REGULATORY COMPLIANCE

LOG MANAGEMENT

The Challenge

IT departments increasingly find themselves spending ever more resources on compliance as laws, regulations and industry standards mandate increasing security awareness and the protection of sensitive data. Depending on the type of organization and its location, several data protection and security regulations may apply. Passing internal and external audits is crucial to continuing business operations.

Data protection and security regulations vary by geography and industry and can be difficult to understand. Some requirements such as the Payment Card Industry Data Security Standard (PCI-DSS) contain specific data handling and auditing requirements while others like the Sarbanes-Oxley Act (SOX) require general control procedures.

Many organizations use frameworks such as ISO27002 and COBIT to satisfy audit requirements. Enterprises both large and small in a wide variety of industries need to comply with regulations. The challenge for IT managers is to meet the numerous regulatory requirements in the most cost effective way possible.

Key syslog-ng benefits for regulatory compliance

- Centralized collection of log messages from a wide variety of devices and applications
- Secure transport of log messages via secure, encrypted SSL/TLS channels
- Encrypted, timestamped log storage to prevent tampering
- Zero message loss ensured by Reliable Log Transfer Protocol (RLTP™), Reliable Disk-based Buffering, and adaptive message rate control
- Flexible message filtering and sorting

The Solution

In response to these regulations, companies have to increase the control over of their business processes. From an IT departments perspective log messages from servers, network devices, and applications are a critical tool in complying with the numerous regulations. Log messages provide important information about the events of the network, the devices, and the applications running on these devices. Log messages can be used to detect security incidents, operational problems, and other issues like policy violations, and are useful in auditing and forensics situations. Collecting and analyzing log messages is also required directly or indirectly by several regulations, including SOX, the Basel II Accord, the Health Insurance and Portability Act (HIPAA), and PCI-DSS.

Implementing a robust log management infrastructure not only facilitates compliance with regulations but also adds business value. Not only does a centralized, secure log management infrastructure provide system administrators with the data to document network configuration changes and detect security events quickly but the massive amount of log messages generated by IT network devices and applications can be transformed into valuable business intelligence.

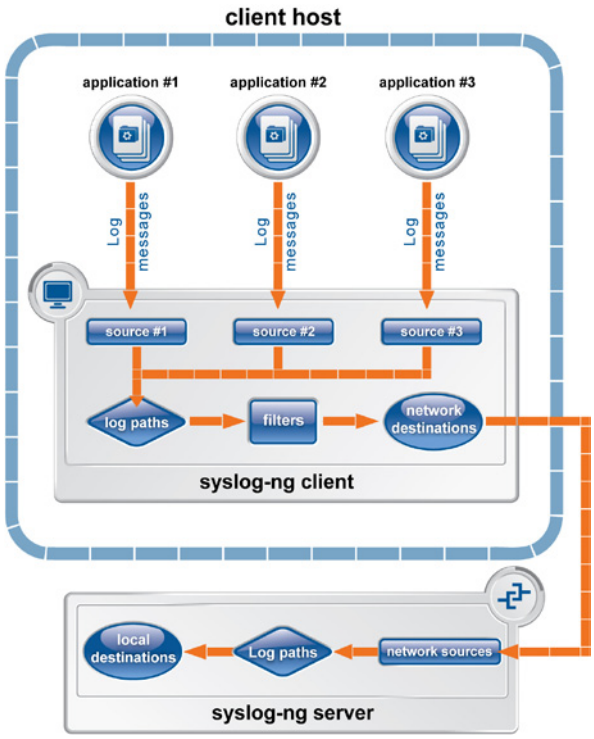

Figure 1. The route of a log message

The syslog-ng application is a tool that collects log messages from clients to a central log server, ensuring the secure transmission and storage of log messages from a wide variety of devices and applications. The syslog-ng Premium Edition application supports over 40 platforms including a wide variety of Linux, UNIX, HP, IBM, Microsoft Windows, and Solaris variations.

Many regulations call for sensitive information to be transported via encrypted channels. Log messages may contain sensitive information that should not be accessed by third parties. Therefore, syslog-ng uses the Transport Layer Security (TLS) protocol to encrypt the communication. TLS also allows the mutual authentication of the host and the server using X.509 certificates.

Preserving the integrity of audit trails in the event of forensic investigations is also essential to meeting many data protection regulations. Log messages must be protected even after they arrive to the log server to prevent manipulation and unauthorized access. For this reason, syslog-ng Premium Edition can store log messages in encrypted and digitally signed log files. Encrypting the log files ensures that log messages can be accessed only by authorized personnel who have the appropriate decryption key; while the digital signature prevents the unnoticed modification of the messages and store them on the central log server in an encrypted, digitally signed format. Timestamps for the stored data can be requested also from an external Timestamping Authority (TSA).

About BalaBit

BalaBit IT Security is an innovative information security company, a global leader in development of privileged activity monitoring, trusted logging and proxy-based gateway technologies to help protect customers against internal and external threats and meet security and compliance regulations. As an active member of the open source community, we provide solutions to a uniquely wide range of both open source and proprietary platforms, even for the most complex and heterogeneous IT systems across physical, virtual and cloud environments.

BalaBit is also known as “the syslog-ng company”, based on the company’s flagship product, the open source log server application, which is used by more than 650 000 companies worldwide and became the globally acknowledged de-facto industry standard.

BalaBit, the second fastest-growing IT Security company in the Central European region according to Deloitte Technology Fast 50 (2010) list, has local offices in France, Germany, Italy, Russia, and in the USA, and cooperates with partners worldwide. Our R&D and global support centers are located in Hungary, Europe.

More information: www.balabit.com

Learn More

To learn more about how syslog-ng Premium Edition can help your organization with specific compliance requirements, please download our white paper, Regulatory Compliance and System Logging.

- Regulatory Compliance and System Logging
- For more information about syslog-ng
- Request a call back