CASE STUDY

Secure Log Management with syslog-ng™

syslog-ng™ Premium Edition

Located in Victoria, British Columbia, the province's capital and one of the most beautiful cities in the world, The University of Victoria, one of Canada's leading universities, provides both students and faculty with a unique learning environment. UVic has earned a reputation for commitment to research, scholarship and co-op education and is home to almost 20,000 students and over 5,000 faculty and staff.

Learn more

- Read more about syslog-ng™
- Request an evaluation
- Request pricing

The Challenge

To lower total cost of ownership for system monitoring and reduce response times to incidents, the UVic IT department set out to establish a central log collection system to feed an alerting and monitoring system for its large, diverse IT environment serving more than 20,000 users. University IT administrators needed to centralize log collection for over 700 unix and windows machines as well as more than 1,500 network devices. Prior to deploying syslog-ng™, the University used native OS vendor tools such as syslogd and Windows Eventlog to collect logs but syslogd did not provide reliable log transmission, nor could it filter log messages using arbitrary message patterns. Windows Eventlog did not consolidate logs into a common repository. With log sources that ranged from traditional syslog and Windows eventlogs to unique program output and log files, finding one tool with the ability to collect and filter the various messages in real time was a priority.

"SYSLOG-NG™ LEADS THE PACK WITH ITS FEATURES AND PERFORMANCE, BUT THAT ALONE DOES NOT MAKE IT READY FOR THE ENTERPRISE. THE FAST RESPONSE AND IN DEPTH KNOWLEDGE OF THE ONE IDENTITY SUPPORT TEAM MAKE SYSLOG-NG™ AN EASY CHOICE."

- Evan Rempel senior system administrator

The Solution

After having reviewed several competitors on both the client and server sides, the university decided to choose syslog-ng™ Premium Edition as its central log management tool.

Not only did syslog-ng™ enable classification of messages in real time with its PatternDB™, but was able to scale to the log message rate generated by the university's large and growing network. By comparing log messages to known patterns, syslog-ng's PatternDB™ is able to identify the exact type of the messages, and sort them into message classes. The message classes can be used to classify the type of the event described in the log message. The message classes can be customized, and for example can label the messages as user login, application crash, file transfer, etc. events. In addition to classifying messages, it is also possible to add different tags which can be used later for filtering messages, for example, to collect messages tagged as user_login to a separate file or to perform conditional post processing on the tagged messages. This exclusive feature of syslog-ng™ offers the UVic system administrators the ability to identify incidents as they occur.

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats. Learn more at OneIdentity.com