

Title: Assuria Log Manager – Release 3.5.2
Number: 10-03 Date: 31 January 2010

Title Assuria Log Manager – Release 3.5.2

Introduction The Bulletin introduces the latest generally available release of Assuria's proven log management technology Assuria Log Manager Version 3.5.2 which can be downloaded from AssuriaOnline.

New features at 3.5.2. release ALM 3.5.2 is released to introduce a number of underlying product improvements and fixes to users. Existing ALM users should contact Assuria for information on upgrading to this release.

Assuria Log Manager ALM is designed to deliver of enterprise wide forensically sound management of audit logs generated by systems, devices and applications. ALM is a fully scalable solution, applicable to installations with ten systems or tens of thousands of systems.

ALM manages large communities of logs from, Windows, Linux and UNIX servers and workstations as well as databases, applications and network devices such as firewalls and routers. The architecture of ALM means that logs can be collected from almost any source enabled via agent 'plug-in' connectors.

ALM provides:

- secure transfer of system logs from individual systems onto a central management system. The secure transfer is performed so that the logs may, if required, later be used for forensic analysis and/or evidential use.
- near real-time alerting against specific events.
- viewing of the centrally held logs
- archiving to long term storage of collected Logs.
- analysis of the logs using analysis rules storing *interesting* events into a database for further analysis, correlation and reporting.
- Searching of the logs for events

Centrally, ALM allows filtering, viewing, analysis, reporting and archiving of the stored logs.

For devices such as Firewalls, Routers and other devices that can forward logs to a 'syslog' server these can be collected by ALM. The ALM agent includes an Assuria 'syslog' server.

Assuria Log Manager agents includes an alerting mechanism that

can be configured by security configuration personnel to alert (SNMP or other) on the occurrence of specified events (such as Administrator / Root login failures).

Additional standard data sources.

New log data sources have been added at this release 3.5.1 including:

- AppGate devices
- Palo Alto devices
- CISCP PIX / ASA analysis rules

For a complete list of supported datasources please contact Assuria.

Further information

For further information about Assuria Log Manager please contact Assuria.

Assuria Limited, Science Technology Centre, The University of Reading, Earley Gate, Reading, RG6 6BZ, UK.

Telephone +44 118 935 7395 Fax +44 118 926 7917 Web www.assuria.com