

Halcyon audit journal monitor



The Halcyon Audit Journal Monitor provides real-time monitoring of the OS/400 system audit journal, QAUDJRN, the key place for logging security related events.

Systems administrators can define the type of events they want to monitor and the Halcyon Audit Journal Monitor will proactively monitor the journal for these events and automatically perform pre-defined actions.

Team this product with the Halcyon Message Communicator and you can be instantly notified of potential security issues.

features

- Monitors for the arrival of different types of journal entries in the system audit journal QAUDJRN
- Comprehensive journal filters can be set up to ignore unimportant entries whilst quickly alerting you to important entries of which you need to be made aware
- Substitution variables can be used to pass variable information for easy and accurate command execution
- An unlimited number of actions can be performed in any pre-defined sequence when your selected journal entries are received by the system
- Further option allows action to be taken only after a pre-requisite number of entries have been logged
- Escalating actions can be defined to draw your attention to critical events
- Actions include executing commands, calling programs, sending a text message to a pager or mobile phone, writing a record to an external log file etc.
- Messages can be sent directly into the Halcyon Enterprise Console when a graphical centralised management tool is required
- Messages can be sent out to mobile phones and pagers using the Halcyon Message Communicator
- Includes full diagnostics and audit trail

Analyse and monitor changes made to user profiles - this could be a change made to a user's special authority, user class or limited capabilities. You might want to know if someone changed their authority to *SECADM for example.

Quickly detect when invalid attempts are made to signon - especially if this happens to be QSECOFR.

Changes to system values can be tracked and traced as these can have significant impact on areas of security and system performance.

Be informed when sensitive objects (such as the Payroll file) are created, deleted, restored, moved, renamed or the ownership to that object or access rights are changed.

Authority failures can be detected and brought to someone's immediate attention. For example, a user might be attempting to access an object they are not authorised to, such as the Supplier master file.

Keep your Auditors happy by monitoring for programs that are changed to adopt authority - keep all those "back doors" closed.

Monitor and log when spool files are read, created, deleted, held, released or the security attributes are changed.

Keep an eye on user profile swapping and be kept informed about what is happening on your system.

Know when users connect and disconnect through FTP.

Command string audit - monitor for when security related commands are executed or commands are issued by a specific user or job.

Actions regarding Jobs can be monitored - for example, when jobs are submitted, changed, ended, held etc.

"We find the Halcyon Audit Journal Monitor very easy to use and extremely useful."

The audit log generated by the system is very large and manually looking for particular events is not easy, especially when managing multiple servers.

By using the Halcyon Audit Journal Monitor to proactively monitor and report events to the Halcyon Enterprise Console, we can see exactly when a monitored incident occurs and take appropriate action."

GE Mettorell

Gary Metherell
Manager
Managed Services
REAL Solutions UK



Halcyon Software Ltd
5 The Forum, Minerva Business Park
Lynchwood
Peterborough
PE2 6FT
England

Tel: +44 1733 234995
Fax: +44 1733 234994
Email: sales@halcyonsoftware.com

IBM and iSeries are registered trademarks of International Business Machines.

download a **FREE** trial at www.halcyonsoftware.com