

Title: Assuria Log Manager – Release 3.5

Number: 96 Date: 12 June 2009

Title Assuria Log Manager – Release 3.5

Introduction The Bulletin introduces Assuria's proven log management technology Assuria Log Manager Version 3.5 which is now generally available and can be downloaded from AssuriaOnline.

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 a fully scalable solution and equally 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 'plugin' connectors.

ALM meets the requirements of enterprise wide management of audit logs generated by systems, devices and applications. ALM is highly scalable from ten systems to tens of thousands of systems.

ALM provides:

- a mechanism for the 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.
- facilities to allow viewing of the centrally held logs
- facilities for the archiving to long term storage of collected Logs.
- facilities for the analysis of the logs using analysis rules storing *interesting* events into a database for further analysis, correlation and reporting.

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 optionally include 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).

SQL Server Database

ALM 3.5 uses Microsoft SQL Server 2005 for its database; for small installations and evaluations SQL Server 2005 Express can be used while SQL Server 2005 is required for larger deployments.

Console.

The ALM Console has an updated look and feel and has many minor changes and addition to improve it's usability and understandability including a dynamic enhanced dashboard.

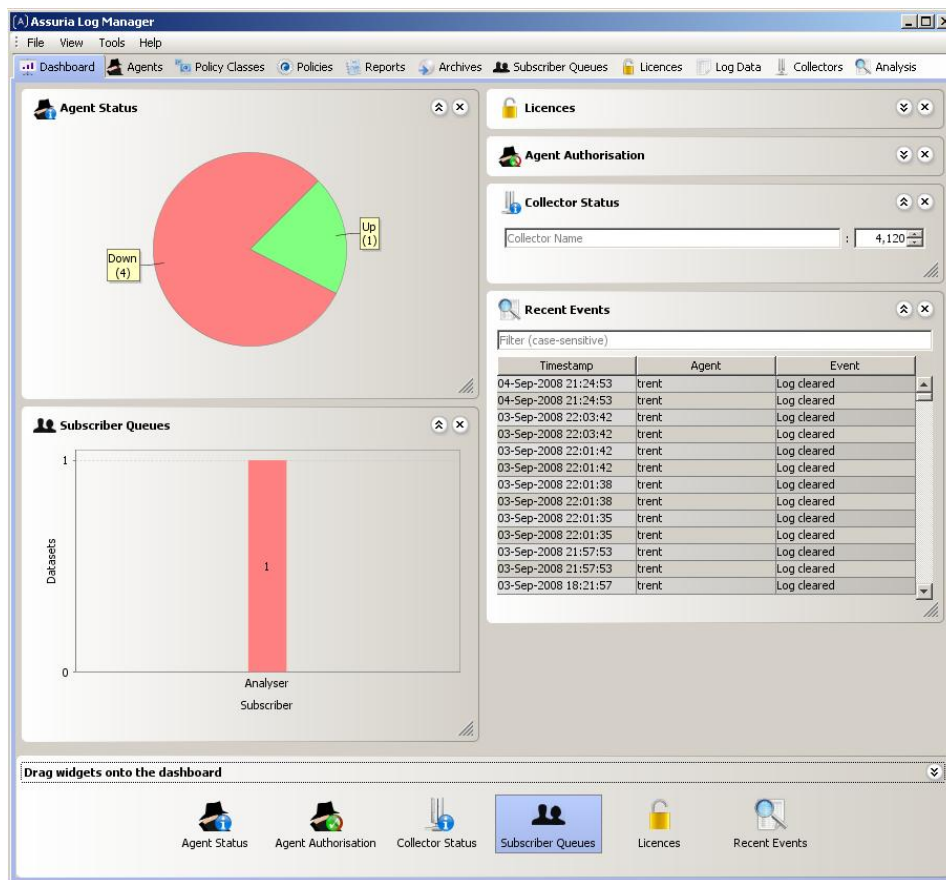


Figure – Assuria Log manager 3.5 – Dashboard

The ALM dashboard provides a number of standard dashboard widgets. Each widget can be dragged onto the dashboard. Widgets can be re-sized, moved and collapsed. Toolbars can be re-positioned.

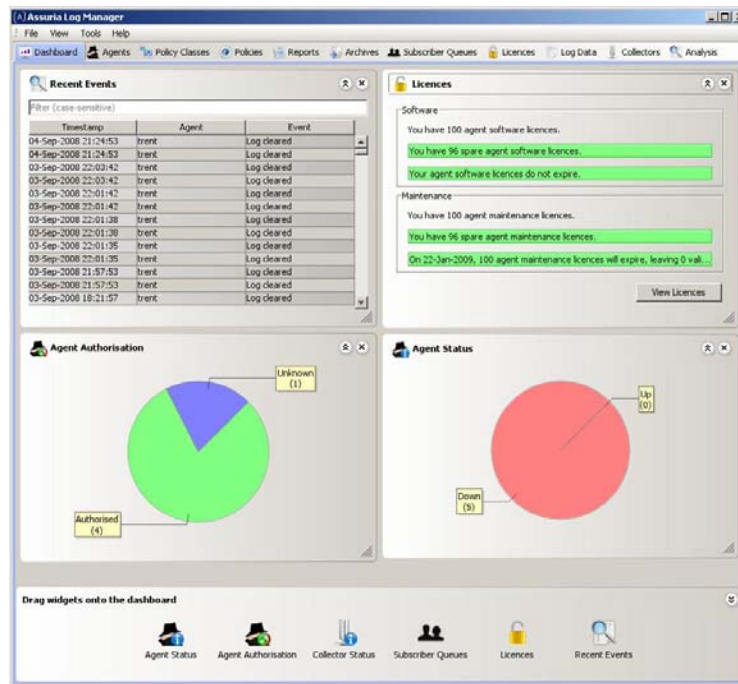


Figure – Assuria Log Manager 3.5 – Dashboard with some widgets re-positioned.

Additional standard data sources.

New log data sources have been added at this release 3.5:

- Sharepoint 2007 logs
- Windows Server 2008 and Windows VISTA
- Assuria built-in syslog server

Data sources currently supported at Assuria Log Manager version 3.0

- Windows event logs (.evt)
- Text log files
- HP Audit logs (HP-UX 11.11 and 11.23)
- Solaris BSM logs 'syslog' from various platforms
- IIS on W2K and W2K3
- SQL Server 2000 / 2005 error logs
- ALM Agent Log file
- Exchange Server 2003 message tracking logs
- RHEL audit logs (raw or via ausearch -i)

In development

- VMware ESX 3.5 logs

Reports

Available reports include:

- Analysis/Count of Notable Events
- Analysis/Count of Notable IIS Events
- Analysis/Count of Specific Forbidden Access Attempts
- Analysis/Count of Specific Unauthorised Access Attempts
- Analysis/List Forbidden Requests
- Analysis/List Unauthorised Access Attempts
- Analysis/Login Failures
- Analysis/Password File Access
- Analysis/User Accounts Changed
- Analysis/User Accounts Created
- Analysis/User Accounts Deleted
- Analysis/User Accounts Disabled
- Analysis/User Accounts Enabled
- Archive/Archive Detail
- Archive/Archive List
- Audit/Audit Report
- Collection/Collection Summary
- Collection/Collection by Agent
- Collection/Collection by Period
- Collection/Collection by Policy

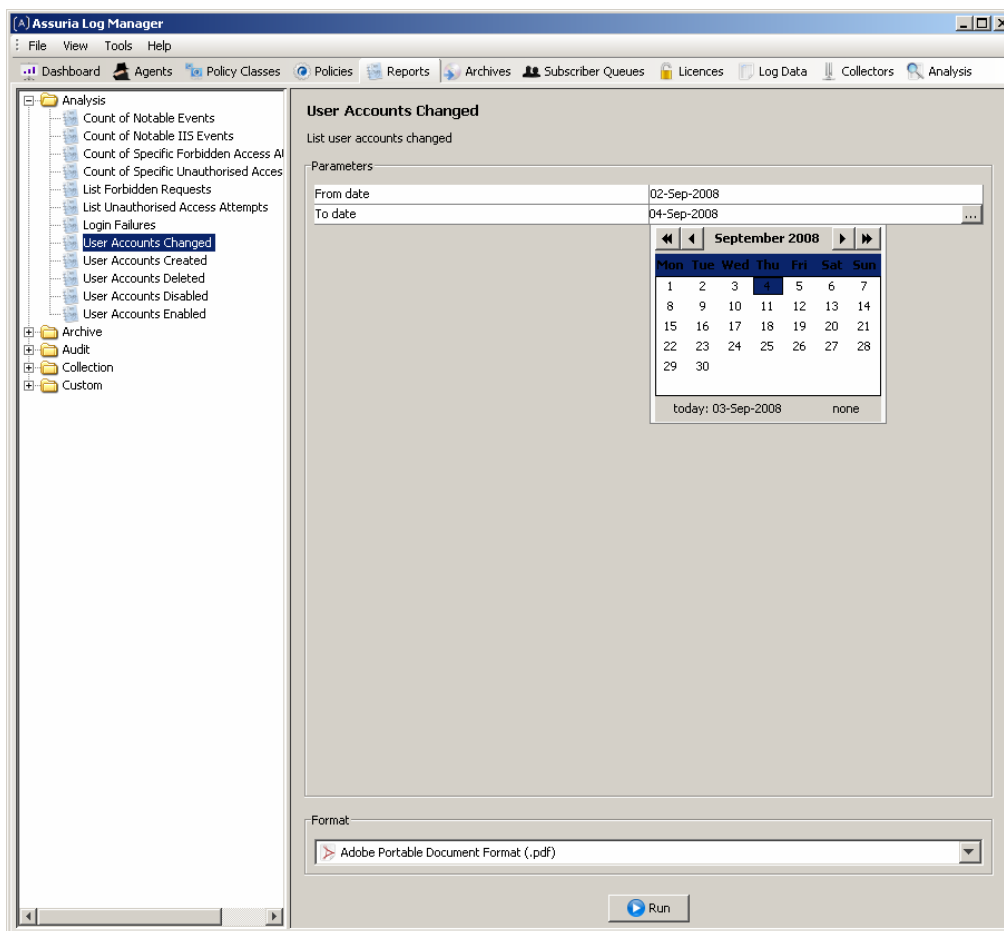


Figure – Reports tab of the ALM Console

Agents available for

Assuria Log Manager agents are available for:

- Windows 2000
- Windows Server 2003
- Windows Server 2008
- Windows XP
- Windows VISTA
- Red Hat Enterprise Linux 4 and 5
- Debian GNU Linux 3.1
- IBM AIX 5.1 to 6.1
- HP HP-UX 11.11 to 11.31 (PA-RISC)
- HP HP-UX 11.31 (ITANIUM)
- Sun Solaris 8- 10 (SPARC)
- Sun Solaris 10 (X86)

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