NXLog

PROVIDING YOU
LOG COLLECTION SOLUTIONS
TO BUILD A SECURE, FLEXIBLE AND RELIABLE
LOG INFRASTRUCTURE

NXLOG
ENTERPRISE EDITION

Fast, reliable and efficient

Avoid vendor lock-in

Superior OS support

Fast, reliable and efficient

Avoid vendor lock-in

Superior OS support

The ideal tool to collect and centralize log data

NXLog ENTERPRISE EDITION

Collect Windows Eventlog

Simple and powerful configuration syntax

Monitor agent health and statistics

Secure and reliable collection

DO YOU NEED TO COLLECT LOG DATA OF YOUR EVENTS?

NXLOG ENTERPRISE EDITION IS HERE TO HELP YOU OUT!

Today's IT infrastructure can be very demanding in terms of event logs. Hundreds of different devices, applications, and appliances produce vast amounts of event log messages. These events need to be filtered, classified, correlated, or other typical processing as they are handled in real time or forwarded and stored in a central location.

In most organizations these tasks are solved by connecting a dozen different scripts and programs which all have their custom format and configuration.

NXLog is a high-performance multi-platform log collection solution aimed at solving these tasks and doing it ALL IN ONE PLACE!

KEY FEATURES:

Integrate with any SIEM
The NXLog EE works with a wide range of SIEM and log analytics products and services. Avoid vendor lock-in. Ability to feed multiple systems.

Superior OS support
- Windows, Linux, Solaris, AIX, FreeBSD, OpenBSD, macOS.
- The ability to collect audit logs natively on each supported platform in addition to OS logs and application logs.

Supports agent-less and agent-based log collection modes
Can be configured to act as a collector agent, log server or log relay and supports hybrid modes. The ideal tool to collect and centralize log data

Outstanding Windows log collection capabilities. The NXLog Enterprise Edition is the most advanced log collector on the market today for the Windows platform.

- Collect Windows Eventlog locally or remotely. Can act as a Windows Event Collector for both Linux and Windows to collect WEF remotely.
- Native Windows Event Tracing (ETW) log collection support.
- Powershell auditing.
- Microsoft Sharepoint log collection support.

- Collect Microsoft IIS logs.
- Microsoft Exchange.
- Windows DNS server log collection.
- Microsoft SQL server auditing.
- Windows Performance counters.

NXLOG ENTERPRISE EDITION

ADDITIONAL FEATURES:

Secure and reliable collection and transfer

- Signed installer packages.
- Message buffering.
- Reliable transfer with protocol level acknowledgment.
- Compression over the wire.
- Employs flow control to ensure disruptions do not cause data loss.
- Full TLS/SSL support for encrypted data transfer.

Remote management

- Managing a large number of log collectors across different platforms can be tough.
- Support SOAP/XMl and JSON REST API for remote management.
- Centralized monitoring and management through NXLog Manager.
- Firewall-friendly.
- Monitor agent health and statistics.

Extreme flexibility

- Agent side enrichment, filtering, pattern matching, message rewrite.
- Simple and powerful configuration syntax.
- Built-in log rotation.
- Read multiple log sources simultaneously.
- Support for different encodings.
- Send to more than one destination if needed.
- Event correlation.
- Use Perl or Python to easily embed custom parsers or integrate with other log sources

Fast, reliable and efficient

- No extra dependencies to rely on. It does not use Java runtime, python interpreter and runs as native code.
- Blazingly fast, scalable.
- Can handle thousands of connections.
- Lightweight with a low memory footprint of a few megabytes.

Supports a wide range of data formats and protocols

- CEF, LEEF, XML, JSON, CSV, KVP, W3C, Syslog, Checkpoint OPSEC, SDEE SNMP, NetFlow.
- Designed with structured data in mind. Most other log collectors are still Syslog based while NXLog embraces structured logging to alleviate the need for writing parsers.

File integrity monitoring

- Detect changes to files and directories on all supported platforms.
- Can also monitor the Windows registry for changes.

For more details please visit:

https://nxlog.co/products/nxlog-enterprise-edition#

NXLOG MANAGER

ARE YOU WONDERING HOW TO MANAGE AND MONITOR NXLOG EE AGENTS?
THEN NXLOG MANAGER IS THE RIGHT CHOICE FOR YOU!

NXLog Manager is a web based application that can be used from a browser and acts as a centralized management console making it possible to manage and monitor a large number of NXLog EE instances effortlessly. Remote management is accomplished over a secure trusted TLS connection with mutual certificate verification. It also comes with a built-in PKI system in order to make certificate and key management a breeze.

KEY FEATURES:

Can **remotely** manage and monitor **NXLog EE instances** using a centralized web based management console

The configuration wizard helps with setting up the log collection configuration without the need to edit text files

NXLog instances can be assigned to templates so that configuration changes can be applied in bulk

The Health of the NXLog instances is monitored and any errors in the log collection system are immediately visible

A built-in PKI system handles X509 certificates to be deployed automatically. All communication is encrypted for maximum security

Distributed mode allows multiple NXLog Managers to be connected when network topology or geographical separation would require this

Provides an Editor to create log extraction patterns to make sure your regular expression will work

For more details please visit: https://nxlog.co/products/nxlog-manager

OUR COMPANY CAN PROVIDE PROFESSIONAL SERVICES
TO HELP YOU BRING THE MOST OUT OF LOG MANAGEMENT

Technical support services

Our support team is available to assist with configuration issues, help with the deployment , and troubleshoot problems to ensure you are not left out in the cold.

Consultation

Log management is not easy to do right. Make sure to discuss your requirements with our experts.

Integration with third party products and services

We can help with the integration of new applications, appliances, SIEM products or other log sources within your log collection infrastructure.

Development services

We offer development services to implement custom modules and parsers for NXLog.

Training

If you are unfamiliar with the product and would like to learn the concepts and usage, feel free to reach out so that we can do a remote training session for your team.

Please contact us with inquiries about our professional services

Our company was established to develop IT security tools with log collection solutions being the primary focus. Using our products customers can build a secure, flexible and reliable log infrastructure which satisfies the highest IT requirements of any organization.

BE OUR PARTNER!

NXLog has become the log agent of choice for thousands of users collecting event data on Windows and Unix/Linux. Ranging from Fortune 500 corporations and large security vendors to small businesses, our customers and users have come to love NXLog technology.

We would love to hear from you if you are a systems integrator, a service provider, a reseller specialized in technology procurement and fulfillment or simply think that your customers would be interested in leveraging NXLog technology.

THESE CUSTOMERS TRUST NXLOG WITH THEIR LOG COLLECTION NEEDS

„I find that your product is very powerful and is one of the best choice for the implementation of a distributed log system in a heterogeneous network where multiple OS (Unix/ Linux and Windows) should be supported."

„While I have used both rsyslog and syslog-ng, I am now drawn towards nxlog as a more powerful tool. It does a lot natively in terms of log massaging and organization. Take a look at it when you have a chance."
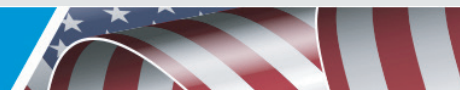
verizon✓   **Disney**   European Commission   **AMERICA'S NAVY**   **WESTERN UNION WU**

NXLog EUROPE

NXLog Ltd.

2315 Szigethalom, Süllő köz 3
Hungary

NXLog USA

NXLog Inc.

2035 Sunset Lake Road, Suite B-2,
Newark, DE 19702, USA

Contact us for more details at: info@nxlog.org or visit http://nxlog.org