Application Note AN2009-48

Remote Syslog for Auditing and Logging Requirements

Huba Leidenfrost

INTRODUCTION

This application note provides a process on forwarding a copy of Windows® event log data from the SEL tough computer with Windows 7 to a central location using the IETF RFC 3164 syslog format. A System Computing Platform running Microsoft® Windows has event data that may be used to meet regulatory compliance with NERC CIP-007-1 R5.1.2 and similar regulations requiring records of accurate time stamped user account access activity.

PROBLEM

SEL tough computer installations have essential audit log data stored in a proprietary Windows event log format. These data are not readily available to a central monitoring and reporting facility. Manual log review on individual silo data does not provide for timely review or automation of log analysis to generate security events. Getting a timely copy of this data back to a central location can be a challenge.

SEL SOLUTION

Configure an SEL tough computer to forward Windows event log data to a centralized location using the syslog format (see Figure 1). Each time there is an auditable event on the SEL tough computer in Windows event log format, the event is simultaneously sent over the network via the nonproprietary syslog format (space delimited ASCII) to your centralized logging facility. To ensure accurate time stamps on log data, connect an SEL-2407® Satellite-Synchronized Clock to your SEL tough computer. Forwarding logs to a central location for analysis provides a building block toward auditable compliance with NERC CIP and similar regulations.

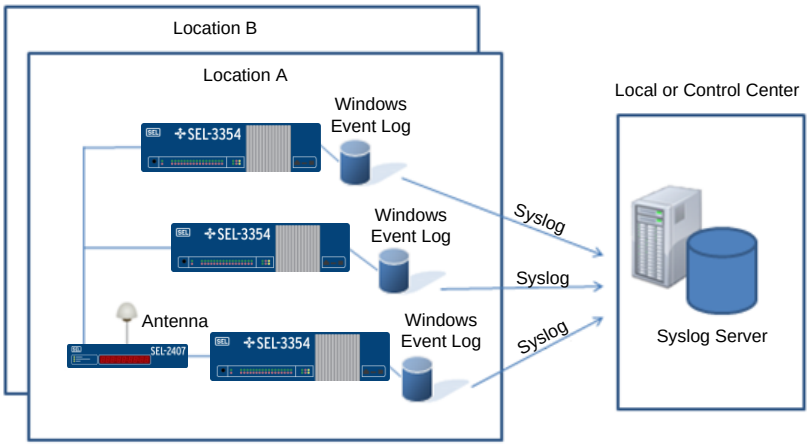

Figure 1 Sending SEL Tough Computer Windows Event Log Data to a Syslog Server

Process to Add Syslog Forwarding Capability to the SEL Tough Computer

Step 1. Select and install a syslog forwarding program on the SEL tough computer (see Table 1 for suggestions).

Step 2. Configure the syslog forwarding program to send Windows event log data to the remote syslog server.

Step 3. Test the configuration to ensure a copy of all the types of Windows event log data you wish to receive for audit purposes shows at the remote syslog server. Use the Windows Group Policy MMC (Microsoft Management Console) snap-in to configure the types of events to be logged or audited.

Table 1 Useful Third-Party Syslog Forwarding Tools for Windows

Tool	Description
Snare agent for Windows	Forwards both standard Windows event logs and custom Windows event logs; provides assistance configuring Windows security audit policy
NTsyslog	Forwards all system, security, and application event logs to a syslog server
Kiwi syslog server	Forwards Windows event logs and more to a syslog server
Kiwi syslog message generator	Automates sending test messages to your syslog server

Now every time an auditable event is logged at the SEL tough computer, a copy of the event also shows at the central log server. The compliance department can then automate actions to retain log data, correlate related log data, and alert administrators of interesting log events according to security policies.

LAN2009-48

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Tel: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com