Nagios Log Server 2024R2 Technical Overview and Terminology Definitions

Purpose

This document is designed to provide an explanation of what Nagios Log Server 2024R2 is, how it can be used, and to define terminology related to it.

Target Audience

This document is intended for use by Nagios Log Server 2024R2 users and administrators.

High Level Overview

Nagios Log Server is an application that provides organizations with a central location to send their machine generated log data to. Collected logs are indexed and stored for later retrieval, querying, and analysis in near real-time. Log Server has built-in support for a wide variety of log sources.

Once log data has been indexed (which usually happens within 5 seconds of arrival) it can be easily analyzed using the graphical query and filtering tools on Dashboards, viewed in Reports, and alerted on.

Finally, the data that is sent to Nagios Log Server can be automatically archived to a shared network drive. The archived data can be restored and re-analyzed at any point in the future.

In summary, this solution can be used to record any log events that are happening across your organization's machines, applications, and network devices. Users can access, search, and visualize the collected data in a central location using the web UI. Having all your data in one location has the added benefit of enabling you to compare or correlate log data from multiple devices. Automated archiving of the log data will assist in maintaining compliance with certain standards that require historical log data retention.

Example Use Cases

- Nagios Log Server could be configured to email administrators immediately if a chosen number of failed login attempts occur on source systems within a set timeframe.
- Nagios Log Server could be used as part of an advanced system to analyze the received log events and send important items (e.g. critical errors and security events) to Nagios Core or Nagios XI for alerting and reporting alongside other standard checks being run by the Core or XI servers.
- Organizations can utilize the graphical and analytical capabilities of Nagios Log Server to analyze web server logs, not only for errors and security issues, but to determine the most requested pages, the geo-location of their visitors, the most popular browsers, and more.

- Developers can send debug logs to Nagios Log Server, and easily filter out the information that isn't important, leaving just the key items of interest.

Benefits Over Text-Based Systems

Though text-based log aggregation systems aren't tremendously difficult to set up, there are a variety of pitfalls and difficulties that must be considered and addressed to maintain and make constructive use of them. Nagios Log Server takes all of these and more into consideration.

Nagios Log Server enables all your organization's log data to be stored and indexed in one central location, allowing for queries to be performed on the data so that narrowing results down to specific sources and occurrences is easily done. The ability for pruning, correlative analysis, and visualization via the web GUI both simplifies and speeds up analysis.

This data can be presented to the user running the query in customized views including a table of results, bar charts, pie charts, and line graphs. Calculations can be run on numeric fields in the log data to provide data such as minimum, maximum, mean, and standard deviation in Dashboard panels.

Nagios Log Server also supports Multitenancy, enabling administrators to easily define which sources are visible to each user, and what administrative capabilities they have within the system.

Log Server Terminology

Alerts

Nagios Log Server can take a variety of actions when query-based alert states occur:

- Send to Nagios XI or Nagios Core via NRDP
- Send an SNMP Trap
- Send an Email
- Execute a custom script

Alerts can also be viewed in the web GUI in the Alerts menu.

Cluster & Instance

- **Cluster:** A collection of Nagios Log Server Instances. Each Instance in the Cluster stores a portion of the data in the Indices as well as sharing in the workload of performing indexing, searching, alerting and maintenance operations. Clustering increases the volume of data Log Server can be used to intake, analyze, and store, and provides data protection through clustered redundancy.
- **Instance:** A single server or VM running Nagios Log Server. Although Log Server can be run as a single instance installation for small requirements and testing, it is designed to be run as a cluster of multiple Log Server instances working together.

Cluster Hostname

Specifying a Cluster Hostname and will populate the source setup guides with that name in lieu of the IP/hostname of the directly accessed instance. This allows those using round robin DNS or load balancers to send logs to one hostname and have them distributed to any member of the cluster.

Config Snapshot

A snapshot of the Logstash configuration which can be restored if needed. These are created automatically when changes to Inputs, Filters, and Outputs are applied, and can be saved manually.

Dashboard

A customizable search, analysis, and visualization page. Each user can have multiple Dashboards, and several built-in Dashboards such as Nagios Log Server Search and Top Sources and Types are automatically included. Dashboards can be easily turned into Reports.

- **Query**: One or more queries can be added giving them different color representation for items matching the query fields.
- **Filter**: Filtering limits the items in the result set to either contain or not contain certain elements. On a technical note, Filters are cached in OpenSearch and usage of filters can dramatically speed up the response time.
- **Row**: Each Dashboard is made up of one or more rows. Each row can contain multiple panels, and be expanded and collapsed as needed.
- **Panel**: Panels are added to rows and can be resized easily by clicking on an edge and dragging. Panels can also be dragged and dropped to be moved around in Rows. There are many different panel types allowing users to create combinations of graphs, table views, or even add a text/HTML block describing other elements on the page.

Log Source

A system or application configured to send log data upstream to Nagios Log Server. Built-in setup guides include:

- Windows and Linux systems
- Windows and Linux files
- Network Devices
- Apache and IIS
- MySQL and MS SQL

Logstash

The package used to receive and pre-process log messages before sending them to Opensearch for indexing. Logstash has dozens of possible Inputs and Filters that can be added through the Configure menu to enable additional capabilities.

- **Inputs**: Additional Inputs can be added to allow Nagios Log Server to collect data from various places, like TCP/UDP ports, SNMP Traps, unix sockets, long running command pipes, etc.
- **Filters**: Filters can be applied to messages before they are sent to Opensearch for indexing. They perform actions such as breaking apart messages into fields for easy searching, adding geo-location information, resolving IP to DNS names, and dropping messages you do not want indexed. Using custom Filters, non-standard log data from less common source types can be organized and utilized.

Opensearch

The Storage/Indexing engine used in Nagios Log Server.

- **Index**: The primary unit of storage, an OpenSearch index, akin to a database. Nagios Log Server creates a new index for each day's logs. Additionally, there are several indices used to store settings, user information, and internal audit logs. An **Open** index is one which is live and queryable on the Cluster. A **Closed** index is one that remains on the Cluster, but must be opened to be queried. Closed indexes use drivespace, but not other system resources.

  Important Note: The default system setting is to close indices older than 60 days. Additionally, Log Server has a maximum limit of 1,000 shards worth of open indices per instance. Each daily index is broken into 5 shards, and a few indices are created for items other than log events, so a single instance allows for less than 200 days worth of open indices. To increase this limit simply add instances to your cluster.

- **Shard**: Each Index is broken up into multiple shards, which allows the distribution of data and workload across the cluster. By default each index in Nagios Log Server has 5 shards. Each shard is a single Lucene instance. Nagios Log Server knows exactly which Shard in the cluster contains each log message, so for direct retrieval it does not need to interact with other Shards.
- **Lucene**: OpenSearch is built on top of Apache Lucene which is a full text indexing and search engine. Coincidentally, Lucene was first introduced in 1999, the same year Ethan Galstad created NetSaint. Lucene joined the Apache Project just after NetSaint was renamed to Nagios.

Report

A customized visualization of specific data which can be emailed and downloaded. Many default reports are included in Log Server such as the SSH Errors Report and the Windows Updates Report. Custom Reports are created by first creating a Dashboard reflecting the desired data set and visualizations, then saving it as a Report.

Snapshot

A backup of a particular index. Snapshots can be restored at future dates if data needs to be recovered.

Snapshot Repository

This must be a shared Network file system that is accessible by ALL Instances. The Repository will hold all archived Snapshots until they are deleted.

User

A person or group granted access to the Log Server web interface via a unique username and password. Each User can be granted visibility of data from all log sources, or a limited view of only specific sources or Host Lists. Admins can also define to what extent each User can view and interact with Alerts, Contacts, and Configurations. Each User can create their own custom Dashboards and Reports, and all users can view Global Dashboards and Reports.

Finishing Up

This completes the documentation on Nagios Log Server Technical Overview and Terminology Definitions. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum Visit Nagios Knowledge Base Visit Nagios Library