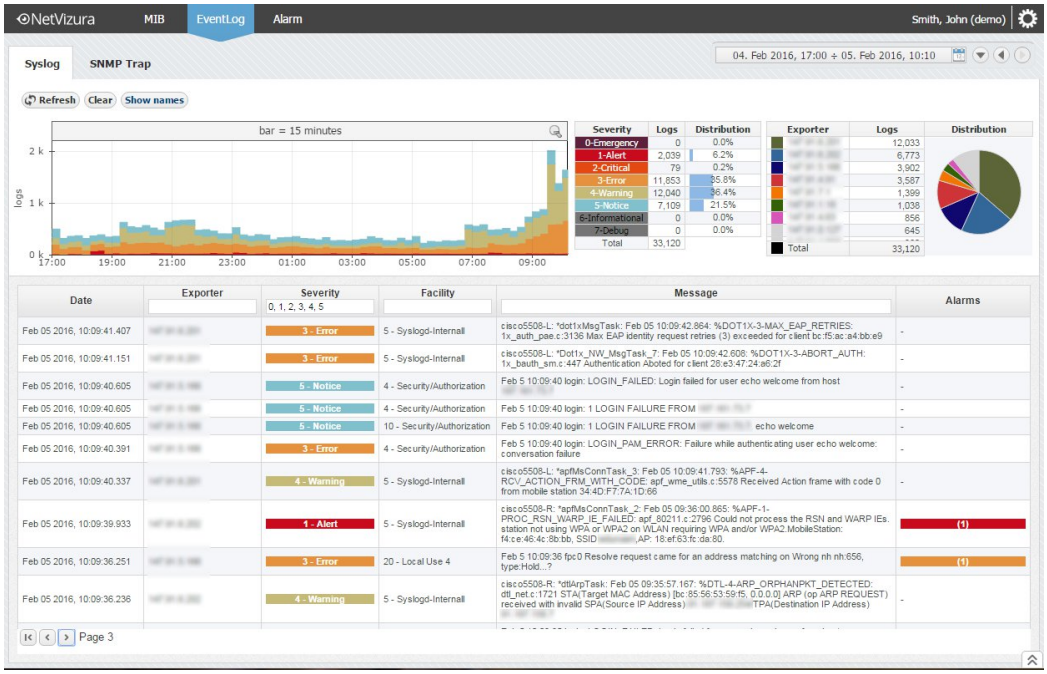
EventLog Analyzer

DATASHEET



NetVizura EventLog Analyzer enables you to collect, store and analyze logs from your network devices. It supports Syslog and SNMP Trap messages exported by most network devices. Log severity level and source device distribution are visualized for all data (including search results) in the selected time window from several mili-seconds to several years.This helps you to identify security incidents, policy violations, and operational issues and shortens the time needed to analyze, contain and counter them.

Key Features

- Central location for log collection, analysis and archive
- Highlights log severity levels, devices and alarms
- Quick search by time window, device IP, message text, severity level etc.

- Automatic database maintenance
- Supports Syslog and SNMP traps from existing devices
- Available for Windows and Linux servers

Feature Highlights

Centralized Log Management

Syslog and SNMP Trap Support

EventLog Analyzer supports Syslog and SNMP trap message collecting and archiving.

Millions of Logs per Hour

Built and tested for more than 50,000 logs per second (millions of logs per hour).

Alarms

Alarms based on Syslog message and SNMP trap message characteristics: source IP, facility, severity and message text. All alarms are accessed from Alarm dashboard allowing quick jumps to objects that triggered the alarm.

Quick and Easy Log Search

Visualization

Log severity levels and device contribution are highlighted on two charts. Color mapping of severity level makes identifying critical logs and their numbers quick.

Quick Filters and Search

One click filters and quick log search available by device IP, log severity, time stamp or log message text.

Great Configuration Abilities

Log Filtering

Filter unnecessary logs from processing by creating filters based on source IP, message facility, severity or containing text for Syslog messages and source IP, Trap OID and Variable values for SNMP trap messages.

Automated Database Management

All collected logs are stored in the database. You can set the maximum database size and conditions for automatic deletion of oldest data.

System Reqirements

HARDWARE	RECOMMENDED REQUIREMENTS
CPU	Quad Core 3.0GHz
Memory	2 GB
HDD Space	12 TB - SAS or SSD in RAID 0 or similar set-up with striping
SOFTWARE	**REQUIREMENTS**
OS	**Server**: CentOS 6 (64 bit), CentOS 7 (64 bit), Debian Wheezy 7 (64 bit), Debian Jessie 8 (64 bit) Ubuntu Trusty Tahr 14.04 LTS (64-bit), Ubuntu Xenial Xerus 16.04 LTS (64-bit) Windows Server 2008 (64-bit), Windows Server 2012 (64-bit), Windows Server 2016 (64-bit) **Workstation:** any OS supporting recommended web browsers
Database	PostgreSQL 9.2+ (free) Detailed installation and repository links provided in the installation guide
Web Browser	Chrome 35.0+, Firefox 26.0+, Internet Explorer 11
Other	Oracle Java 8, Apache Tomcat 6,7 and 8 (free)
INTEGRATION WITH OTHER NETVIZURA PRODUCTS	
Deployment	Stand-alone product, no additional products required
Other Products	Other products are enabled via license key. Certain EventLog Analyzer features enhance other products.

NOTE: The recommended server requirements assume default configuration: 5,000 messages/s, 5 active alarms and 30 days of logs in the database.

Significantly increasing the number of Syslogs and SNMP traps processed and adding alarms can increase CPU and memory requirements. Significantly increasing the number of messages will increase EventLog database size and require more HDD space.

For more examples and up-to-date system requirements, please visit our online guide.

About Soneco

Soneco is a company based in Serbia, that specializes in software development and ICT consulting. Since 2006, we have been growing steadily and our solutions have left a significant mark on some of the core ICT transformations in the region, earning us a wider recognition as a reliable partner and software developer of consistent quality. We have been Cisco Solutions Partners since 2011 and Oracle Gold Partner since 2010.

Soneco continues to focus on client satisfaction and building strong relationships with partners. Our best reference is the number of successfully delivered projects implemented in various industry verticals and a strong reference list consisting of recognizable clients.

Soneco d.o.o.
Makenzijeva 24/VI, 11000 Belgrade, Serbia
Phone: +381116356319
Email: info@soneco.rs

For additional information, please contact us at sales@netvizura.com or visit www.netvizura.com