



UIT LogGuard™ Log Monitoring And Analysis Tool

White Paper
Athens November 2009

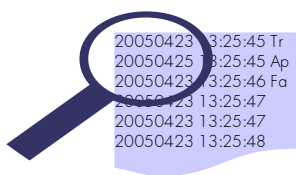




Table Of Contents

Executive summary.....	3
Where it fits.....	4
Functionality.....	5
Architecture description.....	6
Installation types.....	7
Components and standards.....	7
Licencing and Support	8
About UIT.....	8





Executive summary

Now-day's expansion of IT Infrastructure created the demand for accurate monitoring and inspection of heterogeneous mission – critical systems that compose the heart beat of company's IT. In order to cover this demand several solutions/products have been proposed and offer various features that can be categorized to the following groups:

- Log File Analyzers
- Network Monitoring (SNMP – based solutions)
- Revenue Loss and Assurance Monitoring Systems

Starting with Log File Analyzers, the main feature of such solutions is to analyze text – based log files from several systems and issue alerts and in some cases, storing the results to a dedicated database. It is the IT Team responsibility to create the desired reports. Most of the times, such solutions lack the support of SNMP alerts gathering and focus only in near-real time log files analysis.

Network Monitoring tools, focus in SNMP oriented traffic gathering and are able to create real time alerts. The philosophy of the group is based on SNMP traffic gathering, meaning that there is no alternative option in order to gather custom alerts or define within the overall solution, custom-made log analysis tools. Further more almost all of such proposed products define strict rules in storage of gathered events.

Revenue Loss and Assurance Monitoring Systems are complicated systems that provide log analysis in near real time and focus in per group of cases action. This action is triggered once or twice per day when cases analysis has been carried out as a result of a complex business processes . Doing so, Revenue Loss systems are not able to provide near – real time alerts for such events. Further more, most of the times such systems are difficult to migrate and expand due to the fact that enhance complex business intelligence.

In the following pages UIT provides a smart framework that combines the advantages of the three categories in one single product, providing this way a very effective solution that may fits in your organization's IT infrastructure. *LogGuard™* is a solution that will assist your IT Team to gather events, process them, extract the desired KPIs (Key Performance Indicators) and reports and finally notify the involved systems for furthermore actions, even more undertake the processing of the proposed actions.

LogGuard™ is a component based framework that relies on a pure based SOA (Service Oriented Architecture), capable to deliver an outstanding performance as a middle-ware between your SNMP Monitor, Revenue Assurance and minor Log Analyzing tools or even act as one of them. In the following pages you will discover how *LogGuard™* has been designed to catalyze a lightweight business integration deployment project. It offers a “fit-to-purpose” mix of features, functionality, extensibility, and support at the best cost.



Where it fits

LogGuard™ is a framework that fits in the heart of your IT infrastructure, very close to your SNMP Monitoring Platform, your Business Tandem Applications (like Mediation, Rater, Billing, Fraud Management or Revenue Assurance) and other mission – critical systems like Database Servers, Application Servers or ESB whose performance must be continuously monitored. *LogGuard™* interfaces all those systems and acts like a repository of information regarding their performance. Even – more *LogGuard™* can take specific actions when alerts are issued from those systems.

The types of systems that can be monitored are:

- **Network or Hardware:** Use *LogGuard™* framework to assist your SNMP platform or act as an SNMP platform. Benefit from *LogGuard™*'s Fast Polling Agent or SNMP Server in order to collect SNMP Traffic or use the offered Communication Interfaces to dispatch events collected from your SNMP platform.
- **Middle ware Enterprise Applications:** In case you have HTTP Servers, Application Servers, ESB (Enterprise Service Bus), Enterprise Database Servers, *LogGuard™* provides the best solution in order to keep track of their performance by examining their logs in near real time. Especially for Application Servers or ESBs, *LogGuard™* is designed so that it can monitor specific applications like Web Services, Servlets, MBEANs, JSPs or ASP .NET deployed on them and provide you the outcome of their performance. Even more, *LogGuard™* can take specific actions like redeploy or shutdown a Web Service or any other application.
- **Business Applications:** For those applications that are money – makers and your organization relies on them (like Rating-Billing, Fraud Management, Commissioning, Provisioning), *LogGuard™* can continuously monitor their performance and provide your IT team valuable reports and KPIs calculating this way your Revenue Loss. More over, *LogGuard™* can specifically indicate you *per case* problems (for example CDRs discarded from a billing phase due to un-identified tariff plan, or disordered partial CDRs discarded from mediation) in order to reprocess the cases at a later time.

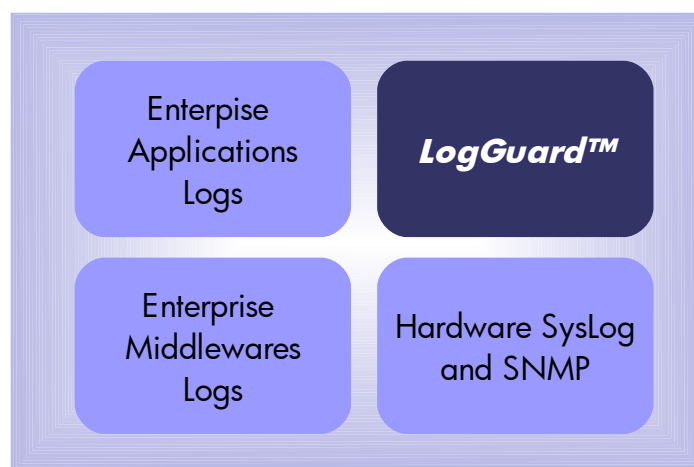


Figure 1: *LogGuard™* Collected Information



As an example the following applications of *LogGuard™* are presented:

- **Stand alone:** This is the simplest case where no SNMP monitoring platform is used. Instead of an SNMP platform, *LogGuard™* can handle the events from several sites or applications in real or near real time or off-line, store them in its repository and take a specific action for each one of them.
- **In combination with an SNMP Platform:** In this case, the existing SNMP monitoring platform (like HP's OpenView, CISCO's LAN Manager) interfaces *LogGuard™*. SNMP Platform as the Active SNMP platform trapping real time SNMP alerts and *LogGuard™* as the near real time or off line log collector. In this case *LogGuard™* after log processing will provide the SNMP Platform the appropriate results. This is the most frequent use of *LogGuard™* since most of the SNMP platforms cannot handle detailed log files analysis such effectively as *LogGuard™* does.
- **In combination with a Revenue Assurance or Fraud Management Platform:**
Undertaking the following roles:
 - *Dispatcher case:* *LogGuard™* can act as a dispatcher system that ignites actions issued from Revenue Assurance Platform. Requests are sent to all the involved systems using several communication interfaces (SNMP, HTTP, Web Service Consumption, JMS, FTP, file interface, Store Procedure Call)
 - *Mediator case:* In this case *LogGuard™* can be used in order to mediate events parsed from Log files and feed the Revenue Assurance Platform with fully mediated information, allowing this way the Revenue Assurance Platform to operate without losing significant resources for file parsing.

Functionality

LogGuard™ framework allows the following group of operations:

- **File Gathering:** Using specific FTP, sFTP agents and file movers it can provide a centralized repository for all selected files from the network.
- **File Parsing and Mediation:** *LogGuard™* parser libraries are very sophisticated achieving this way an outstanding performance. There are two cases of entities: parsers and mediators. Parsers simply parse the row files while mediators combine parsed or un-parsed results to a solid and mediated piece of information. In order to create custom parsers, a JAVA API is available and if a case is a really resource demanding, the native C++ API can be used instead. The results are stored to *LogGuard™* database or sent to other systems using the Event Dispatching Components.
- **Event Dispatching to other Systems:** *LogGuard™* offers a wide open set of components to interface heterogeneous applications. After information is parsed or trapped it can be forwarded to several systems using WEB Service Consumption, HTTP, JMS, FTP, DB Procedure call. Moreover, events occurred from row information can be forwarded to other systems or create email or SMS notifications.



- **Reporting and Analysis:** Using the stored information *LogGuard™* can provide almost any report you need. Reports include per fault case analysis, most frequent events, node specific results, or general KPIs extraction. Reports production is fully expandable since it has a separated engine specifically designed for this purpose.
- **SNMP Server Gathering:** In case you want to use *LogGuard™* for SNMP monitoring, *LogGuard™* offers a fast SNMP Polling agent and a SNMP traps – alerts collector. The results are gathered to *LogGuard™* SNMP Traffic repository.

Architecture description

LogGuard™ Framework is a fully modular framework consisting of the following sub -systems:

- ***LogGuard™* Database:** In order to achieve best performance, two separated schemas are deployed. The first stores the log metrics and SNMP traffic while the second is used to create reports and calculated KPIs.
- ***LogGuard™* Schedulers:** The Core system that is composed from several plug-able components and is responsible to gather SNMP, parse Log files, ignite, accept and forward events.
- ***LogGuard™* Web Interface:** Consists of the Scheduler Configuration Platform and Reports and KPI configuration.

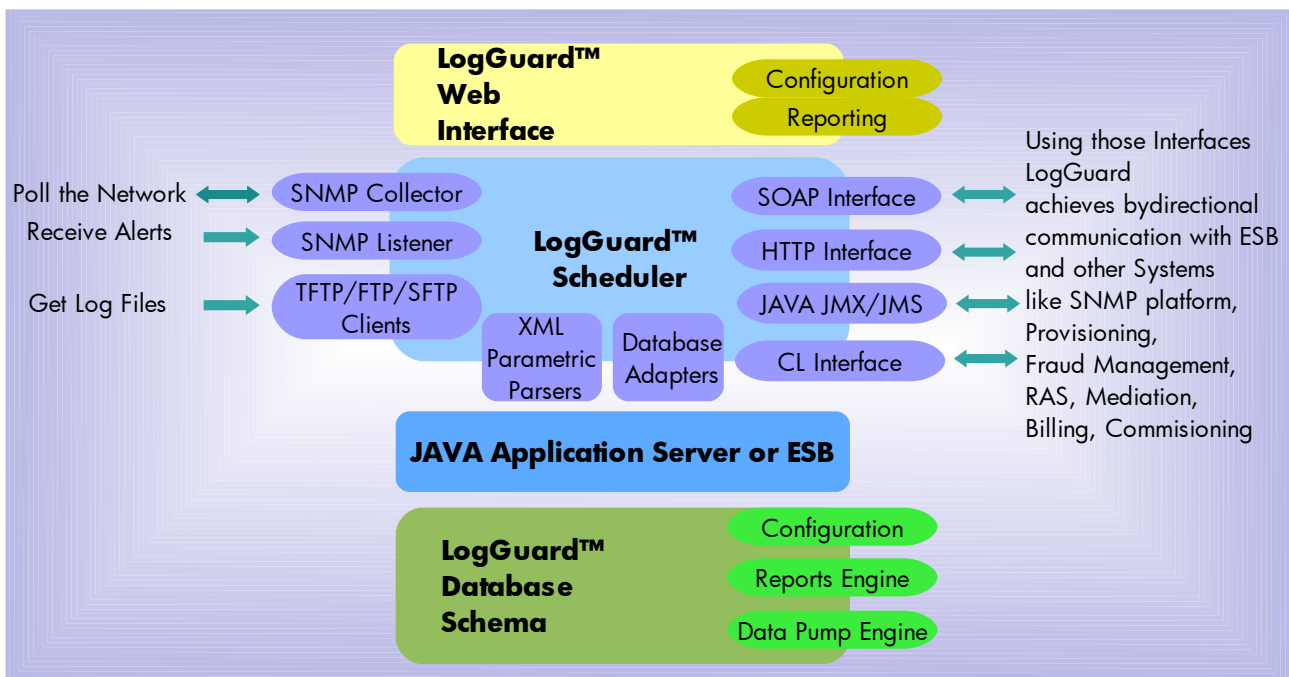


Figure 2: The *LogGuard™* Overall Architecture



Installation types

LogGuard™ offers three types of installations so that you can choose the appropriate one for your infrastructure:

- **Stand alone:** Without an application server. This is the simplest model where no application server is needed. In this type of installation *LogGuard™* will parse and mediate log files, store the parsed entries to its database and dispatch events to several systems. Use this type of installation when you don't need to produce reports from *LogGuard™* report engine, or change the configuration on the Web. Produce reports using your reporting tool by queering the *LogGuard™* Database and change *LogGuard™* 's configuration by editing its XML configuration file.
- **Deployed on Application Server:** In this way you can produce reports using *LogGuard™* report engine, or change the configuration on the Web. Using this type of installation, you can control *LogGuard™* in real time using the *LogGuard™* Web Interface.
- **Deployed on ESB** In this way you can achieve *asynchronous communications using Web Service callbacks* with other SOA based applications, produce reports using *LogGuard™* report engine, or change the configuration on the Web. Using this type of installation, you can control *LogGuard™* in real time using the *LogGuard™* Web Interface.

Components and standards

LogGuard™ uses stable components from the JAVA community to deliver core ESB functionality for a lean SOA deployment. The design aims to of department-scale Web Service deployments with minimal customization and fine-tuning overheads. *LogGuard™* components and technology support details are listed in the following table.

<i>LogGuard™</i> OS Compatibility	Linux and Windows
<i>LogGuard™</i> Database	MySQL v5 , Oracle 9i and above
<i>LogGuard™</i> Configuration	XML
<i>LogGuard™</i> Installation Java Runtime When Stand Alone	JRE 1.4.2 and above
<i>LogGuard™</i> Installation Application Servers	JBOSS 4,5 , Websphere 6
<i>LogGuard™</i> Installation ESB	Websphere ESB v6, GlasshFish, OpenESB
Binding Components	HTTP FTP, File Command Line Interface (CLI) Java Messaging Service (JMS) LDAP, Open LDAP Windows 2003 Active Directory
DB Binding	Any DBMS implementing JDBC
API for custom parser generation	JAVA C/C++ Provided that infrastructure allows JNI





UNIFIED IT Services
67 Ag. Paraskevis str | 15234 | Halandri
<http://www.uit.gr>

Licencing and Support

About UIT

