Linux Incident Response - The journal

Taz Wake | Halkyn Consulting Ltd | Originally published 2023-11-09

High-level summary

The systemd journal is a logging mechanism that has become an integral part of the systemd suite, which is the init system and service manager for modern Linux operating systems. It provides a centralized logging solution, replacing traditional text-based logging systems like syslog. This journal is designed to collect and store logging data in a structured, indexed binary format, which offers several advantages over traditional logging methods, including better performance, more efficient storage, and the ability to include detailed metadata with each log entry.

Data is written to the systemd journal by services and applications which use the native systemd logging API or by intercepting stdout and stderr of daemonised processes. This data includes standard logging information such as timestamps, message severity levels, and the text of the message itself. In addition to this, the systemd journal also captures comprehensive metadata for each log entry, including the process ID, user ID, boot ID, machine ID, hostname, and other system and service-specific information.

The systemd journal stores its data in binary files located in /var/log/journal/ by default. The location can be changed by modifying the systemd-journald service configuration. These files are organized in a way that makes it easy for the systemd-journald service to manage and rotate logs efficiently, and to quickly retrieve log entries based on various criteria.

For forensic investigators, the systemd journal provides a wealth of information. One crucial aspect is that it stores the timezone alongside each log entry. By default, timestamps are stored in the journal as Coordinated Universal Time (UTC), which provides a standard reference time and avoids issues with local time changes such as daylight saving adjustments. However, when viewing logs using journalctl, the system's local timezone setting is applied, making the logs more readable for users.

The systemd journal includes several mechanisms to ensure the integrity and security of log data. It supports forward-secure sealing, which helps prevent tampering by sealing the log files at regular intervals with cryptographic keys that are then discarded. For a forensic investigator, this means that even if the system is compromised, earlier log entries cannot be modified without leaving traces of tampering.

The journalctl command

Journalctl is the primary command-line tool for interacting with the systemd journal. It provides a powerful querying language to filter log entries by various criteria such as

service, priority, or time range. Using journalctl without any arguments will display the entire journal, starting with the oldest entry.

To view the live system journal in UTC, one can use the following command:

To view the journal in the local timezone, simply run journalctl without the flag:

For forensic analysis and/or incident response, it is often necessary to view journal files collected from other systems. This can be done by pointing journalctl to the directory containing the external journal files:

If the external journal files are from a system in a different timezone, an investigator might want to view them in UTC to standardize the times across different systems:

One of the powerful features of journalctl for DFIR investigations is the ability to filter logs by time range, which can be crucial when trying to pinpoint events around a specific incident:

You can also combine time filters with other filters such as a specific unit or priority to narrow down the results further:

For forensic purposes, ensuring the authenticity of log entries is critical. Systemd journal's persistent storage capability can be coupled with the verification feature, which uses cryptographic signatures to confirm that log files have not been tampered with. This can be done using the flag:

Forensic investigators can also use the flag to get the logs in JSON format, which might be easier to parse programmatically:

This format includes all metadata, making it possible to perform detailed analysis using external tools.

Output formats

Below are some of the output formats supported by :

1. **Short (default)**: This is the default format. It's a human-readable format that is compact and omits the hostname and timestamp for brevity.

2. **Short-iso**: This format provides a more granular timestamp in ISO 8601 format including the date and time.

3. **Short-precise**: Similar to , but with even more precise timestamps including microseconds.

4. **Short-monotonic**: Displays the time passed since the system was booted up in a format.

5. **Verbose**: Shows the complete journal entry with all available fields and their values for the most detailed information.

6. **Exported**: Outputs the journal entries in a binary format suitable for backups and transfers.

7. **JSON**: Outputs the journal entries as newline-separated JSON objects, which is particularly useful for processing with script languages.

8. **JSON-pretty**: Similar to the JSON format but pretty-printed with indentation and newlines, which is more human-readable.

9. **JSON-Seq**: Outputs the journal entries as JSON Sequence, where each entry starts with ASCII Record Separator 0x1E.

10. **JSON-SSE**: Outputs journal entries formatted as Server-Sent Events (SSE).

11. **Cat**: Outputs only the message field of each journal entry, omitting all other fields for a very concise view.

These formats allow for flexibility in reviewing and processing log data. For instance, the JSON output can be easily consumed by programs for automated log analysis, whereas the short formats are often sufficient for a quick manual review of the logs. The verbose format is particularly helpful when detailed investigation is required, as it provides all available data associated with each log entry.

Summary

The systemd journal provides a robust and detailed logging system for modern Linux environments. Its structured approach to capturing and storing log data, along with the comprehensive metadata it includes, makes it an invaluable tool for systems administrators and forensic investigators alike. The command is versatile, providing a variety of ways to query and view the log data which is crucial for analysing system behaviour and investigating incidents.

About Halkyn Consulting

Halkyn Consulting Ltd is a UK-based security and risk management consultancy providing 24/7 incident response, digital forensics, threat hunting, virtual security leadership (vCISO) and security compliance support to organisations worldwide. We deliver clear, practical, vendor-independent advice based on real-world threats — no hype, no upsell.

More free security resources are available at www.halkynconsulting.co.uk/security-resources.

Web: www.halkynconsulting.co.uk | **Email:** info@halkynconsulting.co.uk | **Tel:** +44 1244 940858