Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Logging: What is it and why is it important?

Why you need logs and how they can help

Audience: General

Reading Time: 5 Mins

Log files are highly valuble data sets which are frequently used by software developers and engineers to understand what has gone wrong. Is that the limit to their value?

Logging is more than just a tool for developers and engineers to figure out what they have done wrong. Logging should be used to produce thorough audit logs so that if a forensic investigation is required to be done by the authorities, they can then reproduce what occurred in step-by-step detail.

How do developers and engineers use logging?

Logging messages is often a quick and easy way to confirm something is working the way it should be. Developers often use logging commands to debug their programming code and engineers may use it to gain insights into how a particular piece of software operates under the hood.

So, why does logging exist? Everything from a database, to a cloud server will have some type of logging. Generally they are setup by default to log the bare minimum. Often used by system installers and designers to confirm that software and packages have installed correctly. However, the underlying logging systems are often far more robust and can offer much greater depth and clarity of what is happening.

There are many different logging levels and types out there. Depending on the software being used, there is usually anywhere from three to eight different logging levels that can be switched between. These logging levels can also be referred to as logging types. Often the lowest level with the least detail is called the alert log, however as the levels increase, the logging messages verbosity increases. The alert log would only record alerts, an error log would record alerts and errors, there is also usually an info log level that records more details and the highest logging level is usually debug which records everything that the software is doing.

European Union
European Regional Development Fund
The Cyber Foundry project is part funded by the European Regional Development Fund

Lancaster University

MANCHESTER 1824
The University of Manchester

Manchester Metropolitan University

University of Salford MANCHESTER

Setting Your Logs

How do you choose the appropriate log level?

Sadly, there is no simple way to know which logging level you should use. The best method is to test the different levels and find the sweet spot in verbosity related to your businesses use of that software. Some logging levels may report data from the underlying software that is irrelevant to the businesses use, whereas other levels may lack clear details on the actions being triggered and what or who caused the trigger.

How could correctly setup logs help my business?

Once a log is setup correctly it will record exactly what is happening, when it happened and by whom it was initiated. It will detail what the setting or parameter changed was before, and what it has become. It will log all activity - potentially even passive use, where a user logs on but takes no direct action and only views specific data. Logs can detail what has been deleted in such a way that allows recovery, and this is where logs become important to a business.

During an attack data may be changed or deleted by an attacker. They may modify settings or parameters to make it easier for them to attack you again, even after you think you have removed them from your systems. By having detailed logs we can see exactly what they have done, and from that envisage what there plans were and would be going forward.

The more details we have the better we can understand what happened and prevent it from happening again. With less robust logs we may only know an attack occurred and not have the ability to rewind time to understand the exact steps the attacker took.

There are some common logging configuration mistakes and pitfalls. Over time, logs can become extremely large. Most logging software have options to enable rotation and to limit the size of an individual log. These may not always be setup correctly by default. It is a good idea to enable log rotation and to rotate each log once it has reached a specific size. You may also wish to set-up a backup service that will automatically store logs into the cloud for example.

Any kind of automatic syncing software could work if your servers are locally hosted. If your servers are remote/cloud hosted it is best to speak with your service provider about log retention and the backup services that they offer.

Definitions

Debug - Debugging is the process of finding and resolving defects or problems within a computer program that prevent correct operation of computer software or a system.

Trigger - When an event occurs, such as a mouse click, it will be handled and then passed to a function for processing. There are several steps involved in processing events, but the whole procedure is generally referred to as a trigger or trigger function in event-driven programming.

Automatic syncing -
A synchronisation process can occur either manually via a trigger or automatically. Generally, automatic syncing triggers occur when a file has its data changed. This data could be the contents of the file or specific parameters that relate to the file such as its permissions or owner.

Further Reading

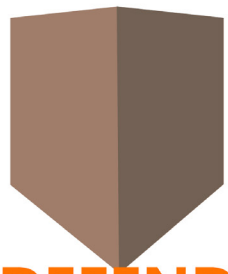
About the Authors

Robert Marsh is a published Internet of Things Forensics Researcher and an award-winning Artificial Intelligence Software Developer. He is currently working as a Cyber Security Analyst with the Greater Manchester Cyber Foundry technical team at The University of Salford.

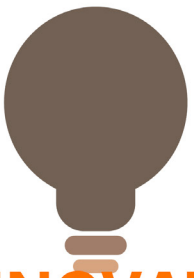
University of Salford MANCHESTER

READ MORE

1. dotCMS. "Special Logging Configurations." DotCMS Content Management System, dotcms.com/docs/latest/special-logging-configurations.
2. "log4j - Logging Levels." Tutorialspoint, www.tutorialspoint.com/log4j/log4j_logging_levels.htm
3. WatsonMatt, Matt. "What Is Structured Logging and Why Developers Need It." Stackify, 13 Dec. 2018, stackify.com/what-is-structured-logging-and-why-developers-need-it/.
4. "Why Do Engineers Care About Logging?" Scalyr, 24 July 2019, www.scalyr.com/blog/why-do-engineers-care-about-logging



DEFEND



INNOVATE

GROW

European Union
European Regional Development Fund
The Cyber Foundry project is part funded by the European Regional Development Fund

Lancaster University

MANCHESTER 1824
The University of Manchester

Manchester Metropolitan University

University of Salford MANCHESTER