Technical Disclosure Commons

Defensive Publications Series

December 21, 2018

VISUALIZATION FOR IDENTIFYING SERVICE RESPONSES

Wagesh Kulkarni

Rakesh Sharma

Hitesh Manwar

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation

Kulkarni, Wagesh; Sharma, Rakesh; and Manwar, Hitesh, "VISUALIZATION FOR IDENTIFYING SERVICE RESPONSES", Technical Disclosure Commons, (December 21, 2018) https://www.tdcommons.org/dpubs_series/1812



This work is licensed under a Creative Commons Attribution 4.0 License. This Article is brought to you for free and open access by Technical Disclosure (

This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

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

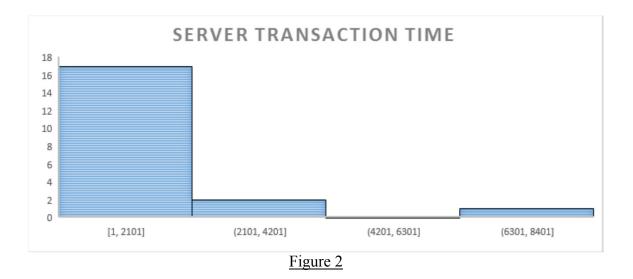
Making sense out of service response logs may be a difficult process for end users requiring a high amount of expertise. Secure web gateway administrators may use command line interfaces to retrieve information about various system and network parameters in order to investigate services, determine if 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.

Server Transaction Time – example calculation

Current Date: Tue, 10 Sep 2016 09:15:54 CET	Number of requests		
Server Transaction Time 1.0 ms	285		
Server Transaction Time 1.6 ms	57		
Server Transaction Time 2.5 ms	165		
Server Transaction Time 4.0 ms	112		
Server Transaction Time 6.3 ms	4397		Low / Expected Server Transaction Time
Server Transaction Time 10.0 ms	6174		
Server Transaction Time 15.8 ms	10091		Most of the request volume should go here
Server Transaction Time 25.1 ms	8351		
Server Transaction Time 39.8 ms	8537	and the second second	
Server Transaction Time 63.1 ms	5927	34,39%	
Server Transaction Time 100.0 ms	7577		
Server Transaction Time 158.5 ms	6015		Medium / Expected Server Transaction Time
Server Transaction Time 251.2 ms	7186		
Server Transaction Time 398.1 ms	6948		Still OK – not too alarming (medium)
Server Transaction Time 631.0 ms	5386	25,82%	
Server Transaction Time 1000.0 ms	4081		
Server Transaction Time 1584.9 ms	3284		High Server Transaction Time
Server Transaction Time 2511.9 ms	2520		-
Server Transaction Time 3981.1 ms	2254	142923	Indication of network slowness between WSA and remote Site
Server Transaction Time 6309.6 ms	38886	39,27%	

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.



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.

3

5753X

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.

atus Capacity			External S				
20% A 3 Check with hitesh Alerts 23% Check with Hitesh	20% CPU Average Utilization 23% Memory Average Utilization		AMP Threat Gr ISE + 2 More	rid	Alerts		
External Service Connection Status AMP Threat Grid	ISE I	SMA	• cdo	• wcc	P Head-End		
ervice Health Check Time rang	ge 24 Hours 🔻						
Service Response Time in secon	nds	24 Hrs	18 Hrs	12 Hrs	6 Hrs	Now	
> DNS Response Time							X Volume Reached: 30%
> Service Transaction Time							¥ Volume Restricted: 25%
							Volume Restricted: 25%
> Client Time							
 Client Time Authentication Helper Wait 	me						Threshold Not Set
 > Service Transaction Time > Client Time > Authentication Helper Wait > Authentication Helper Service Time > DNS 	me						 Threshold Not Set Volume Restricted: 25%
 > Client Time > Authentication Helper Wait > Authentication Helper Service Tir > DNS 	me						 Threshold Not Set Volume Restricted: 25% Volume Exceeded: 28%
 Client Time Authentication Helper Wait Authentication Helper Service Tir DNS Upstreat Proxy 	me						Threshold Not Set Volume Restricted: 25% Volume Exceeded: 28% Threshold Not Set
 Client Time Authentication Helper Wait Authentication Helper Service Tir DNS Upstreat Proxy DLP Time 	me						 Threshold Not Set Volume Restricted: 25% Volume Exceeded: 28% Threshold Not Set Volume Restricted: 25%
 > Client Time > Authentication Helper Wait > Authentication Helper Service Tir 	me						 Threshold Not Set Volume Restricted: 25% Volume Exceeded: 28% Threshold Not Set Volume Restricted: 25% Threshold Not Set

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

18 Jun 2016 14:30 (GMT +5:30)

Figure 4

5

Monitoring / System Status

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

nitoring / System Status /stem Status						18 Jun 2016 14:30 (GMT
Status Capacity		External Servi				
20% A 3 20% CPU Average CPU Av	ge Utilization	AMP	d	Alerts		
23% 23% Memory Av	verage Utilization	ISE + 2 More				
External Service Connection Status						
AMP Threat Grid ISE	SMA	• сро	• wcc	P Head-End		
ervice Health Check Time range 24 Hours	¥					
Service Response Time in seconds	24 Hrs	18 Hrs	12 Hrs	6 Hrs	Now	
> DNS Response Time						Volume Reached: 30%
> Service Transaction Time						¥ Volume Restricted: 25%
> Client Time						Threshold Not Set
> Authentication Helper Wait						¥ Volume Restricted: 25%
> Authentication Helper Service Time						Volume Reached: 28%
0.001s to 0.06s						
0.06s to 0.6s	1111					
0.6s to 1s						
1s to 6s						•
6s and More						
> DNS						¥ Volume Restricted: 25%
> Upstreat Proxy						Threshold Not Set
> DLP Time						Volume Restricted: 25%
> Webroot Service Time						🕌 Threshold Not Set
> McAfee Service Time						¥ Volume Restricted: 25%
> WBRS Service Time						Threshold Not Set

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.

nitoring / System Status /stem Status						18 Jun 2016 14:30 (GMT
Status 20% A 3 Check with hitesh 23%	Capacity 20% CPU Average Utilizatio 23% Memory Average Utiliz	-	External S AMP Threat Gri ISE + 2 More	ervice Connec	tion Alerts	
External Service Connections AMP Threat Grid	ISE ISE	SMA	е сро	• wcc	P Head-End	
me range 24 Hours 🔻						
Service Response Time in secor	nds	24 Hrs	18 Hrs	12 Hrs	6 Hrs	Now
DNS Response Time						Volume Reached: 30%
Service Transaction Time						Volume Restricted: 25%
Client Time						Threshold Not Set
Authentication Helper Wait						Volume Restricted: 25%
Authentication Helper Service Til	ne					Volume Reached: 28%
0.001s to 0.06 0.06s to 0.6s 0.6s to 1s 1s to 6s 6s and More	Responses He 1s to 6s 500 250 0 10.00	10.30	11.00 X			
DNS					0000	Volume Restricted: 25%
Upstreat Proxy						Threshold Not Set
DLP Time						Volume Restricted: 25%
Webroot Service Time						Threshold Not Set
McAfee Service Time						Volume Restricted: 25%
WBRS Service Time						Threshold Not Set

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.

Status	Capacity		External Se	ervice Connect	ion		
20% 🔺 3	20%			• AMP 🔺 5			
eck with hitesh Alerts CPU Average Utiliza		c.	 Threat Grid ISE 		Alerts		
Check with Hitesh	Average Utilization		+ 2 More				
External Service Connections							
AMP Threat Grid	ISE I	SMA	• сро	• WCCP	Head-End		
Fime range 24 Hours 🔻							
Service Response Time in seco	nds	24 Hrs	18 Hrs	12 Hrs	6 Hrs	Now	
> DNS Response Time							Volume Reached: 30%
> Service Transaction Time					n a n à l		Volume Restricted: 25%
> Client Time							Threshold Not Set
> Authentication Helper Wait		I I I I					Volume Restricted: 25%
> Authentication Helper Service T	ime					100 3	Volume Reached: 28%
0.001s to 0.0	ŝs						Response Time X
0.06s to 0.6	s						1 V seconds / Above
0.6s to 1s							Restricted Data Volume
1s to 6s							25 %
6s and More							Done
> DNS		1111			0000		Volume Restricted: 25%
> Upstreat Proxy							K Threshold Not Set
> DLP Time							Volume Restricted: 25%
> Webroot Service Time							Threshold Not Set
> McAfee Service Time							Volume Restricted: 25%

Figure 7