (DNS) server contains the databases that match hostnames of websites on the internet with their appropriate IP addresses. Each time you navigate to a new web page, DNS servers are involved in processing the request and helping your browser get to the right page. DNS server logs are a special type of log file for recording activity on a DNS server.
- **File Replication Service Log** - another type of log file that is only available for domain controllers, they record information about file replications that take place on the computer.
- **Security Log** - security logs are created in response to security events that take place on the computer. These can include a variety of events such as failed log-ins, password changes, failed authentication requests, file deletion and more. Network administrators can configure which types of events are application events and which should be entered into the security log.
- **System Log** - system logs record events that occur within the operating system itself, such as driver errors during start-up, sign-in and sign-out events and other activity.

Linux Event Logs

The Linux operating system is uniquely configured to generate and store log files. Linux creates a continuous timeline of events that take place on the system, including every event related to the server, kernel, and running applications. Linux places events in four distinct categories:

- Application logs
- Event logs
- Service logs
- System logs

These categories are analogous to those used by Windows O/S.

iOS Event Logs

iOS takes a unique approach to event log generation when compared to other operating systems. iOS does not log every event that happens in the system, but it does generate documentation for application crashes. Later versions of iOS (10.0 and beyond) offer an API that can be used to log application events that take place on the system. The iOS logging API allows network administrators to access log file data from:

- App security
- Apple pay

- Data encryption
- Device controls
- Internet services
- Network security
- Privacy controls
- User password management

Why Do IT Organizations Monitor Log Files?

Large IT organizations depend on an extensive network of IT infrastructure and applications to power key business services. Logfile monitoring and analysis increase the observability of this network, creating transparency and allowing visibility into the cloud computing environment. Observability should not be treated as an ultimate goal, however - it should always be seen as a mechanism for achieving real business objectives, such as improving the reliability of systems, meeting security and compliance objectives and driving revenue growth.

Logfile monitoring and analysis can help IT organizations **improve the reliability of their systems** for the end-user. Log files include information about system performance that can be used to determine when additional capacity is needed to optimize the user experience. Log files can help analysts identify slow queries, errors that are causing transactions to take too long or bugs that impact website or application performance.

IT organizations can use log file monitoring to **maintain the security posture of cloud computing environments** and prevent data breaches. Log files capture things like unsuccessful log-in attempts, failed user authentication, or unexpected server overloads, all of which can signal to an analyst that a cyber attack might be in progress. The best security monitoring tools can send alerts and automate responses as soon as these events are detected on the network.

IT organizations can also use log file monitoring to **improve their business decision-making**. Log files capture the behavior of users within an application, giving rise to an area of inquiry known as user behavior analytics. By analyzing the actions of users within an application, developers can optimize the application to get users to their goals more quickly, improving customer satisfaction and driving revenue in the process.