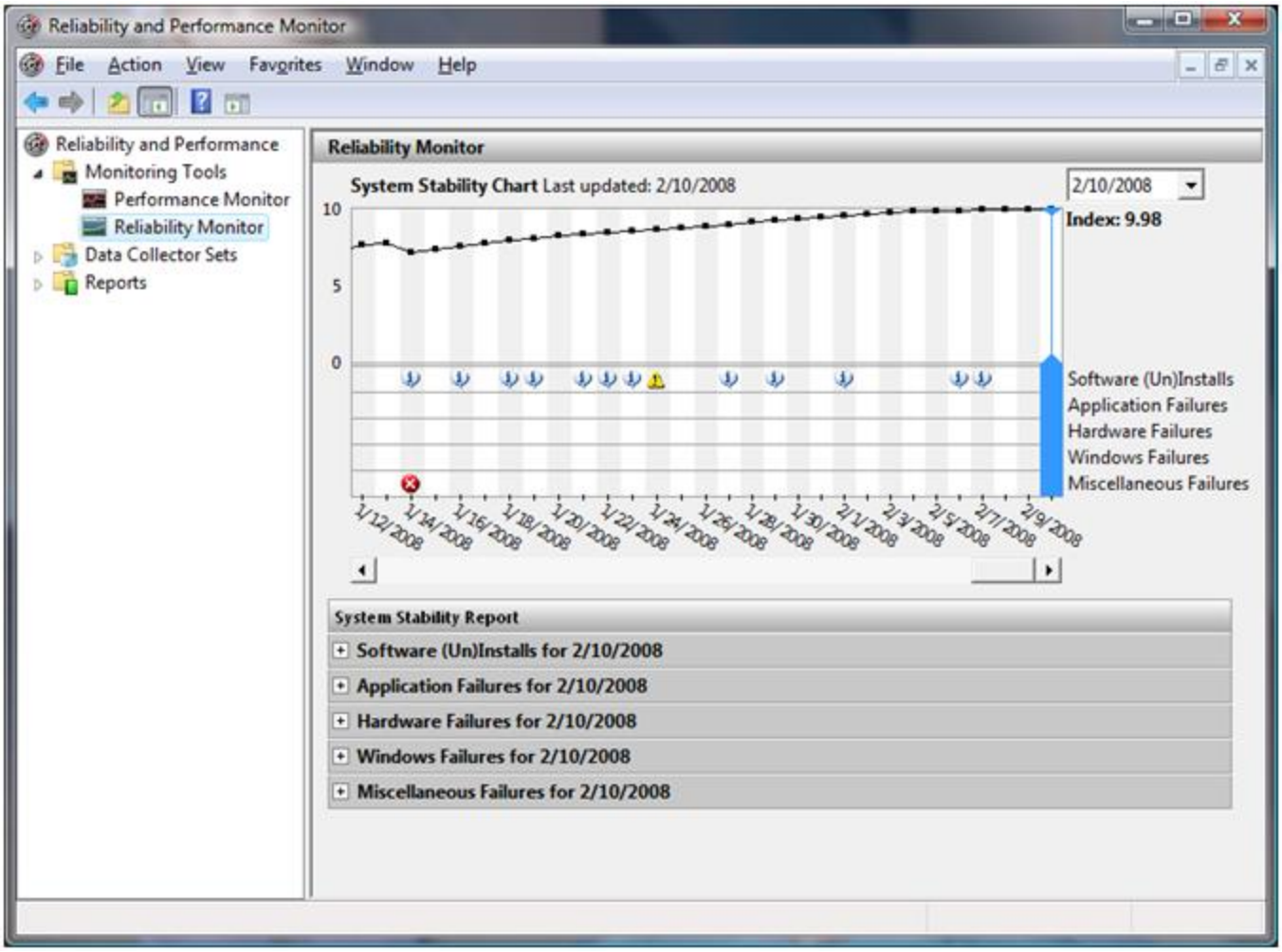
RELIABILITY MONITOR

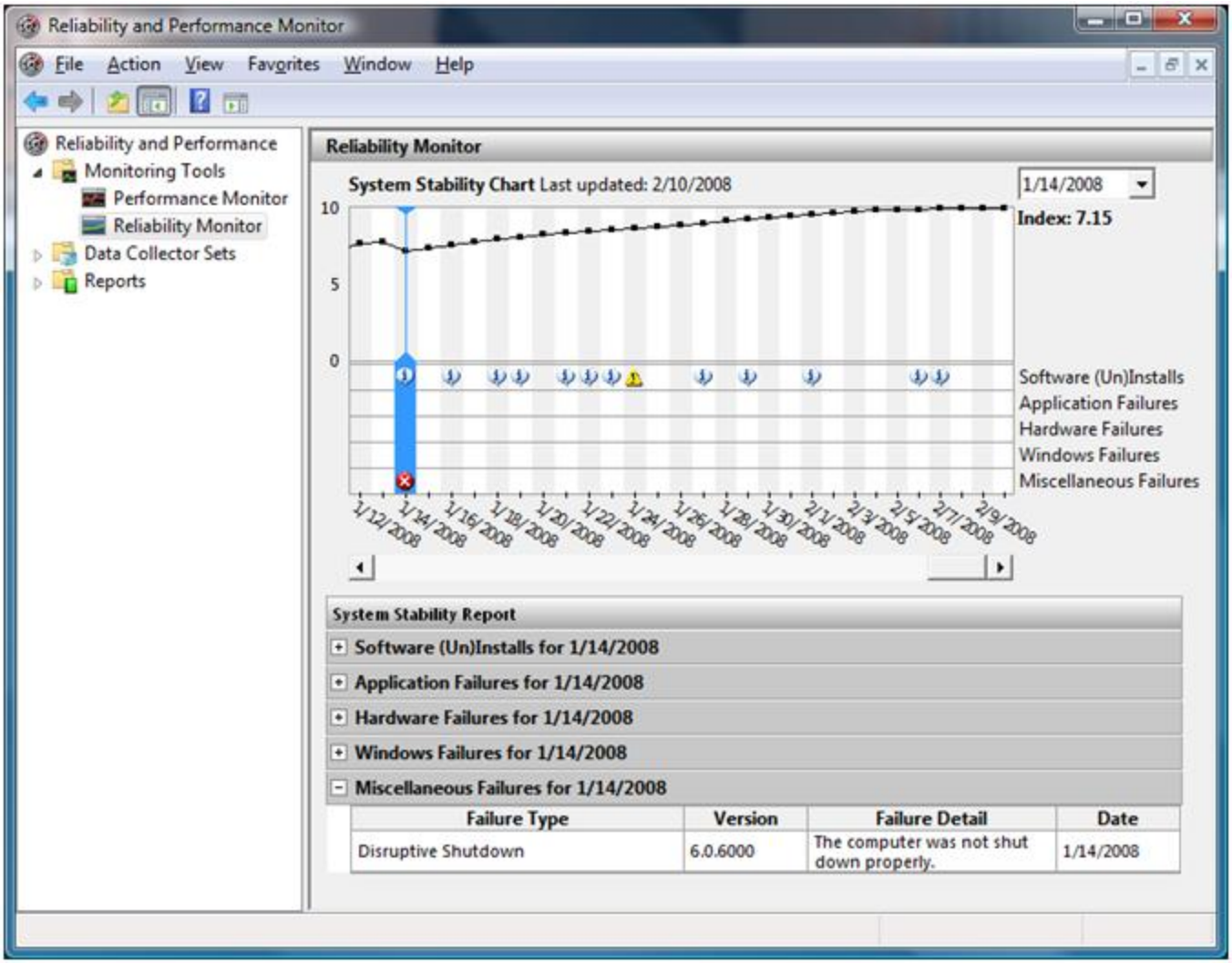
Reliability Monitor provides a quick view of how stability the system has been. In addition, it tracks events that will help you identify what causes reductions in reliability. By recording not only failures (including memory, hard disk, application, and operating system failures), but also key events regarding the configuration of your system (including the installation of new applications and operating system updates), you can see a timeline of changes in both the system and reliability. The reliability monitor also allows you to identify how to get your system back to optimal reliability when the behavior of the system is not behaving as expected.

You can start the Reliability Monitor by running perfmon.msc from the Run line or add it as an MMC Snap-in. When you launch Perfmon.msc, click Reliability Monitor under Monitoring Tools. The longer a system has been in use the more data is recorded and used to determine the system's overall health Index value. An important note here: the Reliability Monitor collects 24 hours of data before it calculates the System Stability Index or generates the System Stability Report. Let's now take a look at some scenarios involving the Reliability Monitor:

As you can see in the below screen shot, my system had an issue back on 1/14/2008:



When I click the Red X, my system informs me that it had a Disruptive Shutdown on this date:



In the days following the event on the 14th, my system's Index gradually increased (see the Index value under the date in the upper left-hand corner). This is obviously good news for me and the health of my system. Looking at this in a real world scenario, we receive calls every day stating that a server and / or workstation started having "Issues" after applying the latest set of Security Updates. Using the Reliability Monitor tool, we can check the history of these updates and determine if in fact the machine did or did not start experiencing a problem before the updates were applied. We often receive calls where an issue started to occur following the installation of security updates and subsequent reboot. The truth in many of these cases is that it was the reboot itself triggered the problems, and not the security updates. That does not mean we don't verify that the problem was not caused by the security updates, however it is crucial to remember that if you have not rebooted a system in a while, there are changes that may have been made to a system that could have caused issues. A classic example of this is uninstalling a piece of software that has a filter driver that starts up at system boot time (such as older backup software). If the filter driver is still referenced in the registry, but the driver itself has been removed from the system, the next time the server reboots, you are more than likely going to experience a STOP 0x7B bugcheck (Inaccessible Boot Device).

Let’s say your computer has been crashing for the past 2 weeks, but you are not sure what you did to make it start crashing. While looking at the Reliability Monitor, you discover that there were no crashes prior to 2 weeks ago. The day before the crashes started, the anti-virus drivers were updated. It’s safe to say at this point that this anti-virus update is the most likely suspect and caused your computer crashes.