Technical Disclosure Commons

Defensive Publications Series

December 21, 2018

VISUALIZATION FOR IDENTIFYING SERVICE RESPONSES

Wagesh Kulkarni

Rakesh Sharma

Hitesh Manwar

VISUALIZATION FOR IDENTIFYING SERVICE RESPONSES

AUTHORS:

Wagesh Kulkarni
Rakesh Sharma
Hitesh Manwar

ABSTRACT

A secure web gateway is a type of security solution that prevents unsecured traffic from entering an internal network of an organization. By translating static log data from a secure web gateway into a meaningful and sensible format, an end user may identify issues that may cause delayed responses from services. Incorporating a visualization of a health view of a system into web gateway software may provide clarity to end users. By binding logged data into five-minute intervals for a selected daily or weekly duration and displaying the data on a single screen, an end user may easily view the health of services.

DETAILED DESCRIPTION

Making sense out of service response logs may be a difficult process for end users requiring a high amount of expertise. Secure web gateway administrators may use command line interfaces to retrieve information about various system and network parameters in order to investigate services, determine if any service responses are encountering issues, and take preventive actions. However, such a trial-and-error approach can be cumbersome. Figure 1 illustrates an example of response times of various services running on a secure web gateway.

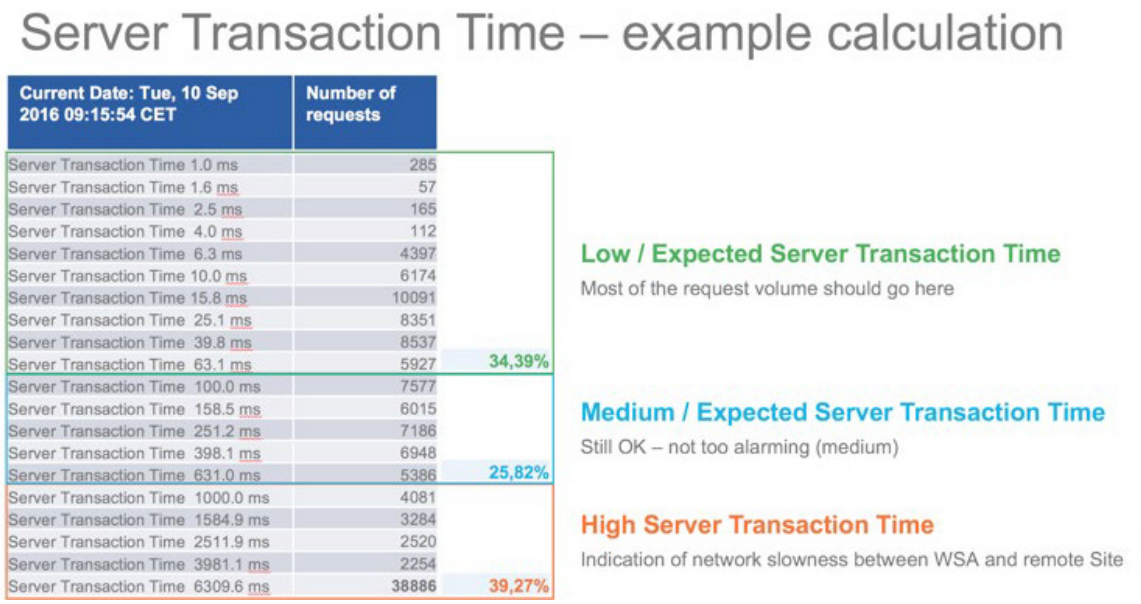

Figure 1

In Figure 1, a distribution of server transaction time is shown. This data may be extracted over a particular five-minute interval (e.g., on 10 September 2016, from 9:10 to 9:15 CET). Using this data, the number of requests that exceed the pre-defined thresholds may be evaluated. These thresholds are dependent on customer networks, and as such may lack a standard definition. To evaluate the health of server transaction times, an administrator may view, for example, the total percentage of transactions which were above 1000 ms. However, since the data represents a snapshot over a five-minute interval, an administrator will be unable to determine when the server began to encounter a delay. Thus, the administrator will be forced to review various five-minute snippets to arrive at a conclusion.

Figure 2, below, depicts an example of the transaction times represented in a histogram.

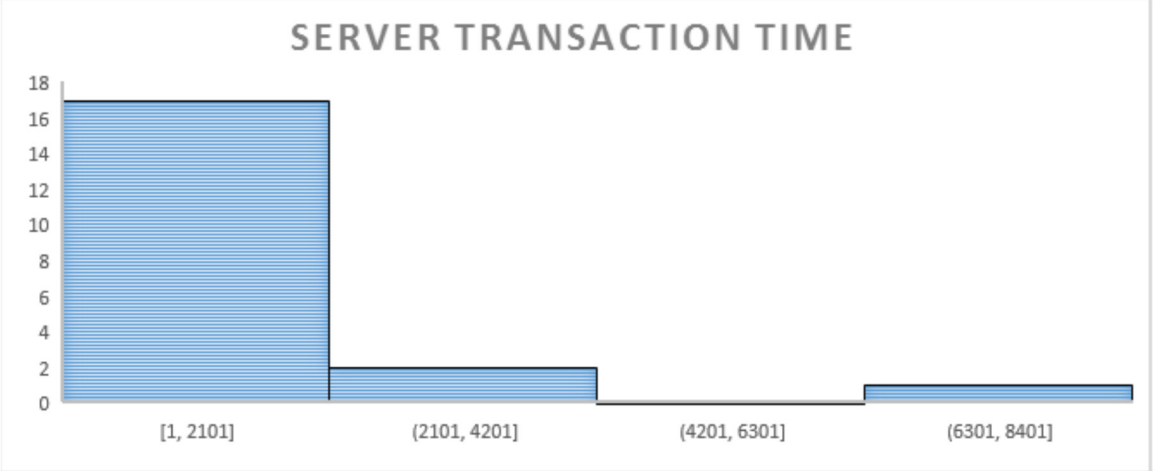

Figure 2

With histograms, the thresholds cannot be defined and diagnoses of the problem becomes even more difficult. Moreover, histograms are likewise unable to indicate when a server began to experience delays.

Embodiments presented herein translate static log data into a meaningful and sensible format that helps to gain an understanding of problems associated with services running in secure web gateway. Data sampled over five-minute intervals is consolidate and represented in the form of a heat map to indicate daily and weekly trends. The summary view contains a tabular view of all the service responses. The heat map view highlights a specific service if the service has exceeded a set threshold. The thresholds can be defined by an end user for both time as well as volume.

For example, for an authentication helper service, an administrator or customer may define a threshold using a rule such as “72% of the time, the authentication helper service response time should not exceed 1 second.” In the user interface, the volume quota enables an end user to define the threshold for total transaction percentage, while a moving indicator enables the end user to set the threshold for a specific service time bracket. A heat map may have four color definitions, such as light blue, dark blue, light red, and dark red. Figure 3, below, depicts an example color scheme in accordance with present embodiments.

Percentage of transactions	Color assigned
Less than 50% of the threshold value	Light blue
Greater than 50% of the threshold value, but less than the threshold	Dark blue
Less than 150% of the threshold value	Light red
Greater than 150% of the threshold value	Dark red

Figure 3

For example, assuming that the total domain name system (DNS) transactions in any five minute interval is 1000. If a threshold is selected such that 70% of the transactions should be below one second, then a total of 700 transactions should be less than one second in order to conclude that the DNS service time is healthy. Implementing a color scheme, if the total number of transaction times below one second is less than equal to 350 (50% of 700), the color assigned is light blue. If the total number of transaction times below one second is greater than 350 but less than 700, the color assigned is dark blue. If the total number of transaction times above one second is greater than 700, but less than 1050 (50% higher than 700), then light red is used. Finally, if the total number of transaction times above one second is greater than 1050, then a dark red color is used.

Figure 4, below, depicts a user interface in accordance with present embodiments.

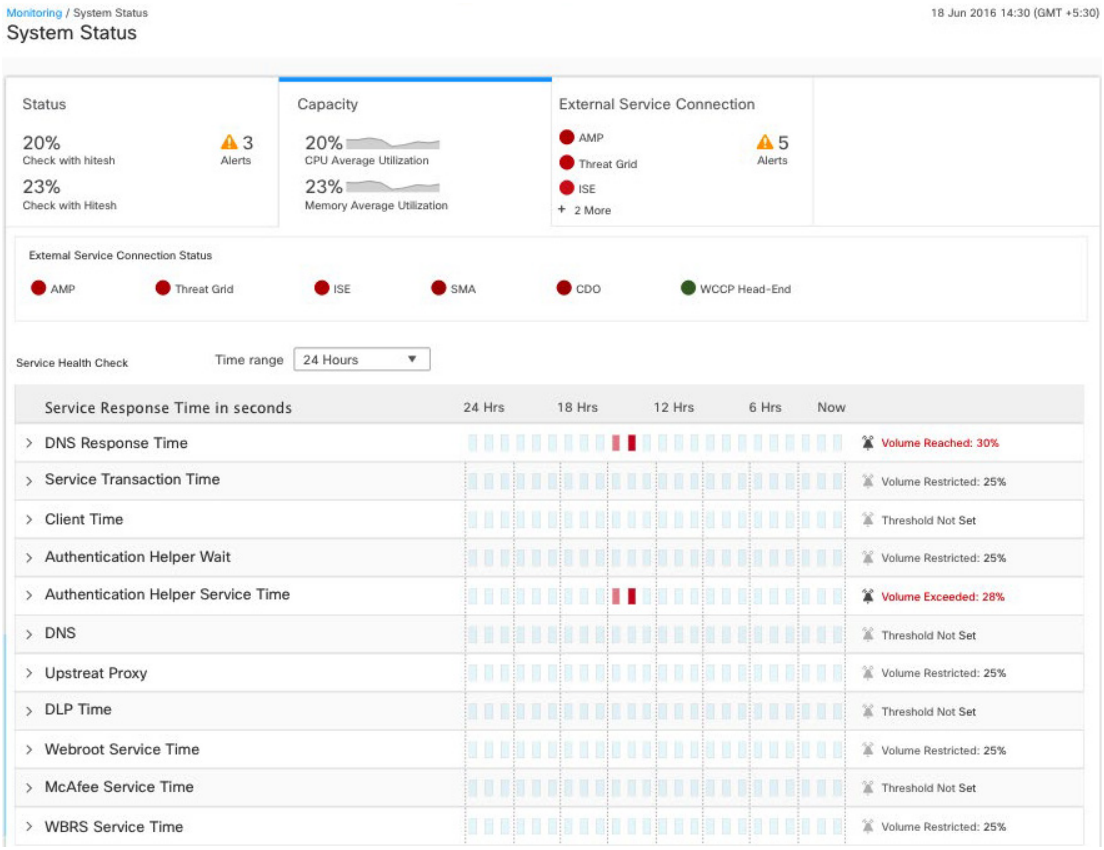

Figure 4

Figure 5, below, depicts a user interface in which details for the service "Authentication Helper Service Time" are expanded in accordance with present embodiments.

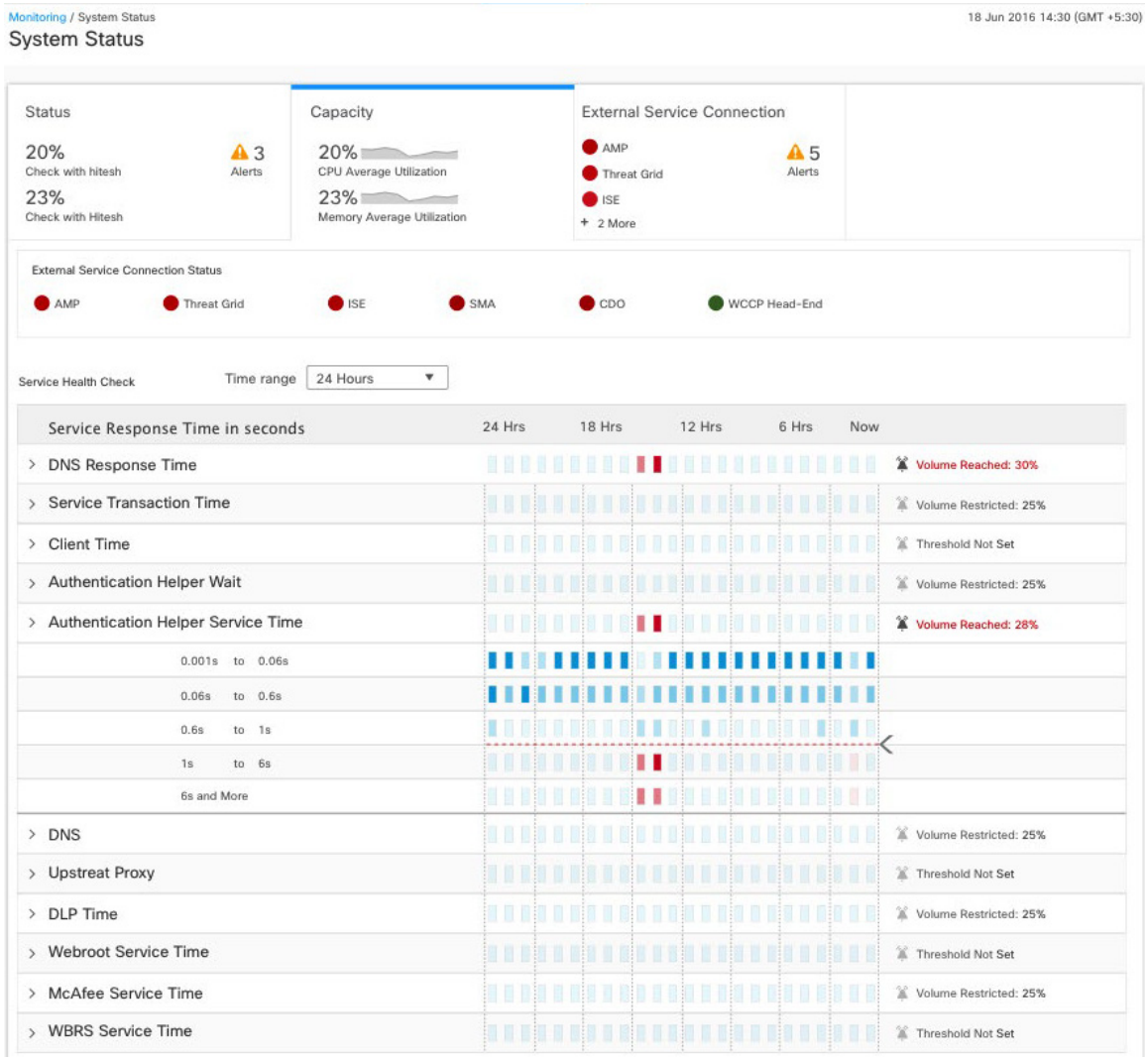

Figure 5

Figure 6, below, depicts a user interface in which further details for a time period are represented by a bar graph in accordance with present embodiments.

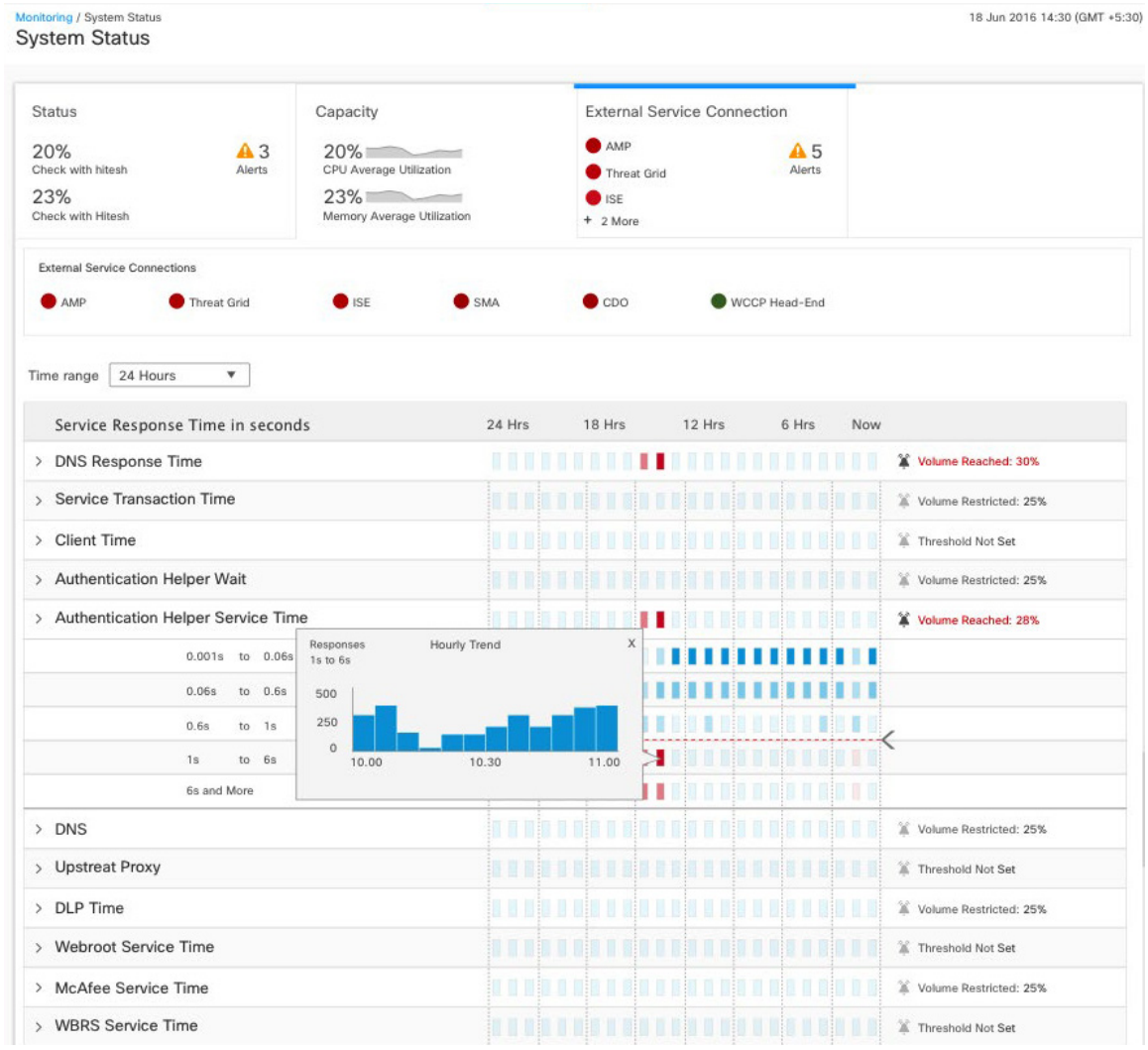

Figure 6

Figure 7, below, depicts a user interface in which a user may set or modify thresholds for service responses in accordance with present embodiments.

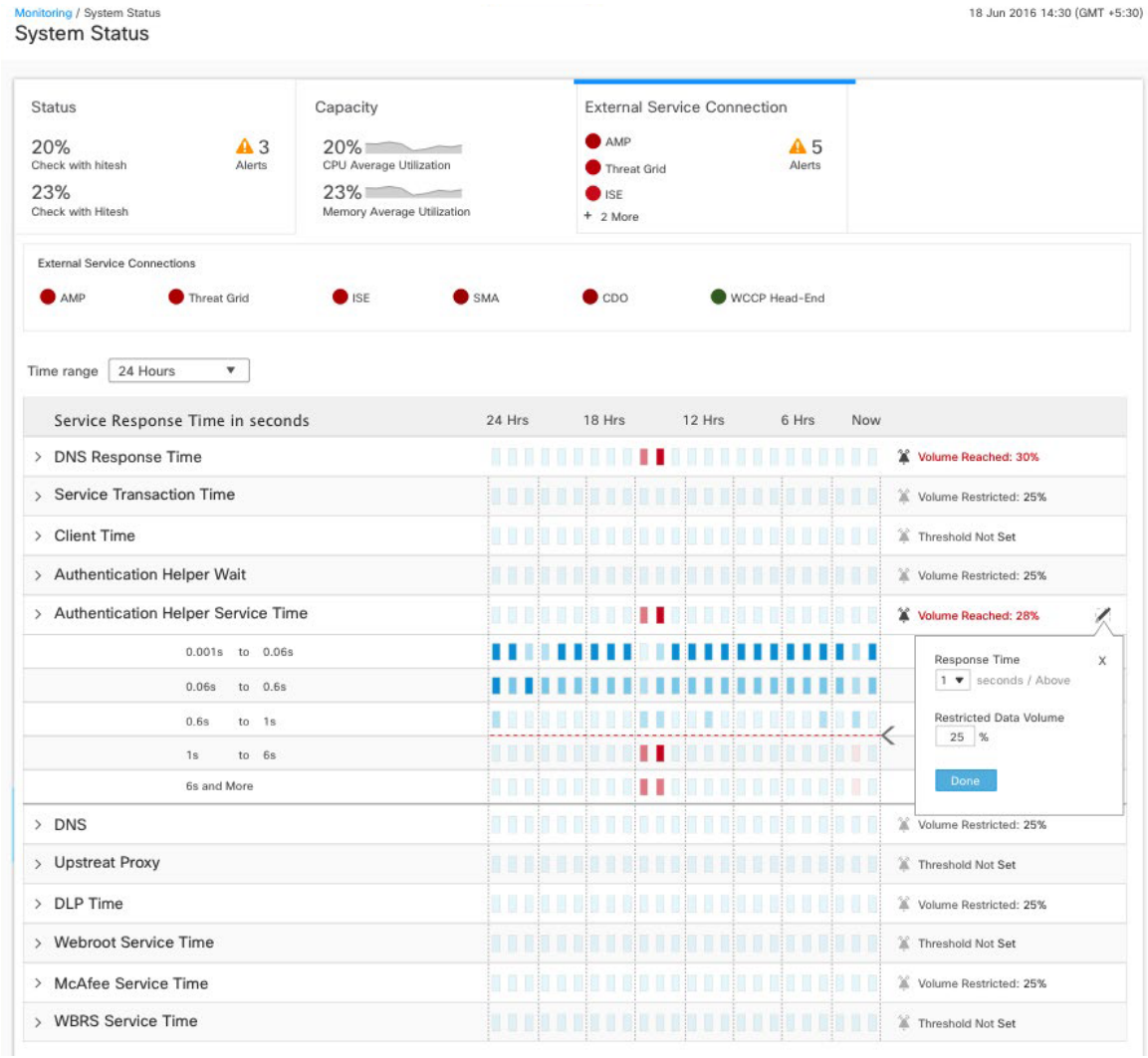

Figure 7