BalaBit IT Security

CUSTOMER REFERENCE: MAGYAR TELEKOM

SCALABLE LOG MANAGEMENT WITH SYSLOG-NG

"COLLECTING AND CENTRALIZING HUGE AMOUNTS OF LOGS WOULD BE IMPOSSIBLE FOR US WITHOUT SYSLOG-NG'S UNIQUE CAPABILITIES.

WITH THE HELP OF BALABIT'S PROFESSIONAL SERVICES, WE WERE ABLE TO DEPLOY A HIGHLY RELIABLE AND SECURE LOG INFRASTRUCTURE TO HANDLE BILLIONS OF LOG MESSAGES."

Krisztian Hary IT security Officer, Magyar Telekom.

Magyar Telekom, part of the Deutsche Telekom Group, offers fixed-line and mobile communications, internet and IPTV services, and IT services under the T-Home, T-Mobile and T-Systems brands. With revenues exceeding $2 billion and more than 11,000 employees, Magyar Telekom is Hungary's largest ICT provider.

Magyar Telekom

THE CHALLENGE

As a communications and internet service provider, Magyar Telekom handles large amounts of personal data. To comply with European Union and national government data-protection regulations and secure its customers' personal data, the Magyar Telekom IT Security policy requires that log messages from all systems handling personal data must be collected and sent to a Security Information and Event Management (SIEM) tool for analysis. Customer data handling systems consist of a wide variety of server operating systems, applications, databases, and middleware.

Due to its large and complex IT environment, Magyar Telekom needed an efficient solution to consolidate many islands of log collection into a single, centralized log management solution. In total, the security team needed to collect, centralize and manage logs from more than 10,000 sources at a rate of approximately 30,000 messages per second. If making sense of more than 2 billion messages per day wasn't difficult enough, the log messages needed to be reliably and securely transferred and stored so that the integrity of the log data feeding the SIEM was preserved.

Not only did the amount of logs pose a problem, but the variety of sources and variation of log structure made collection and centralization difficult. The IT Security team needed to access logs from a variety of server operating systems, security devices, standard and custom applications, as well as several types of databases.

THE SOLUTION

Having had a positive experience using the syslog-ng Open Source Edition, Magyar Telekom turned to BalaBit IT Security to help them design and implement a highly reliable centralized log management solution. syslog-ng Premium Edition provided the IT security team with a solution to filter and structure logs on remote hosts before transferring them to the central log server. To avoid large bursts of log data, Magyar Telekom uses syslog-ng to push log messages in near real-time rather than pulling logs from a central server. This also eliminates the need to access log source hosts remotely.

Due to the sensitive nature of consumer data, Magyar Telekom needed to ensure logs were not lost during collection and transfer to the central server. To ensure reliable transfer, syslog-ng Premium Edition stores messages locally on log source hosts should the network connection or the log destination become unavailable. With the Reliable Log Transfer Protocol (RLTP™), an application level transport protocol, syslog-ng detects the last received message on the receiving end and then starts resending messages from that point, ensuring messages are not duplicated at the receiving end in case of a connection break.

To manage log data traffic centrally, syslog-ng clients transfer log messages to a load-balancing Cisco ACE router with a single IP address. Behind the load-balancer, Magyar Telekom deployed syslog-ng Premium Edition as a central log server in a cluster configuration to provide N+1 redundancy. With syslog-ng as their centralized log management solution, Magyar Telekom was able to consolidate islands of log collection into a scalable, reliable log management tool enabling analysis tools to focus on a smaller, more reliable set of log data.

- Read more about syslog-ng
- Requestion an evaluation
- Request a callback

ABOUT BALABIT

BalaBit IT Security is an innovative information security company, a global leader in the development of privileged activity monitoring and log management to help protect customers against internal and external threats and meet security and compliance regulations. BalaBit is known for its open source log management application, syslog-ng, which has more than 1 million users worldwide.

www.balabit.com