Managing web server performance

You work for a large retailer that relies on Apache servers to support its ecommerce. Your organization is growing quickly and you have some concerns about your infrastructure and its ability to keep up with customer demand. You'd like to create some searches to monitor performance and be able to correlate that information with usage. You can use Splunk software to track page performance, including response codes and times, and to track user data, including geographic location and user activity. Alerts from Splunk can be used to signal conditions that require action on the part of the Web Server Administrator, such as troubleshooting or performance optimizations.

Data required

Web server data

How to use Splunk software for this use case

You can run many searches with Splunk software to manage a web server. Depending on what information you have available, you might find it useful to identify some or all of the following:

Website performance

- Top ten slowest web pages on a web server
- Long-term website performance trends
- Trends in web server response codes
- Web hosts with HTTP error status codes
- Synthetic checks for URL responses

User Activity

- Top five most common web browsers
- Long-term trends in web server user load
- Number of current users on a website
- Most common operating system and browser combination

Additional data points

- Distribution of web traffic across servers
- Web access and web error log correlation
- SSL certificates nearing expiration

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Results

To maximize their benefit, the how-to articles linked in the previous section likely need to tie into existing processes at your organization or become new standard processes. These processes commonly impact success with this use case:

- Dynamic web content comes from a combination of business logic and database tables. Monitoring the application server functions, such as log in, checkout, and form submission, as well as database performance, is necessary to get an end-to-end view of the responsible processes.
- Monitoring the infrastructure that supports the web and app servers to prevent additional problems that might affect the user experience with your web content. You might want to track metrics such as percent busy for compute and storage usage.
- Monitoring the quality of the content available on your websites. For example, are files up to date? Are broken links found and quickly corrected? Are the certificates current?

Measuring impact and benefit is critical to assessing the value of IT operations. The following are example metrics that can be useful to monitor when implementing this use case:

- Response time: A reduction in outliers for the time taken by a server to deliver content to the requesting client.
- Count: A reduction in error status codes.
- Performance: A reduction in performance problems correlated with user load.

Additional resources

This use case is also included in the IT Essentials Learn app, which provides more information about how to implement the use case successfully in your IT maturity journey. In addition, these Splunk resources might help you understand and implement this use case:

- Conf Talk: Addressing customer issues with Splunk
- Blog: Decoding IIS logs
- Blog: Launching websites rapidly, without compromise
- Tech Talk: Splunk Fundamentals: Working with web server data Part 1
- Tech Talk: Splunk Fundamentals: Working with web server data Part 2