



assuria

Assuria Log Manager

Assuria Log Manager

Operating systems, system software and applications have for many years had features to write audit logs to record events, data or actions taken. The benefits of using log data are well known to IT professionals who have used the information contained in logs for diagnostics and to verify actions taken by software, often as the first steps in problem identification.

Today such audit logs have attained a much higher level of importance; this is driven by several factors including policy compliance requirements. Organisations of all sizes and in both the public and private sector are increasingly required to be in compliance with an increasing number of legislative and industry regulations and standards. The requirements are driving organisations to seek tools to assist and automate their log management and compliance processes.

Valuable information

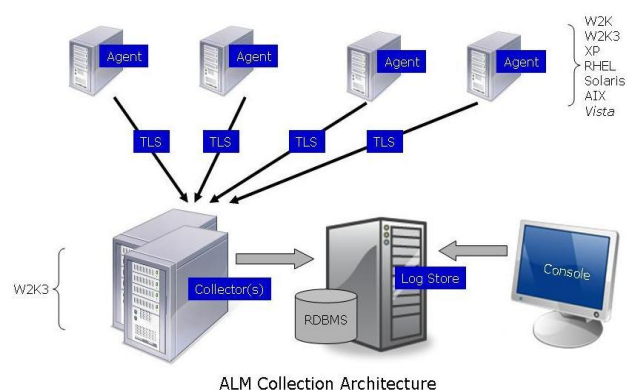
Uses for collected logs and log data can vary from near real-time collection and in-memory correlation of network traffic, through near real-time alerting / host based intrusion detection, regulatory compliance reporting, problem identification and resolution to incident response and forensic analysis.

Logs have become essential to demonstrate compliance to regulations and standards.

Uses for log data in addition to regulatory compliance include:

- Incident response and investigation
- Forensic analysis
- Problem identification and resolution
- Network traffic monitoring (near Real time) and anomaly detection
- Operations and Service Level monitoring
- Marketing analysis

Today's operating systems, applications and network devices, including Windows and LINUX / UNIX, can produce vast amounts of audit data within their logs. There are few tools available today to provide for reliable management of this log data.



Assuria Log Manager

Assuria Log Manager (ALM) is designed to meet the requirements of enterprise wide management of audit logs generated by systems, devices and applications. ALM is equally applicable to installations with ten systems or tens of thousands of systems.

Assuria Log Manager manages large communities of logs from Servers and Workstations, Windows, LINUX and UNIX as well as Databases, Applications and network devices such as firewalls and routers. Assuria Log Manager does not preclude the collection of logs from other devices such as building access control systems.

Multiple users can log into the Assuria Log Manager Console to manage agents, agent policy, create archives, generate reports or other actions required.

Assuria provided 'Content Packs' are used to define log format, content and rules for event identification and tagging. A 'Content pack' is available for each supported type /format log.



assuria

Assuria Log Manager

Features

- **Enterprise wide log collection.** Secure and forensically sound collection of logs into a central store.
- **Real-time alerts.** Configurable to specific log events, sent via SNMP or configurable to other tools.
- **Agent based collection** ensures the Security, Continuity and Integrity of all collected logs.
- **Digitally signed.** A SHA256 checksum is calculated and the log digitally signed before transfer. The transfer of logs over the network is encrypted using TLS.
- **Secure storage.** Log cataloguing, chain of custody records, archive creation and management.
- **Archive** to secure long terms storage, complete with a digitally-signed manifest.
- **Forensic readiness.** Centrally stored, with all of the handling of the logs preserving the original format so that forensically sound data is available for investigation when required.
- **Scalable and Modular architecture.** Designed to support from 1 to 000's of log sources.
- **Log packs** provided by Assuria are flexible and extensible used to describe each log allowing 'interesting events' in the collected logs to be tagged and indexed within the ALM database.
- **Analysis:** Collected logs are processed by a rules-based analysis engine, allowing 'interesting' events to be tagged and written to a database for further analysis and reporting.

* ALM Console and 'log processing' modules are designed and implemented to be cross platform, currently tested on Windows.

- **Reporting.** Flexible analysis, correlation, aggregation and reporting in HTML or PDF.
- **Console.** Assuria Log Manager Console provides all agent control and the management of collected logs along with facilities to run queries, generate and print reports.

Log Sources supported

Supported log sources include:

- Windows .EVT logs
- Syslog, Unix Daemon
- Exchange Server, IIS
- RHEL Audit
- Text files
- Tcl – Plug-ins, support the collection of an infinite number of log formats / types.

Platform support

Console

- Windows*

Collector and log 'processing' modules

- Windows*

Agents

- Windows 2003 Server, XP
- Red Hat Enterprise Linux 4+
- IBM AIX 5L 5.1+
- HP HP-UX 11+
- SUN Solaris 8+

Please discuss your requirements for the support of other platforms and log sources with Assuria.



Castleforce IT Consultancy
www.castleforce.com
tel (north): 0151 203 1400
tel (south): 0118 907 1600
info@castleforce.com

Assuria Limited,
Science & Technology Centre, University of
Reading, Earley Gate, Reading, RG6 6BZ,
W: www.assuria.com E: info@assuria.com
T: +44 118 935 7395 F: +44 118 926 7917