



Event Management

On the IBM System i (formerly the iSeries)

Event Management on the IBM System i

Why is there a need for Event Management?	3
Overview	3
Monitoring	3
Events	3
Strategy	4
How should we manage the events?	6
Methods	6
Strategy	6
What should we manage the events with?	8
Systems Management products from CCSS	9

Event Management on the IBM System i

Why is there a need for Event Management?

Overview

Regardless of whether your network consists of a single System i, multiple systems, physically separate or logically partitioned units, they will all have numerous message queues, containing a plethora of messages. If you now include the History Log (QHST) and the Audit Journal (QAUDJRN), both of which can also contain a huge amount of information, you will begin to see the enormity of the task ahead.

Finally, add into the equation your internal security policies, external auditing requirements (i.e. ISO 9000, Sarbanes-Oxley compliance or preparing for a Basel II implementation) and the task of managing all of this information can become quite a headache.

Has your business ever missed an important event? Without formalised event management, the truthful answer is probably “Yes”! Has a missed event ever had a detrimental or serious effect on your business (for example a system not being available for your users first thing in the morning)? Once again, the truthful answer will be yes.

Support staff could spend their time scouring the queues and logs for important messages, but that would not be a very cost effective use of their time or knowledge and will increase the likelihood that an important event will be missed.

Monitoring

The message queues and logs will serve different purposes and can be a part of the initial installation process:

- QSYSOPR, QSECOFR, QHST (*History Log*).

They can be created as your system grows or to meet specific auditing requirements:

- User Id, display devices, High Availability software, QAUDJRN (*Audit Journal*).

They can come as part of a new application or financial module being installed:

- ERP, CRM, SCM, Domino, MQSeries, Financial reporting.

Events

However, they will all have one thing in common. They can all contain a great deal of useful information that is not always easy to resolve from the rest of the day-to-day data.

Some of these events will be informational, but perhaps useful for auditing purposes:

- CPF1241 – Job &JOB completed normally on &DATE at &TIME.
- CPC0962 - Cleanup of job tables completed.
- User BENTT1 has logged on using FTP.
- Object PAYROLL/OWNBONUS *FILE created.

Some may be a warning of unwanted changes or future problems if unheeded:

- System value QHSTLOGSIZ changed to 0000065535.
- CPI0964 - Weak battery condition exists.
- CPC1123 - Subsystem &1 cannot start prestart job &2.

Event Management on the IBM System i

- *CPF1392 – Next not valid sign-on disables user profile.*

Some may require certain user or operator actions to be performed:

- *Instruct a System Operator to load an optical storage archive.*
- *CPA2087 - Load next volume on the installation device (C G).*
- *CPF1393 – Subsystem XXX disabled user profile YYY on*
- *Authority Failure: BENTT1 Not authorized to object QUSRSYS/PRT25 *OUTQ.*

Finally, in the worst case some will denote a program or system failure:

- *RPG0121 - RG0001 18400 array index is not valid (C G S D F).*
- *CPI0955 - System ASP unprotected storage limit exceeded.*

The next time you sign on to one of your systems, use the WRKMSGQ command to review the myriad number of message queues on your system. Then take a few moments to peruse some of the messages that have been sent to those queues. Now review the History Log (how many days worth of history do you keep on the system?) and look at some of the entries that appear. If you are using the Audit Journal (and if not, review the system value QAUDLVL help text to see what you are missing), review some of the entries at random.

You will begin to understand the size of the task if you wish to ensure that you do not miss that important message (be it system or application driven) and how many different tools you may need to use at the moment.

Strategy

Monitoring for all events from a single point of control allows an overall view of systems within the network and reduces the time taken to respond to urgent messages. This will also allow a common, structured approach to be defined.

Formalising your event management methodology will free up your Support staff allowing them to make better use of their time. Your staff can then be pro-active with regards to system threats instead of reacting after the event has occurred. Standard informational messages could be reviewed and simple filters can be created to ensure that these messages do not cloud the vision of your Support staff.

Now take a moment to look at your queues, logs and individual messages from a different perspective, from a "how can I use these events in a pro-active manner" point of view.

- *Do you have certain message queues or individual messages that could have authorisation rules applied to them?*

For example, a Purchase Ledger system may send a payments file off to your Bank, electronically. Messages to process this data are sent to a specific queue that only three named Users are authorised to access, but require different levels of authentication to complete the task. The first level could be for the Purchase Ledger Clerk to countersign the payments run as completed. The second level could be for a Financial Accountant to

Event Management on the IBM System i

sign off the amount to be paid from the company's account. The final response could be from the Operations staff to countersign that the file transfer has been completed.

Leaving that example behind, here are a few more suggestions to consider:

- *Would it be useful to have the ability to turn certain system or application events into inquiry messages, to force a response and capture when the message was responded to and by whom?*
- *Do you need to monitor for the fact that a certain job has not completed processing according to schedule, either in or out of normal working hours? Or, do you need to monitor for the fact that a certain job has started processing at a particular time?*
- *Each task on the operator's checklist could be created as an event. Thus all operator tasks (iSeries and others) could be electronically audited to comply with the company's new auditing requirements.*
- *Do you need to be warned when system values are amended?*
- *Is there a specific device that is critical should it fail (for example, the President's/MD's PC, or a communications line to Head Office)?*
- *Do you need to monitor whether a message has not been responded to within a given period of time and then notify some individual or contact a number of support staff, to escalate the situation?*
- *How about the ability to commence an automated function, without specifically notifying anyone?*
- *Do you want to track FTP usage across your network?*
- *Would the ability to intercept possible looping jobs before they cause a problem be useful?*
- *Do you wish to offer 24 x 7 support cover, without necessarily having to have staff on site, via pager, email or mobile phone?*
- *High Availability products generate a lot of messages, and right in the middle of one queue could be the message telling you that an object has been put "on hold", or a journal receiver is damaged. If the central system fails, switchover occurs and users then find that half their data may be missing.*
- *Would the ability to control which personnel can answer the messages and in what form that response should take, be important?*
- *Do you need to interface to an Enterprise Management Console within your organisation?*
- *Is there a requirement to transfer certain events via SNMP?*
- *Would you like the ability to perform certain additional actions to strengthen your existing security measures?*

Arrange a brainstorming session with other department managers within your organisation to ensure your individual and joint decisions support the overall objectives set for the business.

The above selection is not an exhaustive list by any means, but as you will quickly discover, the list of requirements might surprise you.

Event Management on the IBM System i

How should we manage the events?

Methods

The best method is to adopt a "management by exception" approach that allows an early warning of impending problems to be issued before a possible disaster occurs. This approach also filters out unimportant messages, provides a historical repository for investigation purposes and provides a single point of control for all of your queues, logs and user defined events. However, it is important to remember that a single point of control also creates a possible single point of failure, so address this issue by implementing a backup or switchover recovery option to cover this eventuality.

Ultimately, you must decide upon your own company's methodology, how you will implement it across your business and in the light of, for example - Sarbanes-Oxley, how you will justify that decision at a later date.

When all of the active jobs and devices, on all of the active systems within your network or networks are running normally and all of those jobs are completing without errors, there is no need to be informed of that fact every second, of every hour, of every day. However, the opposite scenario is also true. Having no warning of a problem before disaster strikes is equally useless, be it a serious disk storage problem or the unattended failure of an overnight routine to pay all of your suppliers.

The better method is to review the message queues and logs on your systems; decide which are critical to your business, which are important and which can be covered by the standard clean up rules. Then look at the additional business requirements that arose out of the brainstorming session, and decide how these need to be defined as events to be monitored.

The basic methodology will be similar for most businesses; however the list of specific requirements will differ between companies, and in some cases, between sites.

Take some time out to review the current practices and procedures across your business.

Strategy

Once you have your queue and log hierarchy arranged and a list of new items from your brainstorming session, start investigating the actual events and how you require them to be managed. Decide which events:

- Cannot be ignored and require positive action as soon as is possible.
- Do not yet exist but must be created.
- Which are critical for auditing purposes?
- Which are important, but not immediately time sensitive?
- Those that can have an automated response defined for them.
- Which are informational but important to note have occurred?
- Finally, those purely informational events that can be safely ignored.

Event Management on the IBM System i

At this time review whether any of your messages require further securing. Sensitive messages may need to be "hidden" from unauthorised staff. It may also be especially important for some of the messages not to be answered incorrectly. It may be desirable to control the responses that a particular User can provide to a message.

Certain events may require automated routines to be defined for them that can run before a situation gets critical, especially if you do not have manned Operations twenty-four hours a day, seven days a week. For example, on a "critical storage" condition message, a job could be started that will delete saved journal files, delete old spool files, clear test libraries, etc. Then this routine could send a message to a nominated support person on his mobile phone to inform him that a situation has arisen and pre-defined actions are being carried out. A response could then be sent from the mobile phone to initiate further action, or time is provided to allow remote access to be set-up.

Guarding against disks filling up unnecessarily in the event of a looping job could prove extremely useful. The ability to immediately detect looping jobs gives users the option to place the job on hold and swiftly resolve the problem before it creates any adverse impact upon the system's performance.

The ability to amend the level of response made to individual messages depending on shift patterns or personnel calendars could be useful. This would allow an earlier automation of response when the site is unmanned and a more manual escalation during manned hours, based on pre-defined service level agreements.

Tracking the success of business critical applications and, at a more detailed level, confirmation that key jobs have started or completed within a defined time frame, could significantly improve efficiency and eliminate time wasting.

The ability to monitor messages whilst a system is in a restricted state might be of paramount importance to your company, during certain scenarios (for example, during a system save or a PTF installation). This might also allow for cost reductions to be achieved across wide area networks.

Try to choose the strategy that will minimise the disruption to your staff and require the minimum level of staff training, both now and in the future. A phased approach can be taken to ensure that critical items are implemented first, important items second and then miscellaneous events planned in at a later date. Another good idea is to incorporate your existing company procedures into the event management process itself, to ensure that a common, already approved approach is taken to resolve any issues.

Finally, start to look for a product to automate as much of the process as is possible so your company's immediate and ongoing needs can be met with the minimum of fuss.

Event Management on the IBM System i

What should we manage the events with?

You have now reviewed your network and generated your list of monitoring requirements. You have also defined your strategy and are now looking for software to help you achieve your goal.

Of course, you could try to ensure that every piece of system operating code, internally produced programming code and every single third party application that you purchase contain all of the event management functionality incorporated within, but we all know that this approach is impractical and unachievable in the real world.

The better option is to purchase a solution that provides an intuitive approach and will wrap around your existing framework, future network growth and any unique business requirements you may have. It should use the latest technologies, with industry supplied APIs and incorporate Internet access.

The solution should allow the initial rules and filters to be built upon and developed, as your knowledge of your hardware and software develops and the complexity of your network grows, forcing additional controls to be added.

The software, as a minimum, should:

- Allow a common, structured approach to be taken across your network.
- Allow for time zone differences across a geographically diverse network.
- Allow the creation of escalation procedures that can warn staff before a critical condition causes a serious failure.
- Have the ability to incorporate business tasks as new events with ease.
- Be able to automate certain simple responses to negate the need to notify staff, e.g. by simply answering the message.
- Allow an automated response to be applied and then inform staff only when the escalation's command or program fails to alleviate the initial problem.
- Assist compliance with any corporate defined audit requirements.
- Detect looping jobs and optionally put them on hold.
- Incorporate shift patterns or calendars allowing for staff availability.
- Secure the product and your system from unauthorised sources.
- Ensure that High Availability software is running as expected.
- Interface with Enterprise Management Consoles.
- Provide a history of event, message and escalation activity for audit purposes.
- Provide audible warnings to be broadcast above the noise of a Computer Room.
- Allow Support staff to be contacted via email, pager, mobile phone or a combination (to allow best use of tariffs).

In summary, the application should do everything it can to help and support your business.

Event Management on the IBM System i

Systems Management products from CCSS

QMessage Monitor provides the total solution to System i Message and Event Management, eliminating the need for manual monitoring. Capable of filtering, answering and escalating messages and log entries or user-defined events, QMessage Monitor makes easy work of Event Management.

Automatic notification via audio, visual, email, pager or mobile phone allows staff to keep in touch with their systems whilst performing other tasks or outside of normal working hours. By restricting what an Operator sees to what the business regards as essential, you can reduce the chance of errors and manage all of your systems from one console.

QRemote Control brings benefits to those companies who value the ability to manage their systems, access application data, run commands and programs directly from their mobile phone, as well as simply receiving and replying to messages sent from the System i. Users benefit from the ability to access information and control multiple systems without the restrictions that come with onsite management.

Organisations can make use of this very flexible application to help them manage not only their systems management, but also business applications can be accessed via a mobile phone wherever their staff may happen to be, whenever they feel the need.

QSystem Monitor is designed specifically for the System i and produces a detailed overview of the status of systems across the network. Critical hardware and performance components can be measured and recorded. User defined events can also be configured and monitored. Historical data targets problems and allows staff to anticipate future requirements. System Managers can resolve recurring and existing problems throughout the network and support staff can detect and react to events on single or networked systems from a central console.

Thresholds can be created and linked to **QMessage Monitor**, to allow support staff to be notified via various methods, of potential system problems before they develop into fully-fledged disasters.

If you cannot monitor it, you cannot manage it.

Pro-active or re-active, let your Business choose!

For further information or customer stories on any of these products please visit the CCSS website <http://www.ccssltd.com>. Contact our sales or support staff via sales@ccssltd.com or support@ccssltd.com.