What is Syslog?

Syslog is a protocol and utility for capturing and logging system information. This system information can be stored locally, remotely, or both. syslog allows a server to forward log messages over the network to SL1. SL1 then uses these messages to monitor the health of the server and trigger events (if necessary).

Because the syslog utility is mature and widely-used, there is an array of commercial and open source implementations. This section provides only a basic outline of how to configure syslog to send messages to SL1.

Entries in a syslog can include the following severity descriptions:

| **Severity** | **Description** |
| --- | --- |
| 0 Emergency: | System is unusable. A "panic" condition. Notify all technical staff. Affects multiple servers, applications, systems, or sites. For example, an outage caused by an earthquake. |
| 1 Alert | Failure in primary system. Immediate action is required. Notify appropriate staff. Example would be "loss of backup ISP connection". |
| 2 Critical | Failure in primary system. Immediate action is required before problem escalates to "alert". For example, "loss of primary ISP connection". |
| 3 Error | Non-urgent failure. Action is required but not urgent. These messages should be relayed to appropriate support staff for resolution. |
| 4 Warning | Indication that an error is about to occur. Action is required but not immediately. For example, "file system is 85% full". |
| 5 Notice | Normal but significant condition. No immediate action required. Events that are unusual but are not considered error conditions. Should be examined to spot potential problems. |
| 6 Informational | Normal operational messages. No action required. These may be harvested for reporting, measuring through-put, etc. |
| 7 Debug | Information that is useful to developers for debugging the application; not useful during operations. |

7. Configure your Linux system to send syslog messages to a syslog serverand Read them

**Intro**

System, network, and host log files are all be valuable assets when trying to diagnose and resolve a technical issue. The difference between having logs and not, could be hours or days of troubleshooting a particular problem. Most of the time, you don’t have hours or days to solve these problems, so make sure you have log files. Better yet, make sure you have easily accessible log files. Better than that, easily accessible and redundant log files.

Redundancy when it comes to sensitive or impactful data is crucial. What if you wanted to see exactly what happened internally before a network device or workstation went down permanently? What if an attacker was successful with an intrusion, did some damage, and covered up their tracks by altering the local logs? You can see why neglecting to *centralize*your logs can be detrimental.

8. Install and Run Splunk on Linux

**What does Splunk do?**

As simply as possible, we offer a big data platform that can help you do a lot of things better. Using Splunk the right way powers cybersecurity, observability, network operations and a whole bunch of important tasks that large organizations require.

Splunk is the key to enterprise resilience. Put simply, that means organizations who use Splunk can tackle digital disruptions a whole lot differently.

To that end, Splunk offers a whole suite of various software, apps and APIs, plus a whole lot of flexibility for your future needs. Our solutions help organizations mature your digital resilience, so you can adapt to anything. The most-well known Splunk products include:

Splunk Enterprise lets you search, analyze and visualize all of your data, providing insights you can act on in real time.

Splunk Cloud Platform which offers data search, analysis and visualization in the cloud (SaaS).

Our Universal Forwarder is the most popular way of getting data into Splunk Enterprise and Splunk Cloud Platform. (Though, to be clear, there are many ways to get data into Splunk.)

Splunk Enterprise Security is our SIEM that helps you do all sorts of things, including security monitoring, incident response and management, compliance and threat hunting.

Our SOAR, user behavior analytics (UBA) and observability solutions.

9. Install and Configure ELK on Linux

The ELK stack is an acronym used to describe a stack that comprises three popular projects: Elasticsearch, Logstash, and Kibana. Often referred to as Elasticsearch, the ELK stack gives you the ability to aggregate logs from all your systems and applications, analyze these logs, and create visualizations for application and infrastructure monitoring, faster troubleshooting, security analytics, and more.

E = Elasticsearch

Elasticsearch is a distributed search and analytics engine built on Apache Lucene. Support for various languages, high performance, and schema-free JSON documents makes Elasticsearch an ideal choice for various log analytics and search use cases.

L = Logstash

Logstash is an open-source data ingestion tool that allows you to collect data from various sources, transform it, and send it to your desired destination. With prebuilt filters and support for over 200 plugins, Logstash allows users to easily ingest data regardless of the data source or type.

Logstash is a lightweight, open-source, server-side data processing pipeline that allows you to collect data from various sources, transform it on the fly, and send it to your desired destination. It is most often used as a data pipeline for Elasticsearch, an open-source analytics and search engine

K = Kibana

Kibana is a data visualization and exploration tool used for log and time-series analytics, application monitoring, and operational intelligence use cases. It offers powerful and easy-to-use features such as histograms, line graphs, pie charts, heat maps, and built-in geospatial support. Also, it provides tight integration with Elasticsearch, a popular analytics and search engine, which makes Kibana the default choice for visualizing data stored in Elasticsearch.

10. Install and Configure GrayLog on Linux

**Introduction**

Graylog is a powerful platform for collecting, storing, analyzing and monitoring logs. It allows organizations to centrally collect and analyze data from various sources, providing convenient access to information and valuable insights about the state of the system. In this article, we will look at why Graylog is needed, its advantages and disadvantages, as well as its application areas.

Graylog is an open source software developed for processing and analyzing log files. It is based on Elasticsearch, MongoDB and Apache Kafka, which provides scalability, fault tolerance and high performance. Graylog provides centralized storage for log files, integrates with various data sources and provides a user-friendly interface for searching, filtering and analyzing data.

**Why is it needed:**

Graylog plays an important role in the security, monitoring and debugging of systems. It allows you to detect and analyze problems related to performance, security and rule violations, providing operational information for decision-making. Some of the main reasons for using Graylog:

Log File Collection and Storage: Graylog provides centralized storage and indexing of log files from all servers and applications in the organization. This allows you to effectively manage and analyze data, making it easy to detect problems.

Monitoring and Notification: Graylog provides the ability to configure monitoring rules and alerts to quickly respond to problems and events in the system. Automatic notification allows you to reduce the reaction time and minimize losses in case of failures or violations.

Data Analysis and Retrieval: Using powerful real-time data analysis and retrieval tools, Graylog allows you to detect trends, anomalies and links between events. This helps to identify the causes of problems, optimize performance and improve system security.