Preemptive Strike

Did the canary pass out?

By Pete Warchol, Siemens Healthcare
http://www.linkedin.com/in/warchol

In the World of IT support, there are two major areas: reactive support and proactive support.

Before I go into these topics, I want to discuss a bit of history. My friend and Siemens colleague, Don Brenner, often sites that in a bygone time, miners used to bring canaries down into the mines. They did this because the small birds would pass out from the dangerous odorless gases long before the miners would become aware of their presence.

For reactive support, the customer is usually already aware of an issue. Something like a URL has stopped responding, they can't log on, or the system is running very slowly. In this scenario, the system has already died!

For proactive support, the customer should not become aware of an issue at all. Behind the scenes, the IT staff received system feedback that allowed them to fix the issue before it reached critical mass. In this instance, the canary has only gotten light headed!

Here are some methods in use today, to tell if the canary is getting woozy:

- Trending/deltas/standard deviations – observing normal behavior and deviations from the norm may give you a clue that something is about to go wrong.
- Thresholds – predetermining the maximum or minimum acceptable value based on experience or product limits, then triggering a warning as that value is being approached.
- Matrix of events – determining, based on experience, when a <u>concurrence</u> of events points to a potential issue.
- Pattern of events – determining, based on experience, when a <u>sequence</u> of events points to a potential issue.

Here are some implementations in use today:

- Early warning system (yellow versus red) – most system monitoring systems have defined what metrics can be watched to determine a degradation in the systems health.
- Predictive failure alert (PFA) – many hardware and software systems are delivered with PFA already built into their products, much like HAL in "2001: A Space Odyssey" predicting the 100% failure of the AE-35 unit within 72 hours.

The ultimate goals are:

- Knowing about it and, hopefully, addressing it before your customer detects it
- Forecasting so you can predict patterns of events instead of just responding to them
- Five nines – 99.999% availability or uptime

Obviously, this will not be accomplished by watching the systems manually. This level of support demands robust instrumentation and usually multiple automated solutions will be combined.

Now let's take the example of a web enabled Java application with a relational database which is SAN (storage area network) attached. This would require multiple solutions to monitor the overall and component health of the system.

Here is a list of possible ways to keep an eye on your system:

1. Overall performance – have a response time tool studying the web traffic and alerting when a break from the acceptable performance occurs.
2. Overall availability – have a tool that tells you if the system is responding to requests or not.
3. Web tier component health – a tool to monitor HTTP activity and alert as needed.
4. Application tier component health - a tool to monitor Java activity and alert as needed.
5. Database tier component health – a tool to monitor SQL activity and alert as needed.
6. Storage tier component health – a tool to measure storage transfer time and queuing and alert as needed.
7. Physical platform component health – tools to detect issues with servers, network switches, firewalls, and WAN connections.
8. Security health – antivirus solutions, intrusion detection solutions, and security auditing solutions.

There are a multitude of vendors out there and they blend their solutions in a limitless number of ways. So, how you mix and match the tools will depend on your budget and the financial importance of a given system to your business.

Let the canaries pass out, instead of letting your system die!

About the author

Pete Warchol has been in the Information Technology industry for more than 20 years. He has held many different roles, spanning software development, business analysis, project management, staff management, systems administration, systems security analysis, and most recently, systems performance analysis. He has earned more than 80 professional certifications, including MCITP (Microsoft), CPHIMS (HIMSS), VCP (VMware), CCA (Citrix), ASE (HP), CATE (IBM), Security+ (CompTIA), and CEH (EC-Council). He is employed by Siemens Healthcare and is a CMG Officer for the Philadelphia regional group (http://regions.cmg.org/regions/phcmg/index.html).