NXLog

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

NXLOG ENTERPRISE EDITION

KEY FEATURES

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 with a single tool.

NXLog

Integrate with any SIEM

- The NXLog Enterprise Edition works with a wide range of SIEM and log analytics products.
- 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.

Agent-based & Agent-less 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

Supports a wide range of data formats and protocols

- CEF, LEEF, XML, JSON, CSV, KVP, W3C, Syslog, 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.

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

- 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.
- Passive network monitor module

NXLOG ENTERPRISE EDITION

ADDITIONAL FEATURES

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.
- Read and write compressed files.
- Batch processing
- Network packet capture support

File integrity monitoring

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

Remote management

- Support SOAP/XMl and JSON REST API for remote management.
- Centralized monitoring and management through NXLog Manager.
- Firewall-friendly.
- Monitor agent health and statistics.

macOS logging

- The most configurable and versatile logging solution for macOS.
- Apple System Log (ASL) log collection
- Basic Security Mode (BSM) auditing
- macOS events can be capture directly from the ULS logging facility
- Collection of macOS kernel logs
- Highly configurable log filtering and enrichment capabilities

Industrial Control Systems (ICS/SCADA) Support

- Protocol parser for BACNET
- Improved handling of complex data in MODBUS packets
- Protocol parser for PROFINET
- Shipping individually signed packages on Debian
- Collect logs from major ICS solutions (Schneider Electric Citect SCADA & Siemens SIMATIC PCS 7)

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.
- Failover support.
- Data at rest protection

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.
- ID resolution for better readability of log events

Learn more about NXLog Enterprise Edition:
https://nxlog.co/products/nxlog-enterprise-edition

NXLOG MANAGER

KEY FEATURES

REMOTELY MANAGE AND MONITOR YOUR NXLOG ENTERPRISE EDITION AGENTS

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 Enterprise Edition 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 to make a certificate and key management a breeze.

Deploy your configuration changes and monitor your agents remotely.

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

Learn more about NXLog Manager:
https://nxlog.co/products/nxlog-manager

04

NXLOG ADD-ONS

OPTIONAL MODULES

NXLog Azure & Office 365

Can retrieve information about various user, admin, system, and policy actions and events from Microsoft Azure and Office 365. Once configured, the add-on prints Syslog events, each with a JSON payload, to standard output for processing by NXLog.

NXLog Exchange

The nxlog-xchg add-on can be used to retrieve administrator audit logs and mailbox audit logs. These logs include actions taken by users or administrators who make changes in the organization.

NXLog Salesforce

The Salesforce add-on provides support for fetching Event Log Files from Salesforce with NXLog. The script collects Event Log Files from a Salesforce instance by periodically running SOQL queries via the REST API.

NXLog Box

The Box add-on can be used to pull events from Box using their REST API. Events will be passed to NXLog in Syslog format with the JSON event in the message field.

NXLog Okta

The Okta add-on can be used to pull events from Okta using their REST API. Events will be passed to NXLog in Syslog format with the JSON event in the message field.

NXLog Amazon S3

The NXLog Amazon S3 add-on can receive events and send events to Amazon S3 cloud storage. The NXLog Python modules for input and output are used for this, as well as Boto3, the AWS SDK for Python.

NXLog Cisco FireSIGHT & Cisco IPS

There are two add-ons available for Cisco applications. One is to collect events from the FireSIGHT system via the eStreamer API and a second add-on to collect alerts from a Cisco IPS-enabled device.

NXLog Google API

The NXLog Google API add-on can collect Google Cloud Platform logs and send logs to Google Pub/Sub Service.

Learn more about NXLog Add-Ons:
https://nxlog.co/products/nxlog-add-ons

Technical support services for NXLog Enterprise Edition

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.

PROFESSIONAL SERVICES

05

MAIN BENEFITS

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

NXLog 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.

Contact us to get the best-in-class log collection professional services.

Learn more about our Professional Services:
https://nxlog.co/services

06

BE OUR PARTNER!

NXLOG PARTNER PROGRAM

NXLog has become the log agent of choice for thousands of users collecting event data on heterogeneous sources. Ranging from Fortune 500 corporations and large security vendors to small businesses, our customers and users trust in NXLog.

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. See our technology ecosystem: **https://nxlog.co/technology-ecosystem**

These customers trust NXLog with their log collection needs

SAAB RICOH AIRBUS orange™ FINANSBANK verizon

"Since we work with so many different clients, we never know what request the client is going to throw at you and we want to know that we can support those requests no matter what they are, and with NXLog it's sort of like the swiss army knife of logging tools."

"I find that your product is very powerful and is one of the best choices 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 messaging and organization. Take a look at it when you have a chance."

NXLog Ltd. develops multi-platform log collection tools that support many different log sources, formats, transports, and integrations. The tools help administrators collect, parse, and forward logs so they can more easily respond to security issues, investigate operational problems, and analyze event data.

NXLog Europe

NXLog Ltd.
2315 Szigethalom, Süllő köz 3
Hungary

NXLog United States

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

SOLUTIONS

NXLog Enterprise Edition

NXLog Manager

NXLog Add-Ons

REQUEST A FREE TRIAL

*For more information on NXLog visit our **website**, checkout our **integrations' page** or **schedule a meeting** with one of our representatives.*