Three important things you need to know about syslog

Why are syslogs important?

System logs (syslogs) store messages produced by host systems. These logs are useful for system management, security auditing, and software debugging. You may also need to provide syslogs to compliance auditors or law enforcement. As a result, you can run into problems without comprehensive and accurate syslogs. Without good syslogs, audit trails can run cold or you may fail compliance audits.

In the past, syslogs could be traced back to local physical devices, such as computers, printers, or routers. However, with the proliferation of VMs and cloud container architectures, syslogs are now more likely to refer to remote logical devices. Since logical devices are much more dynamic and ephemeral than physical devices, the importance of syslog management on modern infrastructures only increases.

VMs and containers are software defined devices that can be deployed or destroyed at whim. They may move from one server to another based on dynamic loads, spawn new instances of themselves, or migrate to new locations. This makes syslogs on modern infrastructures more difficult to collect, process, and parse. This is the reason why many organizations are now turning to automated log management solutions.

Syslog management

Now we know that syslogs are important, but do you need to manage them?

One possible option is to not manage them at all. We could call this laissez-faire syslog management, or simply, lazy syslog management. The benefit of this method is that it consumes no upstream cycles. The downside is that when you need to access your syslogs, they may be difficult to find. Syslogs are usually archived (rotated) or deleted to save precious storage space. So, while you can save time by not actively managing your syslogs, more time is lost later when you need to search for them. Also, this approach will result in much more stress, because when you need the logs, you really need the logs. In the case of syslogs, non-management is not a viable option.

Syslog Daemons

Linux systems come prepackaged with syslog daemons that automatically collect system events. These daemons capture syslog messages and store them in log files under `/var/log` on each host. These syslog daemons can also be configured to forward log files to one or more remote syslog servers for easy retrieval and backup. There are similar logging agents that run on Windows systems, but they are not pre-installed as part of the operating system.

The most common syslog daemons are syslogd, rsyslog, and ng-syslog. Syslogd is the original logger dating back to the early days of Linux. The other two are more recent inventions that add extra features to the basic syslogd functionality. Although each tool has its own use cases, they all play by the same rules, defined as the syslog protocol (RFC 5424). The syslog protocol defines a layered architecture that separates message

content from message transport. This means that every syslog message contains both structured and unstructured data. The structured data defines message attributes such as type and severity, while the unstructured portion carries the message content.

Unified Log Management

Since most servers run Linux, they automatically collect syslogs. To begin harvesting this valuable data you just need to setup one or more syslog servers and then configure your syslog daemons to forward syslogs to them. With all your logs in a central location, you will then be ready to take the next step to automated log management. An automated LMS can easily ingest consolidated syslog data for further analysis.

Syslog aggregation is a start, but you should really put all that data to use. Although syslogs include some structured data, it is not trivial to extract meaningful information from them. The messages are unstructured, and the data velocity is too fast for manual inspection. This means that only machine analysis can extract meaningful insights. With the right analysis engine in place, you can detect and resolve issues in real-time. Stop hoarding your syslogs for a rainy day and start extracting business insights instead.

Although syslogs are important, they don’t tell the whole story. Centralized log management solutions can easily correlate syslogs with other data sources, such as application or network events, to form a unified view of your infrastructure. They also include natural language search and graphical user interfaces that anyone can use. Allowing authorized access to this unified infrastructure data allows teams to share information more freely and discover new ways to improve operations.