Purposes

This document describes several use cases for Nagios Log Server and provides a general overview of the benefits received when implementing Log Server. This document is intended for use by IT Managers, Sales staff, and anyone looking to gain information on the practical applications of Nagios Log Server in their organization or IT infrastructure.

Use Cases for System Administrators

1. **Data Retention & Auditing** – Use Log Server to dive deep into network logs and events. When a network incident occurs, use Log Server to help find a solution by discovering what went wrong while keeping historical records of all network events and activity. Nagios Log Server provides system administrators with the ability to audit network incidents, retain critical event data, and solve problems faster.

2. **Security / Threat Investigation** – Log Server can provide system administrators with a dynamic threat response. Log Server has the ability to alert on log events based on their subject matter. If there is a security breach, Log Server can provide teams with the information necessary to mitigate future compromises and spot the problem at the source. Log Server's ability to provide teams with this useful information maximizes company resources and minimizes down-time.

3. **Root Cause Analysis** – System administrators using Log Server can use historical data to determine what when wrong in a particular incident. Analyze log events to see what went wrong, what time the incident took place, and help determine how to resolve the issue.

4. **System Diagnostics** – Nagios Log Server can provide system administrators with the tools necessary to spot and diagnose server and application errors by providing insight into when issues occur, and what specifically caused the log event.

Use Cases for Managers

1. **Log Event Data Backups & Storage** – Implementing Nagios Log Server allows Managers to have an automatic backup of all network log event data for historical referencing. In a multi-instance environment, Log Server provides fail-over protection and redundancy to ensure data security. Maintain full access to historical data for company audits and organizational standards.

2. **Change Control & Auditing** – Log Server allows management to see who is making changes on the network. Ensure users aren't making changes that shouldn't be made and determine if new user permissions should be implemented. See who does what and drill down to specific user actions.

Use Cases for Developers

1. **Debugging & Troubleshooting** – Quickly debug applications with "line-by-line" event analysis. See when problems occur and determine whether development changes should be made. Log Server can provide fast debugging and troubleshooting capabilities to developers to ensure programs and projects function the way they should. Filtering out all of the items you do not want to see so you can just spend your effort looking at the information you need.

2. **Spot Performance Bottlenecks** – Use Log Server in development scenarios to spot performance bottlenecks in applications. When analyzing debug logs, Log Server can help determine what tasks are most time intensive in your code and where greater efficiency is needed. Ensure your applications run quickly and smoothly with Nagios Log Server.