End-Point

LOG MANAGEMENT

The Challenge

Log collection and management is usually focused on servers, network devices and security appliances but some organizations are taking their log management to another level. More and more, the laptops and desktops of employees are being monitored for security threats. In these situations, IT security professionals are collecting log messages from desktops and laptops and transferring them to Security Information and Event Management (SIEM) systems or other analytic systems to detect and prevent security threats.

Deploying a robust log management solution on end-points can be challenging. Client OSs and host-based Intrusion Detection Systems (IDS) can generate a wide variety of log messages, many not related to security threats. The solution needs to be secure and reliable and, at the same time, be lightweight so as to be transparent to end users. Monitoring remote end-points introduces more complexity to log management as remote connections can be unreliable, lack bandwidth and are often insecure. Most log collection tools and agents shipped with SIEMs lack the ability to ensure the confidentiality and integrity of the messages while they're transferred to the central log server which is especially important if clients connect over the public Internet and do not handle the regular disruptions in network connectivity well which often happens on mobile clients. Moreover, most collection tools only support a narrow range of OS platforms and cannot be deployed as a comprehensive solution in complex IT environments.

The Solution

Scalability

syslog-ng can meet the requirements of this challenging configuration. With support for more than fifty OS platforms including traditional server and desktop platforms as well, syslog-ng can be deployed as a single log management solution even on end-points. Depending on the exact configuration, syslog-ng can manage more than 650,000 log messages per second and one syslog-ng server can manage the logs from several thousand log sources. This scalability enables syslog-ng to meet the challenges of the largest, most complex networks. To optimize network capacity, particular for remote end-points, syslog-ng offers advanced filtering and classification features. It can filter out irrelevant messages and classify important data reducing the data load on both the network and the SIEM.

Reliability

To ensure reliability, syslog-ng Premium Edition combines several unique features to ensure zero messages are lost. First, syslog-ng supports reliability by transferring log messages via TCP as its transport protocol. It also uses Reliable Log Transfer Protocol (RLTP™), an application level acknowledgement protocol to ensure that messages from the syslog-ng client have been received by the server. Should the central log server become unavailable, client-side failover ensures messages can be sent to alternate destinations and local disk buffering ensures that messages are written to a local disk until they can be safely transferred to the central server.

Security

In situations where laptops are outside of the company network, syslog-ng can securely forward event logs to the central SIEM by TLS-based mutual authentication, eliminating the need to set up a VPN connection just for that purpose. By placing a syslog-ng server in a DMZ, configuring TLS-based authentication, opening a port on the firewall and configuring syslog-ng clients on the laptops to send their messages there, network administrators can catch problems (viruses, malware infections etc.) by analyzing the event logs from the end users' computers even before they enter the company's network.

About BalaBit

BalaBit IT Security is an innovative information security company, a global leader in the 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 logging company", based on the company's flagship product, the open source log server application, which is used by more than 850 000 companies worldwide and became the globally acknowledged de-facto industry standard.

BalaBit, the fastest-growing IT Security company in the Central European region according to Deloitte Technology Fast 50 (2012) 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

- BalaBit syslog-ng products
- Request evaluation version
- Request a callback