



Better Monitoring with WebWatchBot Series

Monitoring Failures: Introduction

In the world of website monitoring and server monitoring, failures are well known and cover a wide spectrum of undesirable events. Specifically, there are two categories of failures: planned and unplanned. Unplanned failures have two sub-categories: hardware failures and software failures.

Hardware failures can manifest themselves as software failures but are detected in different ways. Slow disk reads can mean a hardware problem, dropped packets can indicate a network problem, and random crashes and reboots can mean faulty memory.

Software failures can cause much frustration with cryptic error messages or mysterious and unreported failures. A bug in software can appear at any time and cause outages that repeat based on events or other software interacting on the same machine.

The importance of defining failures is one that leads to a monitoring strategy of identifying when to be notified in order to take corrective action. There is little argument that hardware failures should always trigger notification, so that corrective action can be taken immediately. Software failures are not so cut-and-dry.

Take for example, a website that occasionally – once a week - produces an HTTP 500 “Internal Server Error”. Since the error only appears once a week, it is prudent to investigate the cause of the error, but it is certainly not time critical.

If the same web server and web page were to suddenly produce an HTTP 301 “Redirect”, with a location of an entirely different website, it would be imperative to investigate immediately.

The bottom line on failures is that a policy of what constitutes failures and the prioritization of the severity of those failures should be discussed and put into place in every organization to ensure a solid monitoring strategy.