Linux Incident Response - A Guide to syslog-ng

Taz Wake | Halkyn Consulting Ltd | Originally published 2023-11-20

Understanding Syslog-ng in Linux Environments

Syslog-ng stands as a sophisticated evolution of the syslog protocol, designed to offer advanced logging capabilities within Linux systems. Its enhanced functionalities are crucial in managing the complex log data prevalent in modern IT infrastructures.

Core Operations of Syslog-ng

The primary role of Syslog-ng is to collect, process, and forward log messages from diverse sources. Utilising Linux syscalls such as , , , and , it efficiently manages file operations and network communications, making it a versatile tool for log data management.

File Writing and Data Management

Syslog-ng excels in writing logs to various file formats, including text, binary, and structured formats like JSON. Logs are typically stored in directories like or , containing detailed information such as timestamps, hostnames, program identifiers, and the log messages themselves. This wealth of data is pivotal for a comprehensive understanding of system activities.

Syslog-ng and the Systemd Journal

Interfacing seamlessly with the Systemd Journal, Syslog-ng can access logs centralised in this journaling system used by many Linux distributions. While it doesn't write directly to the journal, Syslog-ng can effectively reroute these entries, integrating them with other log sources for in-depth analysis.

Configurational Flexibility of Syslog-ng

The configuration possibilities in Syslog-ng are extensive, offering granular control over log management. It allows for defining sources, applying filters based on content or metadata, and choosing from various output destinations. This configurational depth is key to customising log management to suit specific organisational needs.

Comparison with Rsyslog

In the realm of log management tools, Syslog-ng and Rsyslog both stand out, each with distinct advantages. Syslog-ng is particularly noted for its ease of configuration, especially when it comes to forwarding log data to remote servers. Its user-friendly setup and powerful filtering capabilities make it a preferred choice for scenarios where straightforward and customisable log management is crucial. This ease of configuration can significantly reduce the time and complexity involved in setting up remote log

forwarding, making Syslog-ng an attractive option for environments where quick deployment and ease of use are priorities.

While Rsyslog is celebrated for its high performance and ability to handle high volumes of log data efficiently, Syslog-ng often becomes the go-to for its more intuitive setup. For those seeking a balance between functionality and simplicity, particularly in scenarios involving the forwarding of logs to remote servers, Syslog-ng often emerges as the preferred choice. This preference is further reinforced when the specific filtering needs, or the requirement for an easy-to-navigate configuration, outweighs the high-volume processing capabilities offered by Rsyslog.

Integration with SIEM Systems

Syslog-ng, as a versatile log management solution, plays an integral role in strengthening security infrastructures. It achieves this by efficiently forwarding log data to Security Information and Event Management (SIEM) systems and centralised log collectors. This functionality is fundamental for the real-time monitoring and alerting capabilities crucial in modern security operations centres (SOCs).

The software supports a range of transmission protocols to cater to different security and operational needs. For instance, it can transmit logs over TCP (Transmission Control Protocol), offering a reliable, connection-oriented communication. This ensures that log data is not only sent but also acknowledged, making it suitable for environments where loss of log data is unacceptable. UDP (User Datagram Protocol) is also supported, which, while less reliable than TCP, offers faster transmission, beneficial in high-volume log environments where speed is a priority. Additionally, Syslog-ng can secure log data in transit using SSL/TLS (Secure Sockets Layer/Transport Layer Security), ensuring confidentiality and integrity, which is critical in protecting sensitive log information.

The message format in Syslog-ng is another key aspect. It adheres to standard syslog formats, typically comprising a priority value, a timestamp, the hostname or IP address, the application or process name, and the actual log message. This structured format is pivotal for SIEM systems and log collectors, as it aids in the accurate parsing, categorisation, and analysis of log data. Syslog-ng can be configured to include additional metadata or use custom formatting if required by specific SIEM systems or logging policies. The flexibility in configuring message formats and the support for secure and reliable transmission protocols make Syslog-ng a critical component in the architecture of log management and security event monitoring systems.

Understanding Severity and Facility Codes

In compliance with the syslog protocol, Syslog-ng employs a dual coding system comprising severity and facility codes to efficiently categorise and manage log messages. This system is particularly beneficial for incident responders, as it allows for the prioritisation and rapid identification of logs based on their nature and source.

Severity codes in Syslog-ng range from 'Emergency' to 'Debug', offering a granular view of the urgency and nature of each log entry. For instance, a severity level of

'Emergency' (code 0) indicates a system-wide critical condition, whereas 'Debug' (code 7) represents detailed developmental messages that are typically used during troubleshooting or debugging processes. Understanding these severity levels enables incident responders to quickly assess the criticality of events and allocate resources accordingly.

The severity codes are as follows:

- Code 0: Emergency - System is unusable.
- Code 1: Alert - Immediate action needed.
- Code 2: Critical - Critical conditions.
- Code 3: Error - Error conditions.
- Code 4: Warning - Warning conditions.
- Code 5: Notice - Normal but significant condition.
- Code 6: Informational - Informational messages.
- Code 7: Debug - Debug-level messages.

Facility codes, on the other hand, indicate the system or application that generated the log. For example, 'kern' (code 0) is used for kernel messages, while 'mail' (code 2) pertains to the mail system. This categorisation aids incident responders in quickly pinpointing the source of an issue, allowing for more efficient problem-solving and analysis.

The facility codes include:

- Code 0: kern - Kernel messages.
- Code 1: user - User-level messages.
- Code 2: mail - Mail system.
- Code 3: daemon - System daemons.
- Code 4: auth - Security/authentication messages.
- Code 5: syslog - Messages generated internally by syslogd.
- Code 6: lpr - Line printer subsystem.
- Code 7: news - Network news subsystem.
- Code 8: uucp - UUCP subsystem.
- Code 9: cron - Cron subsystem.
- Code 10: authpriv - Security/authentication messages.
- Code 11: ftp - FTP daemon.
- Code 12: ntp - NTP subsystem.
- Code 13: security - Log audit.
- Code 14: console - Log alert.
- Code 15: solaris-cron - Scheduling daemon.
- Codes 16–23: local0 – local7 - Locally used facilities.

For an incident responder, the comprehension of these codes is invaluable. They not only provide immediate insight into the nature and origin of a log entry but also assist in filtering and analysing log data effectively, making Syslog-ng a powerful tool in the arsenal of cybersecurity professionals.

Performance and Scalability

Syslog-ng is designed to handle large volumes of data efficiently, incorporating features like log buffering, flow control, and multi-threading. These features ensure that it remains effective even in demanding, high-volume environments.

Real-world Configuration Scenario

A practical configuration in Syslog-ng might involve collecting system logs, filtering for SSH-related messages, and storing them in a specific file. This setup can be invaluable for a Security Operations Centre (SOC) analyst focusing on potential security breaches or irregularities in SSH traffic.

Importance for Incident Responders

Syslog-ng is an indispensable asset for cybersecurity professionals, particularly in the realms of incident response and forensic investigations. Its ability to generate detailed logs is crucial in providing deep insights into various aspects of system operations, including but not limited to unauthorised access attempts, operational irregularities, and general system behaviour. These logs serve as a rich source of data for understanding the sequence of events leading up to, during, and after a security incident.

The logs generated by Syslog-ng are replete with critical information that can be instrumental in identifying and mitigating security threats. They record a comprehensive range of events, from system errors and service interruptions to suspicious activities and breach attempts. This granularity not only aids in pinpointing the exact nature and source of an issue but also provides a chronological trail of events, which is vital for understanding the scope and impact of a security incident.

For incident responders, the speed at which they can detect and respond to an issue is often as important as the response itself. Syslog-ng's structured and categorised logging, enhanced by severity and facility codes, allows for quick parsing and identification of critical issues. This immediacy in recognising potential threats enables responders to take swift action, potentially mitigating harmful effects before they escalate.

In terms of investigation, the logs from Syslog-ng can be found in various standard locations on a Linux system, typically in the directory. However, Syslog-ng also offers the flexibility to configure custom logging paths, which can be tailored to suit the specific needs of an organisation’s security infrastructure.

Analysing the data from Syslog-ng efficiently requires the use of specialised tools. Popular choices among cybersecurity professionals include log management and analysis

software like Splunk, LogRhythm, or Elasticsearch with Kibana. These tools not only facilitate the aggregation and indexing of log data for easier access but also provide advanced search capabilities, data visualisation, and alerting mechanisms. This enhances the ability of incident responders to swiftly sift through vast amounts of log data and extract actionable insights.

Moreover, Syslog-ng's compatibility with various SIEM (Security Information and Event Management) systems further bolsters its utility in cybersecurity contexts. By integrating Syslog-ng with a SIEM system, organisations can centralise their monitoring and analysis efforts, creating a more cohesive and effective security posture. This integration allows for real-time analysis of log data, automated alerting of suspicious activities, and aids in compliance with various regulatory standards that mandate the collection and analysis of log data.

Summary

Syslog-ng stands out as an essential log management tool in Linux environments. Its advanced functionalities, coupled with extensive configurational options and robust integration capabilities with SIEM systems, make it an indispensable asset in effective log management and cybersecurity operations.

If you want to know more about Linux Incident Response in general, as well as analysing the log files and being able to practice responding to a realistic Linux-based intrusion, have a look at FOR577 (*Linux Incident Response and Threat Hunting*) from the SANS Institute. You can find out more at http://sans.org/for577.

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