

Create regular expression filters in a chart

Published: 2017-11-16

Regular expression (regex) is supported in the Metric Explorer when drilling down for detail metrics. The following examples will help you create regex strings for filtering detail metrics keys, such as IP addresses.



Note: In the ExtraHop system, regex is most effective when you want to filter metric data by a parameter contained within the metric key, such as a number within any IP address. Regex is not effective for filtering for details by an exact match, such as filtering to specify an exact IP address.

Chart Scenario	Regex filter	How it works
Compare HTTP status codes 200 to 404.	<code>(200 404)</code>	Matches 200 and 404 codes where the symbol serves as an OR function.
Display all HTTP 400 and 500 error codes occurring on your network.	<code>^[45]</code>	Matches a 4 or 5 in the status code.
Display any IP address with a 187.	<code>187.</code>	Matches 1, 8, and 7 characters in the IP address.
Review all IP addresses containing 187.18.	<code>187\.18\.</code>	Matches 187 and the character . that follows the 187. For example, this filter returns results for 187.18.0.0.0, 180.187.0.0.0, or 187.180.0.0.0/16.
Display any IP address except 187.18.197.150.	<code>^(.?!187.18.197.150))*\$</code>	Matches anything except 187.18.197.150.