LOG ANALYSIS

(PART 2)

COMPONENTS OF A LOG

It includes different entries present in a log.

COMMON LOG COMPONENTS

- Timestamp
- Hostname or Source Identifier
- Application or Process Identifier
- Severity Level
- Log Message
- User or Entity Information
- Event ID or Unique Identifier
- Status or Outcome
- Additional Metadata
- Custom Fields

TIMESTAMP

It indicates the date and time when the event occurred.

Essential for chronological ordering of events and correlating activities.

Example:

2023-12-19 15:30:45 (Year-Month-Day Hour:Minute:Second)

HOSTNAME

Identifies the source of the log entry, often the device or system generating the log.

Helps identify the origin of the event in a networked environment.

Example:

web-server-01 or 192.168.1.100

PROCESS IDENTIFIER

Specifies the application or process related to the logged event.

Facilitates categorization and quick identification of the source.

Example:

sshd (SSH daemon), apache (Apache web server)

SEVERITY LEVEL

Indicates the severity or importance of the event.

Assists in prioritizing and filtering events based on their impact.

Example:

INFO, ERROR, WARNING

LOG MESSAGE

Contains detailed information about the event or activity.

Provides context and specifics about what happened.

Example:

Accepted publickey for user123 from 192.168.1.100 port 22 ssh2

USER INFORMATION

Specifies the user or entity associated with the event.

Helps in user activity tracking and security investigations.

Example:

user123, admin

EVENT ID

A unique identifier assigned to each log entry.

Facilitates referencing and tracing specific events.

Example:

EventID: 1234-5678-ABCD

STATUS

Describes the result or outcome of the event.

Indicates whether the event was successful or encountered an issue.

Example:

Success, Failure

ADDITIONAL METADATA

Supplementary information providing context to the event.

Enhances the understanding of the log entry.

Example:

Session ID, Source IP, Destination IP

CUSTOM FIELDS

Organizations may include additional fields specific to their needs.

Tailors log entries to meet unique requirements.

Example:

CustomField1: value1, CustomField2: value2

LOG FORMATS

LOG FORMATS

Log formats refers to the structure in which log entries or records are presented within log files.

- Increase Readability
- Increase Interoperability

COMMON LOG FORMATS

- Syslog
- JSON
- CSV
- XML
- Custom Formats

SYSLOG

Syslog is a standard for message logging, offering a way for devices to produce and consume logs.

Each syslog entry consists of a timestamp, hostname, application, severity level, and the log message.

See Example →

SYSLOG CONT...

Example:

<13>Jan 25 08:31:45 web-server-01 sshd[1234]: Accepted publickey for user123 from 192.168.1.100 port 22 ssh2

- <13>: Syslog priority (facility 1, severity 5).
- Jan 25 08:31:45: Timestamp.
- web-server-01: Hostname.
- sshd[1234]: Application (sshd process with PID 1234).
- Accepted publickey...: Log message.

JSON

JSON is a lightweight data interchange format using key-value pairs.

It provides a structured and easy-to-read format.

See Example →

JSON CONT...

Example:


```
{
"timestamp": "2023-01-25T08:31:45",
"hostname": "web-server-01",
"application": "sshd",
"severity": "INFO",
"message": "Accepted publickey for user123 from 192.168.1.100 port 22 ssh2"
}
```

CSV

CSV separates values with commas and is straightforward for both humans and machines.

Example

```
2023-01-25 08:31:45,web-server-01,sshd,INFO,Accepted publickey for user123 from 192.168.1.100 port 22 ssh2
```

XML

XML uses a hierarchical structure with tags, making it easy to represent nested data.

See Example →

XML CONT...

Example:

```
<log>
  <timestamp>2023-01-
25T08:31:45</timestamp>
  <hostname>web-server-01</hostname>
  <application>sshd</application>
  <severity>INFO</severity>
  <message>Accepted publickey for user123
from 192.168.1.100 port 22 ssh2</message>
</log>
```

CUSTOM FORMATS

Organizations may use custom log formats tailored to their specific needs.

Example:

[2023-01-25 08:31:45] [INFO] [web-server-01] [sshd] Accepted publickey for user123 from 192.168.1.100 port 22 ssh2

IN THE LAST **PART 3,** I WILL DISCUSS

LOG COLLECTION METHODS, SOURCES & LOG ANALYSIS TECHNIQUES