

# CCSS NEWS AND UPDATES

Pro-Active Systems Management Solutions for the iSeries

JULY 05

ISSUE 12



## COMPANY NEWS

### QSystem Monitor helps storm water pump manufacturer meet ISO 9001 and SOX standards

ITT Flygt recently had to re-certify its ISO 9001 accreditations; QSystem Monitor was an important tool for Eric Larmier, Director of Information Systems, Nanterre, France. "The one-screen display dashboard is fully part of managing and controlling our iSeries infrastructure. As such, it is included in all of our ISO procedures and is part of our ongoing quality assurance" Larmier explains. "QSystem Monitor delivers indicators that show that the information systems infrastructure is mastered by the IT department."

[Click here for full details](#)

### Sarbanes-Oxley provides the opportunity to get the most out of your iSeries

The strict internal control and audit requirements of the Sarbanes-Oxley Act may very well be helping CIOs better manage their iSeries. "Sarbanes-Oxley illustrates what pro-active IT managers have always known. Effective systems management is more than a 'best practice' aspiration, it's the critical foundation that will determine the success of the entire organization," says Ray Wright, Managing Director of CCSS, which develops and markets the QSystems Management Suite of IBM iSeries monitoring software.

[Click here for full details](#)

### Now Available ...

You can now benefit from having direct access to Part I and Part II of **The Art of Security Audit Journal Maintenance** articles, to view previous issues of our '**Latest News and Updates**', please visit our website at <http://www.ccsstld.com/news/newsletters.html>

## TECHNICAL TIP

### The Art of Security Audit Journal Maintenance - Part III

*By Kurt Thomas*

In Part II of The Art of Security Audit Journal Maintenance, I introduced you to the basic concepts of Audit Journal filtering. We'll now continue by discussing the more complex case, filtering based on message content.

Here's the table from Part II again:

MSG ID	Occurrences	Description
UCA0001	668,169	Authority to &10/&9 &11 granted for user &12.
UCA0002	293,864	Authority to &10/&9 &11 replaced for user &12.

UDQ0001	176,163	Object Deletion - &10/&9 &11.
...	...	...
UPS0016	6	Profile Swap: Token has been generated for user &9.
UVP0016	2	Network Password Error at server &9 for user &13 on computer &12.
UPS1008	1	User &9 is using Management Central.

You can see that the table contains the message "Authority to &10/&9 &11 granted for user &12." If you were to display this Journal entry as a message every time, your Console would just fill with these. So by default, this should be filtered out.

However, there are times when you will be interested in this message. For instance, you may want to be alerted whenever objects in the library ACCTNG are being accessed by user SUSPECT. The distinguishing bits of information are contained in the message fields (message variables) here.

You cannot use Audit Journal Filters for this task, as they don't look at anything more detailed than the code of the Journal entry (message ID). Message fields are beyond them. For this to work, you need to: (a) not filter these messages with Audit Journal Filters, and then (b) set up Auto-Replies to filter based on message ID and message field contents.

If you need to determine which message field contains which kind of information -- this is different for different kinds of Journal entries -- then in the QMM PC Console, display the message properties, and compare the contents of the More and Help dialogs. The More dialog contains the raw message fields; the Help dialog, for Security Audit Journal messages, contains the contents of the message fields, too, but with a speaking name. In More, it's "Message variable 2: MILLER" --- in Help, it's "User profile: MILLER".

Your task is to go through the table you generated for your system. Add a new column -- "Filter Action". If you are not the Security Officer for this system, I recommend you work closely with the Security officer on these steps. For each message ID, determine how you would like to filter it: no filtering, Audit Journal filters, or Auto-Replies. Don't try to be perfect the first time --- filter definition is an iterative process. Also, it will probably pay to revisit your filter settings every few months to determine whether they still match your requirements.

### "Engage Filters!"

You can set Audit Journal filters both in the PC Maintenance and in the iSeries software. In both, you can define filters based on the type of the Journal entry and the age of the Journal entry. (You can also filter by the message severity, but we'll leave that aside for the moment. The message severity does not exist before the Journal entry is converted to a message, so if you try to apply filtering before the conversion, it will disrupt the space-time continuum. Just kidding.)

In the PC Maintenance, you can find the Audit Journal Filters in the Advanced section, where Looping Jobs is, too. If it's not there, you need to update QMessage Monitor.

In the QMM iSeries menu, these Filters are in Menu 15 "Advanced", item 9 "Maintain: Audit Journal Filters".

In both cases, you can define Filters at a Default level, and at the level of individual systems, with the latter overriding the former.

The PC menu and the iSeries menu allow you to assign filters based on categories of entries (messages), in effect clustering several types of entries (messages) together. E.g., "AF" is the umbrella for all "Authority failure" messages.

Only on the iSeries menu can you additionally go down to the level of the individual Journal entry type (message ID) and assign filters there. So the iSeries software allows you to be more specific.

So much for today. You have done well. This three-part series has been extended to include a fourth installment. (Readers of Douglas Adams will recognize the concept.) In the final installment, your preparation will pay off. You will enable Security Audit Monitoring and get a whole new view of your system.

## **SHOW BUSINESS**

**Fall Common Expo - Sept 18-20 - Orlando, Florida**

<http://www.common.org/conferences/2005/fall/>

**Fall iSeries Technical Conference - Oct 17-21- Miami Beach, Florida**

<http://www-304.ibm.com/jct03001c/services/learning/ites.wss?pageType=page&c=a0000716>

Struggling with Sarbanes? Serious about Systems Availability? Desperate to tackle those Event Management issues? Stop by our booth at the forthcoming Technical Conference and COMMON shows and talk to the experts. Our team will be on hand to help resolve all the iSeries issues that are holding back system productivity, from routine daily operations to new security protocols and audit compliance agendas.

To book your demo in advance, please send an email with your preferred time and contact details to: [sales@ccssltd.com](mailto:sales@ccssltd.com)



<http://www.ccssltd.com>

© 2005. All Rights Reserved.