**Layers of Syslog**

1. Syslog content:

* This layer refers to the information contained in the event message.
* It includes details about what happened, such as system errors, warnings, or other activities that can help to understand the issue when a network device encounters a problem.

1. Syslog application:

* This layer is responsible for generating, routing, interpreting, and storing the syslog messages. It creates and manages the syslog functionality.
* The syslog application captures the event messages, determines how to handle them, and decides where to send or store them.
* It acts as the intermediary between the source of the event (e.g., a network device) and the destination (e.g., a log file or a syslog server).

1. Syslog transport:

* This layer deals with the transmission of syslog messages from the source to the destination.
* It defines how the messages are sent over the network or transported between different systems.
* The transport layer use various protocols, such as User Datagram Protocol (UDP) or Transmission Control Protocol (TCP), to ensure reliable delivery of the syslog messages reach their intended recipients.

**What Is Syslog Server?**

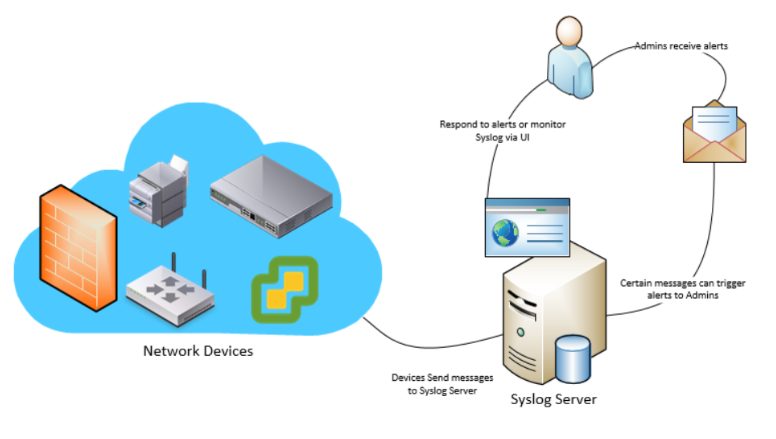
Syslog servers are used to collect syslog messages in a single location.

A syslog server might be a physical server, a standalone virtual machine, or a software-based service.

To make it possible for syslog servers to receive, interpret, and store the messages, they usually have a couple of common components:

Syslog Listener: This allows the server to receive messages by gathering Syslog data.

Database: This is important for larger networks to be able to store syslog data for easy reference.



|  |  |  |
| --- | --- | --- |
| Aspect | Syslog | Event Log |
| Purpose | Logging, capturing, transmitting a wide range of system messages | Stores information about specific events only |
| Scope | Widely used across different platforms | Primarily used and integrated in Windows operating systems |
| Event Types | Captures various types of system events | Focuses on specific events like application errors, login sessions, password attempts, locked accounts, etc. |
| Information Stored | Contains customizable event details | Stores standardized event information (date, time, user, event ID, source, etc.) |
| Source | Can be generated by multiple devices or applications within a network | Typically generated by the operating system, applications, or services within the system |
| Accessibility | Typically sent to a centralized syslog server or stored in log files | Accessed locally on the system or over the network |

What Does Syslog Do?

Syslog provides a way for network devices to send messages and log events.

Syslog has a standard format; all applications and devices can use.

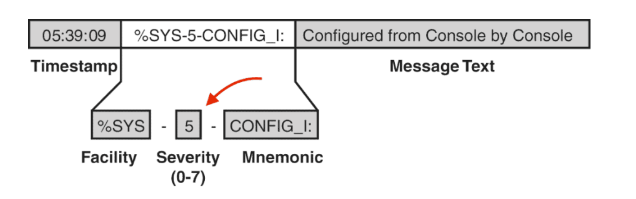
A syslog message contains the following elements:

* Header
* Structured data
* Message

Syslog Header

The header includes information about the version, time stamp, host name, priority, application, process ID, and message ID.

The structured data comprises data blocks in a specific format, which is followed by the log message.



Log messages should be encoded using the 8-bit Unicode Transformation Format (UTF-8), but apart from that, the messages can be configured based on individual needs.

The flexibility of the message content is part of what makes syslog so popular and effective.

The severity levels for syslog messages range from 0, which signals an emergency, to 5, which constitutes a warning.

There are additional options for informational messages (level 6) and debugging (level 7).

While this information is advantageous, you can’t use syslog to gather information from devices the way you can with Simple Network Management Protocol (SNMP).

Syslog only supports sending messages to a defined location when certain events happen.