NXLog Platform Feature List

nxlog.co/platform/plans

AGENT PLATFORM SUPPORT	
Feature	**Description**
Microsoft Windows support	NXLog collects various logs from MS Windows, including DHCP, DNS, file integrity monitoring, Active Directory, Exchange, IIS, SQL Server, etc
GNU/Linux support	NXLog runs on various enterprise Linux distributions such as RHEL/CentOS, Debian/Ubuntu, and SLES
Apple macOS support	Run on Apple macOS operating system
Support for x86 64-bit processors	Run the agent on current Intel and AMD 64-bit hardware
Support for x86 32-bit processors	Run the agent on Intel and AMD 32-bit hardware
Support for ARM 32-bit processors	Run the agent on 32-bit ARM systems such as armv7
Support for ARM 64-bit processors	Run the agent on 64-bit ARM systems such as Apple M1 and M2 and others
Support for IBM Power 64-bit processors	Run the agent on 64-bit IBM Power systems
Support for Sparc 64-bit processors	Run the agent on 64-bit Oracle/Sun/Hitachi Sparc systems
FreeBSD support	Run the agent on FreeBSD, a modern BSD UNIX distribution
IBM AIX support	Run the agent on the IBM AIX operating system
Oracle Solaris support	Support of Unix-like Solaris OS made for Oracle DB and Java apps

CUSTOM INTEGRATION	
Feature	**Description**
Health check	Provides HTTP response capabilities for checking NXLog's health status
External programs extension	Call an external program such as a shell script or native executable to process logs
External programs output	Sends logs to the input of an external program, such as a shell script or native executable
External programs input	Collects the output of an external program, such as a shell script or native executable
Python extension	Enhance NXLog with custom Python script support, compatible with Python 3
Python output	This module for custom log transport methods to Python scripts
Python input	Custom Python script feeds logs to NXLog. Python module required. Compatible with Python 3
Perl extension	Module extends NXLog with Perl script support for log processing
Perl output	This module makes it possible to execute Perl code in an output module that can handle the data directly in Perl
Perl input	Module makes it possible to execute Perl code in an input module to capture and inject event data directly into NXLog
Ruby extension	Module enables log processing with Ruby methods, offering logging and event manipulation functionalities

Ruby output	Customize log transport in Ruby, compatible with Ruby 2
Ruby input	This module is compatible with Ruby version 2 and has not been tested with newer versions
Java extension	Process NXLog log data using Java classes and methods
Java output	Send logs to a custom Java application. The Java application must implement the NXLog Java class to receive log records
Java input	Feed logs to NXLog from custom Java apps. Configure path and JVM
Go extension	Provides support for processing NXLog log data with methods written in the Go language
Go output	Send logs to Go scripts. Specify path to shared library
Go input	Collect logs using custom Go methods. Feed logs to NXLog. Configuration needs path to Go dynamic library

DATA COLLECTION CAPABILITY

Feature	Description
Event Log for Windows 2008/Vista/later	Collects Windows Event Log messages locally from Windows Vista/2008 and later
Collect logs from files	Provides support for collecting logs from files
Write mark log messages	Periodically generates the specified message to provide agent heartbeat
Receive logs via HTTP and HTTPS	Accepts log messages via HTTP or HTTPS connections. Supports multiline and multipart batching
Collect operational logs from NXLog	Collects the internal logs of the NXLog agent directly
Collect from the kernel log buffer	Collects logs from the kernel log buffer on Linux, BSD, and macOS
Event Log for Windows XP/2000/2003	Module to collect Windows Event Log messages on Windows XP, 2000, 2003
Collect logs from named pipes	Collects log messages from a named pipe on UNIX-like operating systems
Systemd input	Collects system logs from the systemd journal on Linux systems
TCP input	Receives data over the network using plain TCP connections
Test generator	Generate simple events for testing, with an incremented integer up to the number of events specified
TLS/SSL input	Receives logs over the network using TLS/SSL-secured connections
Collect logs from Unix Domain Sockets	Collects logs over UNIX Domain Sockets (UDS) like /dev/log
WTMP	Parses wtmp and btmp logs on UNIX and Linux systems
Receive logs via UDP	Provides support to receive logs via the UDP protocol
Collect process accounting logs	This module can be used to collect process accounting logs from a Linux or BSD kernel
Basic Security Module Auditing input	Registers an InputType to parse BSM Auditing files & logs from kernel
Network traffic log collection	Collect network traffic information using passive network monitoring
Batched compression input	Provides a compressed network transport with optional SSL encryption
DBI input	Sends log data to a database table using the libdbi library
Linux Audit System input	Provides rule management and log collection for the Linux Audit Framework, without external dependencies

macOS ULS input	Collects logs from the Unified Logging System (ULS) on macOS 10.12 Sierra and later
Database log collection	Collects logs from database tables via Open Database Connectivity (ODBC) drivers
Basic Security Module Auditing	Collects Basic Security Module (BSM) logs used by BSD derivative operating systems, such as Solaris, macOS, and FreeBSD
AIX auditing	This feature reads audit logs directly from the AIX kernel
File integrity monitoring	Periodically scans files and directories and generates events when changes are detected
Collects logs from Google Pub/Sub	Subscribe and collect logs from a Google Pub/Sub topic using it's REST API
Collect from Apache Kafka topics	Publishes events via the Apache Kafka messaging system
macOS Endpoint Security input	Collects logs from Apple Endpoint Security on macOS 10.15 Catalina and later
Windows Performance Counters input	Collects Windows performance counters as logs
Windows Registry Monitoring input	Periodically scans the Windows Registry and generates events when changes are detected
Collect logs from Amazon S3	This module can be used to collect logs from Amazon S3 and compatible services
Collect from Microsoft Azure	Collects logs from Azure Table storage, Azure Blob storage, and Azure Log Analytics tables
Collect from Check Point devices	Collects logs remotely from Check Point devices using the Opsec LEA protocol
Event Tracing for Windows input	Collects logs from the Event Tracing for Windows (ETW) API
Collect from Google Cloud Logging	Collects logs from the Google Cloud Logging REST API
Collect logs from Microsoft 365 log collection	Collects logs from Microsoft 365 services
Collect logs from a Redis database	This module can retrieve data stored in a Redis server. The module issues LPOP commands using the Redis Protocol
Salesforce log collection	Collects Event Log Files from Salesforce using the REST API
Windows Event Collector input	This module collects Windows events forwarded by Microsoft Windows clients with Windows Event Forwarding (WEF)
Collect logs over ZeroMQ	Collects logs over ZeroMQ (zmq, 0mq) message transport
Parse NetFlow payloads	Collects and parses NetFlow and IPFIX data using UDP
Parse SNMP trap messages	Collects and parses Simple Network Management Protocol (SNMP) trap messages over UDP
Collects events from Okta System Log	The module can collect events from Okta System Logs with SWSS authorisation.
Collects metrics from bundled OSQuery	The module can collect OS-level metrics with embedded OSQuery engine.
Collects agent's internal metrics for forwarding	Collect agent's internal metrics for forwarding

DATA PROCESSING AND PARSING

Feature	Description
Filter	This module forwards logs if the specified condition is met.
Format Converter	This module can parse and convert logs to BSD syslog, IETF syslog, CSV, JSON, and XML data formats.
Timestamping	This module provides support for the Time-Stamp Protocol as defined in RFC 3161.

Character set converter	Tools for converting text between character sets
Parse or generate logs in CSV format	Parses and generates any comma- and delimiter-separated data (CSV)
File operations	Performs file operations for log rotation and log file management within the NXLog Agent
Processing logs in Graylog Extended Log Format (GELF)	Sends and receives logs in the Graylog Extended Log Format (GELF)
Parse and generate logs in JSON format	Parses and converts JSON formatted logs
Parse and generate logs formatted as key-value pairs	Provides functions and procedures for processing data formatted as key-value pairs (KVPs)
Grok pattern matcher	Grok patterns parse unstructured logs into structured data for analysis
NXLog pattern matcher	Performs efficient pattern matching with an XML pattern database file
Parse or generate logs in syslog format	Parses and converts log data to and from the various syslog formats
Parse and generate logs in XML format	Functions for XML log formatting and parsing, converting messages and extracting fields
Process multiline logs	Parses log messages that span multiple lines
W3C Extended Log Format	Parses log data in the W3C Extended Log File Format and similar formats
Blocker	This module blocks log messages and can be used to simulate a blocked route
macOS system logs	Collects and parses Apple System Logs (ASL) files on Apple macOS machines
Log compression and decompression	Compress and decompress data using gzip or zlib algorithm
Log encryption and decryption	On-the-fly encryption or decryption for log data to provide data-at-rest encryption for log files
Compare lists	Provides functions to implement file-based blacklisting and whitelisting functionality
Resolver	Functions for resolving IP addresses, user IDs, group IDs, and their names
Rewrite logs	Add, remove, delete, or rename fields in events. Useful for cleaning, enriching, or adjusting logs at the point of collection
Buffer processing	Module supports disk- and memory-based log message buffering
Pattern matching	This module makes it possible to execute pattern matching with a pattern database file in XML format
Event correlation	This feature provides conditional execution based on correlation between events
HMAC message integrity checking	This module is the pair of pm_hmac to check message integrity
De-Duplicator processing	This feature filters out repeating messages through checking the previous message against the current
Parse events in the AIX Audit format	Module parses AIX Audit logs for comprehensive log management
ArcSight Common Event Format	Generates and parses data in the Common Event Format (CEF) developed by Arcsight
Log Event Extended Format (LEEF)	Parses and generates data in the Log Event Extended Format (LEEF) by Qradar
Microsoft DNS Server	Parses debug logs generated by Microsoft DNS Server
Microsoft Network Policy Server	Parses log data in the Microsoft Network Policy Server (NPS) Radius log format
SAP Security Audit Log (SAL)	Parses SAP audit log files created by SAP application servers

HMAC message integrity processing	HMAC algorithm secures log messages with cryptographic checksums, preventing unauthorized alterations

DATA SENDING CAPABILITY

Feature	Description
Write logs to files	This module can be used to write log messages to a file
Sends logs over HTTP or HTTPS	Sends logs via HTTP or HTTPS connections using POST requests. Supports multiline and multipart batching
Send logs to named pipes	Sends log messages to a named pipe on UNIX and Linux operating systems
Null output	Sends logs nowhere, fast. Equivalent to sending output to /dev/null. Data sent here will be discarded
Send logs to Raijin	Sends logs to the Raijin Database, a powerful, high-volume, schemaless database engine for log storage
Send logs over TCP	Sends logs over plain TCP connections
Send logs over TLS/SSL	Sends log data over TLS/SSL encrypted connections
Send logs via UDP from a spoofed source address	Sends log data over UDP. Useful for daemons which do not support other transports
Send logs over UDS	Sends logs over UNIX Domain Sockets (UDS) on Linux and UNIX systems
Send compressed log batches	Send compressed log batches over the network to other NXLog agent instances configured with this feature
Block log messages	This module is mostly for testing purposes. It will block log messages in order to simulate a blocked route
Send logs to a database	Sends log data to an external database with the libdbi library
Send logs to an Elasticsearch server	Improve Elasticsearch server performance with batched event transmission and dynamic indexing
Send logs to a database	Writes logs into database tables using Open Database Connectivity (ODBC) drivers
Send logs via UDP from a spoofed source address	UDP logging with IP spoofing sends packets with forged source IP
Send logs to Google Chronicle	Send logs to Google Chronicle using the unstructured logevents or UDM endpoint
Send logs to an Apache Kafka topic	Publishes event records to an Apache Kafka topic
Send logs to Microsoft Azure Monitor	This module forwards logs to Azure services that support the Azure Monitor Logs Ingestion API
Collector from Azure Monitor Log Analytics API	The improved module that allows to collect log entries from Azure Monitor Log Analytics API with internal pagination of oversized requests
Send logs to Google Pub/Sub	This module uses the Google Pub/Sub REST API to publish logs to a Google Pub/Sub topic
Linux to OpenTelemetry collector or backend Solution Pack	Easily collect various Linux system and security logs and send them directly to OpenTelemetry collector or backend.
Send logs to an Apache Hadoop cluster	Sends log data to Apache Hadoop using webhdfs
Send logs to Microsoft Sentinel	Forwards logs to Azure in a blob, table or Azure Log Analytics Workspace
OpenTelemetry Collector	This module accepts HTTP(S) and GRPC connections using the OpenTelemetry Protocol (OTLP) Specification. It supports traces, logs and metrics.
Send logs to Google Cloud Logging	Send logs to Google Cloud Logging REST API

OpenTelemetry Exporter	This module establishes HTTP(S) and GRPC connections to the collector or backend using the OpenTelemetry Protocol (OTLP) Specification. It supports traces, logs and metrics.
Send logs to a Redis server	Store data in a Redis server. Issues RPUSH commands using the Redis Protocol
OpenTelemetry to Google Chronicle Solution Pack	Easily collect OpenTelemetry logs and traces and send them to Google Chronicle.
Send logs over ZeroMQ	Sends logs via ZeroMQ (zmq, 0mq) message transport
OpenTelemetry to NXLog Platform Solution Pack	Easily collect OpenTelemetry logs and traces and send them to NXLog Platform.
Send logs to Amazon S3	This module can be used to send logs to Amazon S3 and compatible services
OpenTelemetry to Splunk Solution Pack	Easily collect OpenTelemetry logs and traces and send them to Splunk.
Microsoft Windows to OpenTelemetry collector or backend Solution Pack	Easily collect various Windows system and security logs and send them directly to OpenTelemetry collector or backend.
macOS to OpenTelemetry collector or backend Solution Pack	Easily collect macOS system and security logs and send them directly to OpenTelemetry collector or backend
Syslog to OpenTelemetry collector or backend Solution Pack	Easily collect logs on enterprise products using syslog and send them to OpenTelemetry collector or backend
Sends metrics to Prometheus	This module can store of latest metrics snapshot to be scraped by Prometheus.

DATA STORAGE

Feature	Description
Log storage - single node, on-prem	Free on-premises storage

REMOTE ADMINISTRATION

Feature	Description
Agent management	Allows to manage up to 10 data sources in Free Plan and above 10 in Premium
Remote management	Provides secure remote administration capabilities

SIEM SUPPORT

Feature	Description
Micro Focus ArcSight Logger SIEM support	Enable Micro Focus ArcSight SIEM integration
Microsoft Sentinel SIEM support	Forward logs to Microsoft Azure Sentinel SIEM
Securonix SIEM support	Enable Securonix Next-Generation SIEM integration
IBM QRadar SIEM support	Enable IBM QRadar SIEM integration
Splunk SIEM support	Enable Splunk Enterprise SIEM integration
Google Chronicle SIEM support	Enable Google Chronicle SIEM integration

SOLUTION PACK

Feature	Description

Okta to NXLog Platform Solution Pack	Collects Okta events and forwards them to NXLog Platform storage for visualization and analysis.
Okta to Google SecOps Solution Pack	Collects Okta events and forwards them to Google SecOps for visualization and analysis.
Configure log collection on Windows systems and send logs to Graylog	Configure log collection on Windows systems and send logs to Graylog
Configure log collection for Microsoft IIS logs and send them directly NXLog Platform	Configure log collection for Microsoft IIS logs and send them directly NXLog Platform
Configure Microsoft 365 message collection and send logs to NXLog Platform	Configure Microsoft 365 message collection and send logs to NXLog Platform
Collects OSQuery metrics and sends them to Prometheus	Collects local metrics with embedded OSQuery engine and prepare them for Prometheus to be scraped.
Collects Windows Performance Monitor metrics and sends to Prometheus	Collects local metrics with Windows Performance Monitor counters and prepare them for Prometheus to be scraped.
Collects OSQuery metrics and sends them to NXLog Platform	Collects local metrics with embedded OSQuery engine and forward them to OpenTelemetry Metrics collector.
Configure collection of OpenTelemetry logs and traces via HTTP or gRPC and send them to Microsoft Sentinel	Easily collect OpenTelemetry logs and traces and send them to Microsoft Sentinel.
Expose Agent internal metrics for Prometheus Scraper.	Expose Agent internal metrics for Prometheus Scraper.
Expose Agent internal metrics via OpenTelemetry HTTP and gRPC endpoints.	Expose Agent internal metrics via OpenTelemetry HTTP and gRPC endpoints.
Microsoft Windows to Google Chronicle Solution Pack	Easily collect various Windows system and security logs and ship them directly to Google Chronicle
macOS to Google Chronicle Solution Pack	Easily collect various macOS system and security logs and ship them directly to Google Chronicle
macOS to Azure Sentinel Solution Pack	Easily collect various macOS system and security logs and ship them directly to Azure Sentinel