

Election Webserver Incident 11/5/19

Incident: Shortly after 8pm on 11/5/2019 we were notified of our County website being unresponsive.

Response: We immediately contacted our network admin team and started gathering information. We found that the CPU usage on our webserver was hovering between 98% and 100%. The cause of the high usage was an IIS (Internet Information Services) Worker process that handles all of the incoming requests to our website. The webserver was rebooted in an attempt to reset all of the incoming website requests. Immediately after coming back online, the same process brought the CPU usage back to near 100%. Again, the server was taken offline and rebooted to add more memory in hopes to alleviate some of the stress off of the CPU. Once again, the CPU process returned to near 100%. At this same time, we were investigating the firewall to look at all of the incoming traffic and were able to rule out any type of denial of service attack. In order to gain access to the webserver and upload the election results, we decided to close all incoming connections to the webserver on the firewall. This dropped the CPU usage to minimal levels of 5%-10%. At this same time, a redirect of www.davisvotes.com was made to point to the Clerk-Auditor's Facebook page where election results were posted. Once both actions were complete, we opened outside access to our firewall once again. A short time after, we removed the redirect of www.davisvotes.com and pointed it again to our county webserver. CPU usage never reached the same debilitating levels.

*** See the attached Analytics Chart showing the timeline of these actions and the effects on CPU usage.

Post Incident Activity: In the hours that followed the incident, we continued gathering information.

- Our firewall logged 2,142 unique IP address visits from 8pm to 10:20pm. (This doesn't take into consideration for multiple attempts per each user/ IP address)
- Our webserver logged 53,687 requests from 7:45pm to 8:30pm.

We started performing stress tests on a non-production server with the same resources and settings as our production server. We performed many tests and found we were repeatedly able to recreate the same symptoms of the incident by simulating a high number of users to the election results page in a short amount of time. (250 users/visits per 10 seconds) Conversely, we found that other pages on the Clerk-Auditor election page were able to support the high volume of traffic in a short time span. We determined the election results page was able to handle a high number of users if the number of incoming users are spread out over a more extended period of time. (1000 users/visits per 10 minutes)

In further testing of the elections-results webpage, we found a tab offering the Prior Year results of the last 100 years of elections to be the primary cause of the resource strain on the CPU. When the content of the Prior Year results were removed, we again stress-tested the webserver and found it was easily able to handle 500 users/visits per 1 second. A significant turnaround in

performance. It was determined the file containing the last 100 years of election results was added in the March/April timeframe of 2019. In previous election years, the past 15 years of results were available on the election results page.

Future Procedural Changes: We have learned many things from this incident that we can use for future elections.

- We will break out the Prior Results data to its own stand-alone webpage.
- Prior to any future election, we will simulate stress tests to confirm our webserver will be able to accommodate expected and unexpected traffic loads. We will restrict uploads of any additional content in the window prior to the election and after stress testing.
- Additional measures and plans will be in place prior to the next election, but are not shared in this document due to security concerns.

Analytics chart showing CPU Usage time for webserver “WWW” on November 5, 2019 to current.

Figure a.

The CPU usage spikes to near 100% for the first time approximately 8:00pm.

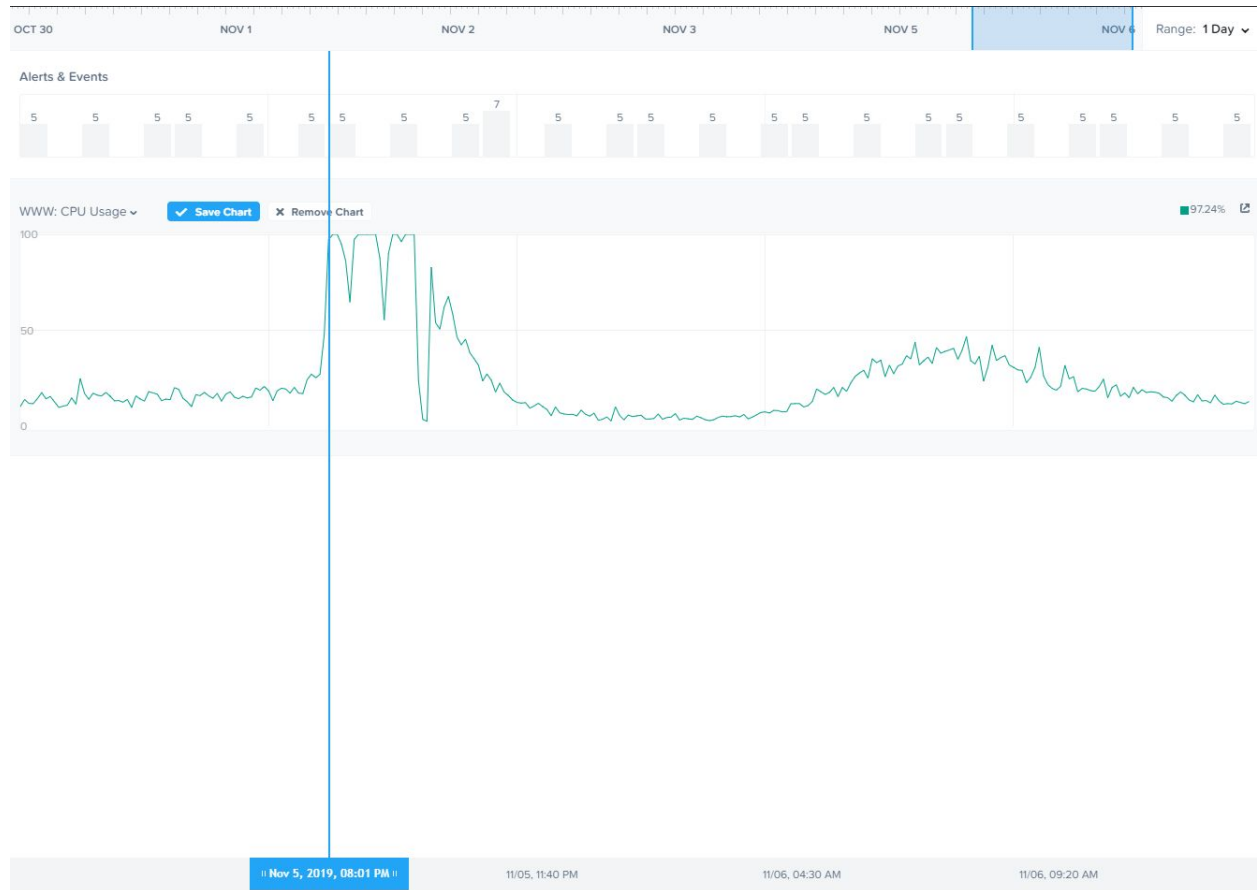


Figure b.

Webserver is rebooted at approx. 8:26 in attempt to terminate IIS Worker Process that has maxed out CPU. Notice the small dip in usage that immediately spikes after the webserver returns online.



Figure c.

Webserver is again rebooted at approx 9:05pm. The purpose of this reboot is too add more memory in an attempt to alleviate the CPU pressure. Again, the usage spikes after coming online.

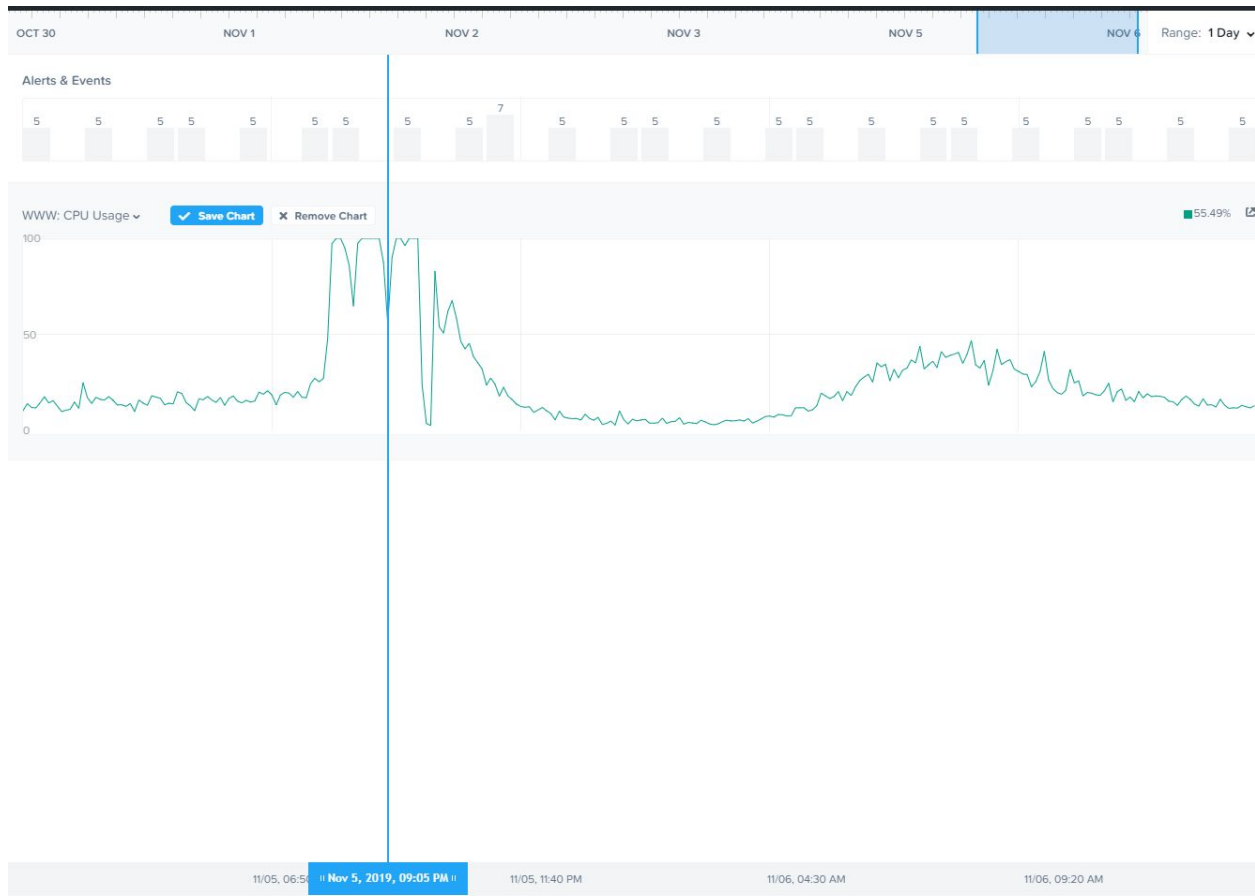


Figure d.

Approximately 9:50pm access to the webserver from outside the Davis County network has been closed on the firewall. CPU resource usage dropped below 5%. The webpage responded appropriately and allowed election results to be uploaded. During this time, a redirect of "www.davisvotes.com" was pointed to the clerk auditor's facebook page.

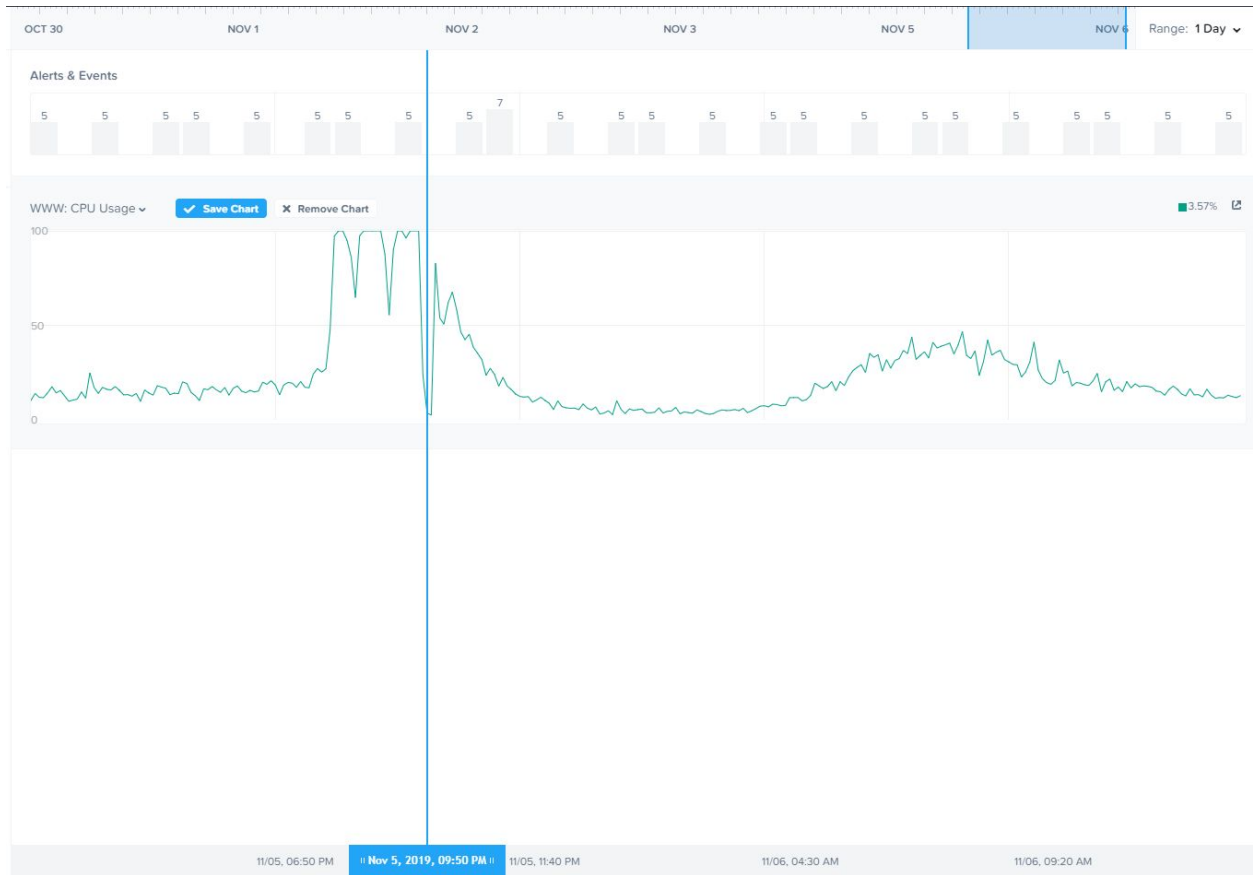


Figure e.
Approx. 10pm, outside access to the webserver has been restored. CPU usage climbs but never fully maxes out again.

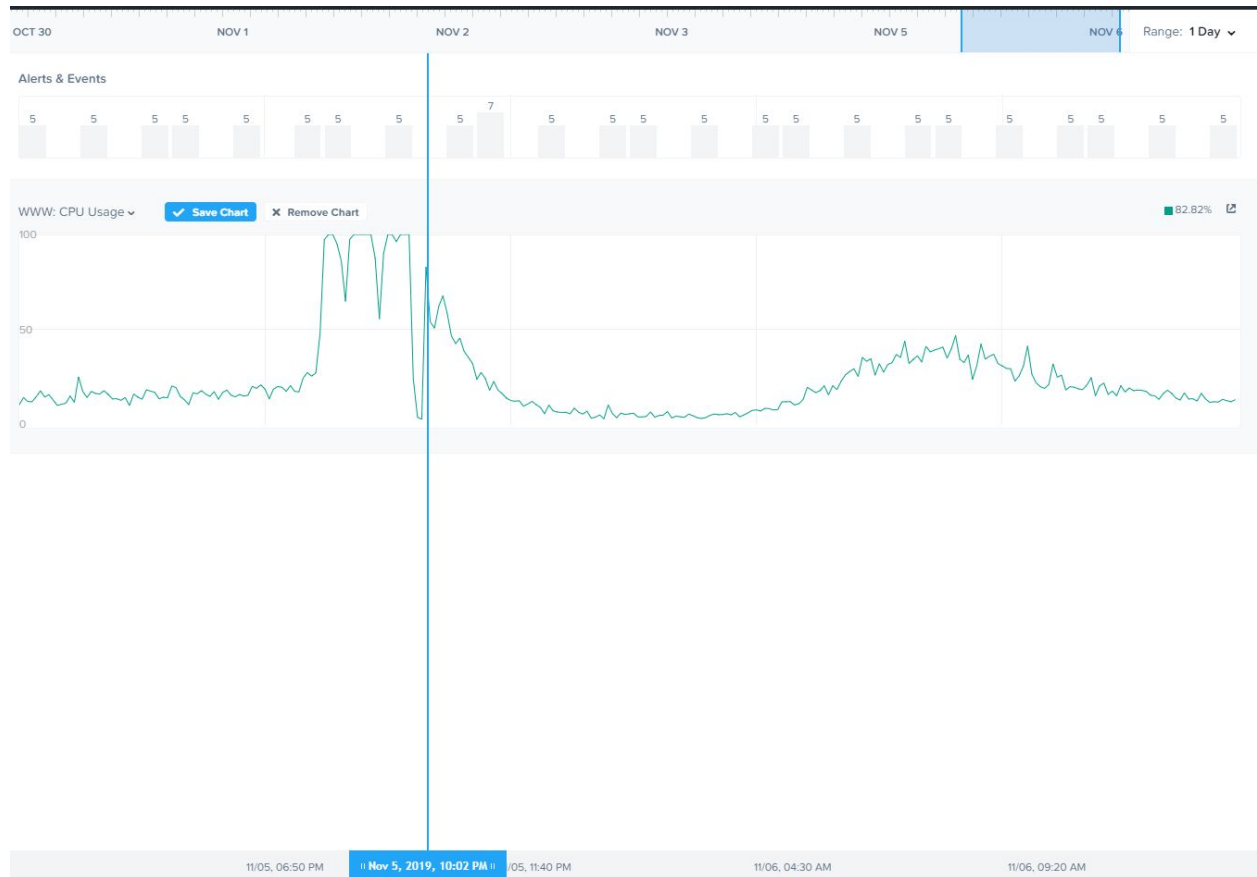


Figure f.

Approx 10:20 pm the redirect of www.davisvotes.com to Facebook has been removed. Once again www.davisvotes.com is linking to the Webserver.

