Operational Tools Case Study: Pro-Active Database Administration

How the deployment of an integrated alerting Tool was able to drastically reduce the overnight incident callout rate for database administration for a multi-national banking organisation, and lead to improved business processing.

The Challenge

Database Administration for a large multi-national investment bank is never easy. In the case of this particular company there were trading centres ranging from New York, London, Paris, to Singapore and Tokyo, which were all supported by the same centralised team. DBAs from this team worked on overnight callout shifts, usually one week in four.

Given the literally hundreds of servers which hosted the middle- and back-office infrastructure, each DBA on call expected to be paged several times every night. A typical overnight rota would involve as many as 25 or 30 calls during a week to deal with production incidents.

This type of reactive incident handling was very costly; not only in terms of manpower but also in terms of the impact on business processing which had to be interrupted and/or re-run when incidents occurred.

In summary, this was a classic case of IT Production “fire-fighting” when it was clear that there were significant underlying problems with the IT Production infrastructure that needed to be addressed.

Our Involvement

Although the organisation had a relatively mature post-incident analysis process for addressing overnight incidents, this frequently resulted in no actions being taken, since the necessary diagnostic tools were not in place.

In addition to the requirement for processes, there was clearly a need for suitable operational monitoring tool that could diagnose incidents pro-actively.

The ideal tool would not only report on underlying causes but also enable corrective action to be taken to prevent reoccurrence of incidents.

Based on our prior experience of software monitoring tools, we were given a free hand to implement a new Database Monitoring Tool into Production in order to realise the pro-active database administration that was required.

Approach

Fortunately, the company had already invested in a monitoring tool, although it had not been appropriately deployed, the customisation was not appropriate and it was not integrated with the company’s enterprise-wide console. Consequently it was not being used in production.

We determined that the initial phase of this project should be to identify the key metrics that were needed in order to identify potential incidents. This involved detailed technical discussions with the resolving DBA team and Help desk team, to identify common incidents,

and their underlying technical causes. From this, a series of key technical metrics were created, which were our target monitoring set.

As with any complex enterprise-wide software product, there were features that were suitable for the specific requirements, and others were unavailable. So the next phase of the project involved using a combination of “native” features and customised add-ons to configure the tool to monitor the metrics set we had defined.

During this phase, a lot of attention was paid to how to deploy the tool in production so that it would scale to lots of supported servers, many with multiple databases, and how the command server should be scaled. Assistance was sought from the vendor and user groups about how to scale the tool to support the hundreds of systems that would be monitored.

The third phase of the project involved integration of the tool with the enterprise-wide console, using SNMP traps to alert the operations team. We also designed and deployed a new web-based front-end to the command server, which enabled DBAs and Operations teams to view the status of potential alerts.

Having created the solution, the key to getting DBA and Operations “buy-in” was to pilot it on a selected few systems, backed up by further training and involvement. Since these teams had already been involved in the early stages of design, defining metrics, thresholds etc. they became more committed to the final solution.

A pilot deployment enabled us to adjust threshold levels, as well as the way alerts were generated, so that the appropriate level of alerting was given, and sufficient advance warning was given for corrective action.

The pilot deployment ultimately spent many weeks “dry running” the monitoring tool, until DBAs became convinced that the tool would not generate spurious call-outs, but would enable genuine pro-active action to be taken.

The product was eventually deployed on hundreds of servers world-wide, integrated into the centralised console system.

Benefits

The new monitoring tool immediately began to demonstrate significant benefits both for the business and for the DBA and support teams.

During the few months following deployment, the number of support calls in a typical shift week fell from 25 or 30 to only two or three.

Not only that, but the pro-active nature of the tool enabled corrective action to be taken to prevent business loss. One striking example of this was in early July when a USA-based server triggered pro-active alerts that indicated that a serious incident was likely to occur in the next couple of days.

Armed with this information, the UK teams arranged for the server to be taken out of commission on 4 July (a non-trading day in the US), to address the problem, and reinstated for the following day. Consequently, all work could be done in normal UK business hours and the bank experienced no computer outage.

Further Information

Dennis Adams Associates does not disclose any client names, details, or any commercially sensitive data with third parties.

For further enquiries, please contact us via our web site at **http://www.dennisadams.co.uk** or email to **info@dennisadams.co.uk**.