FORENSICS

syslog-ng Use Case

The Challenge

In today's IT environment, security events are question of when, not if. The challenge for IT security organizations is to react quickly to both internal and external threats. Whether a company has been hit with a Denial of Service (DoS) attack, had sensitive data stolen or has been the victim of fraud, log messages generated by network devices and applications are critical to determining the cause. Firewalls, intrusion prevention applications, routers, servers, VPNs, and numerous applications generate logs that document the workings of IT networks. During a forensic investigation, a comprehensive collection of log messages is required since it is not possible to know what data will be needed prior to a security event.

If an IT network has been compromised, IT security organizations need to detect the attack as quickly as possible to minimize damage. As organizations use web-applications more frequently, they are subject to more external attacks. Denial of Service attacks, viruses and other malware can disable critical web-applications with disastrous consequences for business. The first place system administrators look for clues of an attack are log messages from various network devices and applications. Reviewing log messages can be a time-consuming and costly exercise if logs are missing or not centrally located.

Not all security threats originate from external sources. Data leakage and theft by employees have become more prevalent as sensitive data such as confidential financial information and intellectual property are increasingly stored on company IT networks. Log messages are a powerful tool to monitor and record user access. When collected and stored properly, log messages can provide a finger print of user access and activity. In the event a company finds itself in legal proceedings, log messages can be used as evidence if they have been stored in a secure and tamper-proof format.

Key syslog-ng benefits for forensics

- Easy access to log messages via centralized log collection
- Faster search times with flexible message filtering, classification, and normalization
- Secure transport and storage of log messages to prevent tampering
- Log Data integrity ensured by Reliable Log Transfer Protocol (RLTP™) and disk-based buffering

The Solution

How does an organization ensure the integrity of log messages for forensic investigations? It implements a robust log management infrastructure. syslog-ng can simplify log collection, improving performance and and reliability.

Reliability

Secure Forwarding of Log Files (SSL/TLS)

syslog-ng Premium Edition enables forwarding of log files to distant servers. The log files from different servers can thus be gathered and stored centrally on dedicated log servers. The syslog-ng application is natively capable of handling SSL/TLS channels to secure the transfer of log messages. SSL also enables mutual client-server authentication with the help of X.509 certificates.

Secure Storage of Log Messages

syslog-ng Premium Edition can store log messages securely in encrypted, compressed, and timestamped binary files, so any sensitive data is available only for authorized personnel who have the appropriate encryption key to avoid data tampering and unauthorized access to sensitive data.

Disk-based Message Buffering

syslog-ng Premium Edition saves messages on the local disk if the central log server or the network connection becomes unavailable. When the connection goes back up, syslog-ng automatically sends the messages to the server in the original order. The content of the buffer is not lost even if the syslog-ng application needs to be restarted.

Application-level Acknowledgement

syslog-ng Premium Edition 4 F2 supports the Reliable Log Transfer Protocol (RLTP™) that allows the logserver to notify the clients when a message is received. The client deletes a message from its buffers when the logserver has received it. The client also keeps track of the messages the server has acknowledged as received, and sends only the unacknowledged messages after a network outage or other incident, thus avoiding message duplication.

Performance

Centralized Log Collection

Centralized log management is essential to quickly react to internal and external threats. The log messages from numerous network devices such as servers, routers, and firewalls and a wide variety of applications ranging from Intrusion Detection solutions to server OS software need to be collected and stored so that log analysis tools can transform potentially millions of log messages into actionable information about network operation and security. The syslog-ng Premium Edition application supports over 40 platforms including a wide variety of Linux, UNIX, HP, IBM, Microsoft Windows, and Solaris variations.

Log Classification and Filtering

Depending on the configuration, syslog-ng can receive more than 650,000 log messages per second. Moreover, syslog-ng can manage and classify log messages so that sophisticated data analysis tools only process logs relevant to security events, improving query times.

About BalaBit

BalaBit IT Security is an innovative information security company, one of the global leaders in developing privileged activity monitoring, trusted logging and proxy-based gateway technologies to help customers be protected against insider and outsider threats and meet security and compliance regulations. BalaBit, the second fastest-growing IT Security company in the Central European region concerning Deloitte Technology Fast 50 list, has local offices in France, Germany, Italy, Russia, and in the USA, and cooperates with partners worldwide. Its R&D and global support centers are located in Hungary, Europe.

More information: www.balabit.com

Learn More

- Read more about BalaBit syslog-ng products
- Request evaluation version
- Request callback