# Linux Logging: Syslog and Log Collection

Reading

30 minutes

✓ Status Incomplete

## Introduction

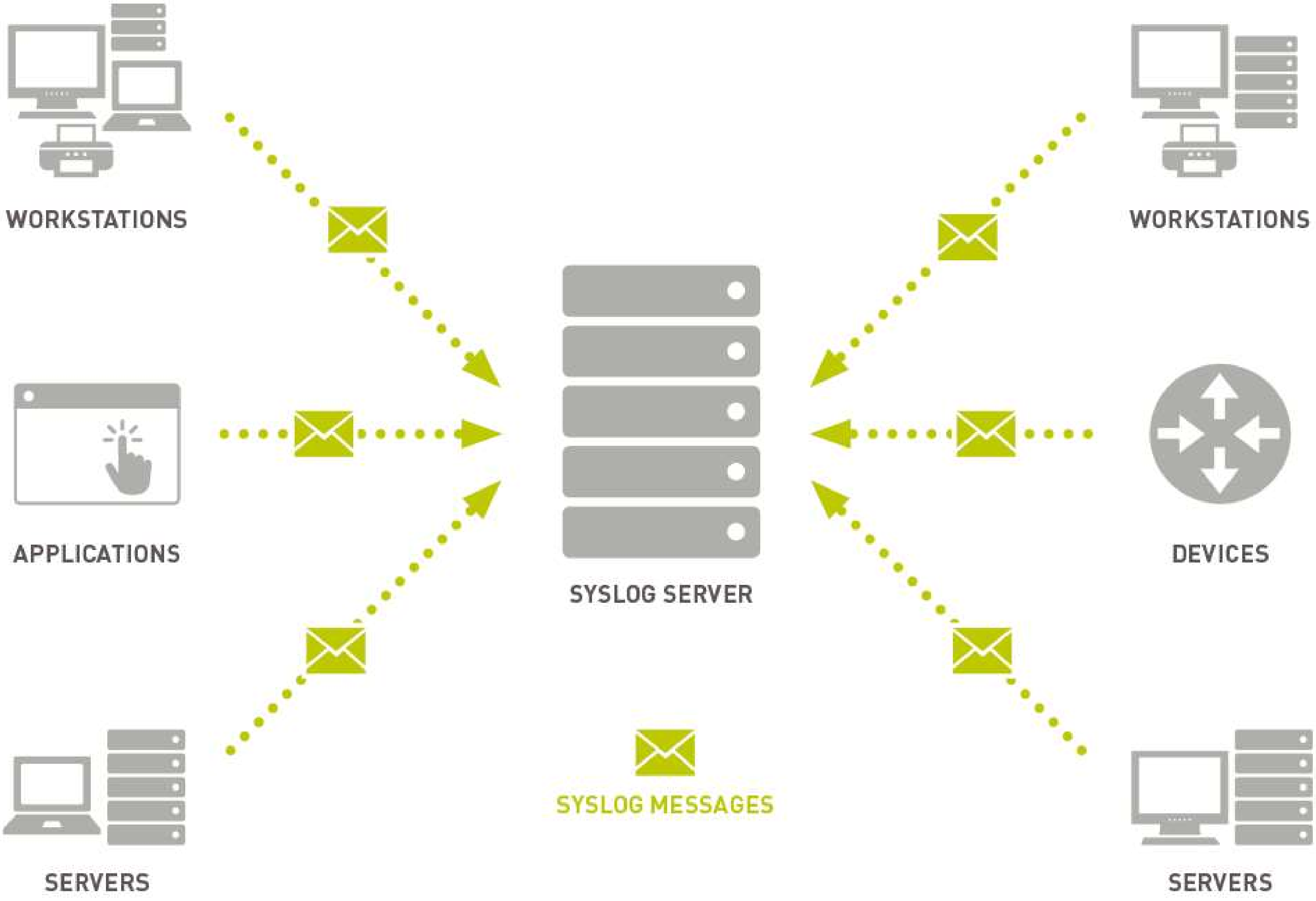
In this reading, you will learn about **System Logging Protocol** or **Syslog** and **log** collection as a way to have a centralized location for the searching and evaluating of log contents. Syslog is the general standard for logging system and program messages in the Linux environment.

## Reading

**Syslog** consists of two parts: The first is a client that can export or send its logs using the **Syslog protocol** and the second, a server, called a **Syslog server**, that collects the logs.

**Syslog** is available on Unix- and Linux-based systems and many web servers including Apache. This service constitutes the system log daemon, where any program can do its logging which includes a severity level (e.g., "debug", "info", "warning", "error") and message text. Syslog is not installed by default on Windows systems; they use their own Windows Event Log.

In this diagram from Paessler, you can see the typical logical layout of Syslog.



*(image source: Paessler)*

As you examine the layout, you should observe in **Syslog** that there is a central server that events can be logged to. All that is typically needed is that the clients be given the server's address.

## The Benefits and Limitations of Using Syslog

This protocol provides you with a single view of all of your device health and connectivity statuses. This means it can allow easy monitoring and quick responses when issues are detected.

There are also benefits to collecting and storing log messages from multiple devices and servers in a single location, and not on the originating system. This way if a bad actor tries to cover their tracks, the logs are out of reach.

Because Syslog uses **UDP** or **TCP**, the protocol is routable. This means that one Syslog server can cover a whole organization. With proper security such as aN SSL connection, this also means that the server can be cloud based and serve a global organization.

One of the major limitations of Syslog is that it is an active protocol that needs to send its output to a server and does not store them at the client. This means, for example, that if the network is down, the server will not receive the Syslog messages and an event might go by unnoticed.

Another limitation to Syslog is the system itself offers no security for the messages being sent. They can be read by anyone on the network, creating a security concern if the log data contains sensitive information. There is also no built-in mechanism for encryption, so this sensitive information can be compromised if intercepted. To add to these limitations, there is also no built-in authentication of the source of a message. This means that an attacker could potentially send false messages to a Syslog server, making it difficult to trust the integrity of the log data.

# Further Reading

## Syslog

> Read the following articles and focus on the Syslog components and transmission. Make sure that you understand the parts of a **Syslog** message, as these will help you when you need to analyze them in **Wireshark**.

1. IT Explained: Syslog.

In this reading, you will examine some common implementations of Syslog and of the types of events that are commonly seen.

1. Syslog Tutorial: How It Works, Examples, Best Practices, and More

> You do not need to memorize the values in the **Syslog** message, but you will need to know where to look them up if needed.

✓ Mark Completed

← Previous
Windows Logging

Next
Centralized Logging →

### How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

# W01D4

Thu Jun 27

› Lectures (1)

## Work (7)

**4 hrs**

- 📖 Common Network Conversations & Their Protocols
- ? Network Administration Quiz ✓
- 📖 Windows Logging
- 📖 Linux Logging: Syslog and Log Collection
- 📖 Centralized Logging
- ? Logs
- 📖 Troubleshooting Approaches

W01D4 Schedule »