Create regular expression filters in a chart

Published: 2018-11-12

Regular expression (regex) is supported in the Metric Explorer and can be added to filter detail metrics in a chart. The examples in this topic show you how to create regex strings for filtering detail metric keys, such as status codes and IP addresses.

In the ExtraHop system, regex is most effective when you want to filter detail metric data by a parameter contained within the detail metric key, such as a number within any IP address. Regex is also effective for excluding specific keys from charts or displaying a specific combination of keys. Learn more about drilling down for detail metrics as you edit a chart ⬈.

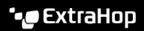| Chart Scenario	Regex filter	How it works
Compare HTTP status codes `200` to `404`.	`(200|404)`	Matches `200` and `404` codes where the `|` symbol serves as an OR function.
Display any HTTP status code that contains a `4`.	`[4]`	Matches any value that contains a `4`. For example, this filter can return `204` and `400` status codes.
Display all `500`-level HTTP status codes.	`^[5]`	Matches any value that begins with a `5`. For example, this filter can return `500` and `502` status codes.
Display all `400` and `500`-level HTTP status codes.	`^[45]`	Matches all values that begin with a `4` or `5`. For example, this filter can return `400`, `403`, and `500` status codes.
Display any HTTP status codes except `200`-level status codes.	`^(?!2)`	Matches all values except values beginning with a `2`, where `^(?!)` specifies the range of results to exclude. For example, this filter can return `400`, `500`, and `302` status codes.
Display any IP address with a `187`.	`187.`	Matches `1`, `8`, and `7` characters in the IP address.
Review all IP addresses containing `187.18.`.	`187\.18\.`	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`.	`[^187.18.197.150]`	Matches anything except `187.18.197.150`, where `[^]` specifies the exact value to exclude.
Exclude a list of specific IP addresses	`[^187.18.197.150|187.18.197.151|187.18.197.152]`	Matches anything except `187.18.197.150`, `187.18.197.151`, and `187.18.197.152`, where the `|` symbol serves as an OR function

Chart Scenario	Regex filter	How it works
		and [^] specifies the exact values to exclude.