Drill down

Published: 2019-02-10

An interesting metric naturally leads to questions about behavior in your network environment. For example, if you find a large number of DNS request timeouts on your network, you might wonder which DNS clients are experiencing those timeouts. Drill-down functionality in the ExtraHop system can help answer these types of questions when viewing metric data in charts.

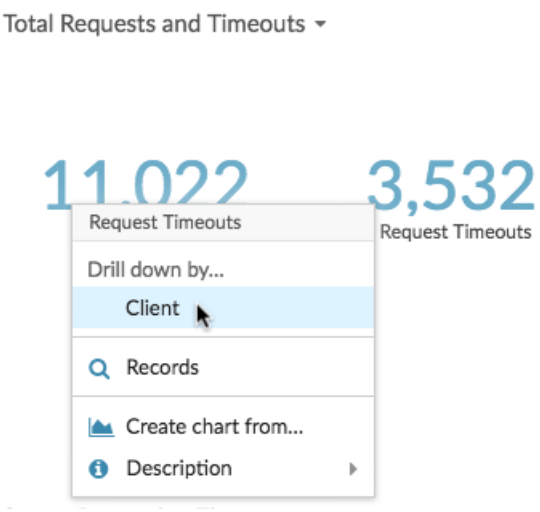
In the ExtraHop system, you can easily drill down from a top-level metric into specific details about the devices, methods, or resources associated with that metric. When you drill down on a metric by a key (such as a client IP address or resource), the ExtraHop system calculates a topnset of up to 1,000 key-value pairs. You can then investigate these key-value pairs, known as detail metrics, to learn which factors are linked to the interesting activity.

Drill down on metrics from a dashboard or protocol page

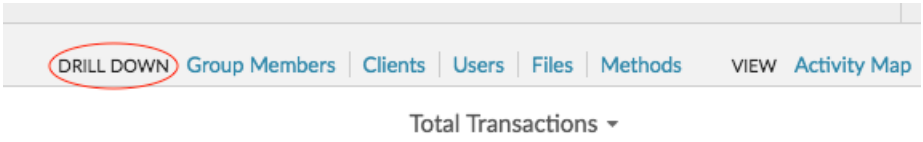
Drilling down on any metric you see in a chart or legend helps you see which key, such as client IP address, server IP address, method, or resource, contributed to that value.

The following steps show you how to locate a metric and then drill down:

1. Log into the Web UI on the Discover or Command appliance.
2. Find an interesting metric by completing one of the following steps:
   - Click **Dashboard**, and then select a dashboard from the left pane. A dashboard appears containing metrics.
   - Click **Metrics**. Click **Device**, **Device Group**, **Activity Group**, or **Application** in the left pane. Then select a device, group, or application. A protocol page appears containing metrics.
   - Click **Metrics**, click **Network** in the left pane, and then select a flow network. A protocol page appears containing metrics.
3. Click on a metric value or a metric label in the chart legend, as shown in the following figure. A menu appears.



Tip: On a protocol page, you can also click a drill-down shortcut button in the DRILL DOWN section, located in the upper right corner of the page. The type of shortcut buttons vary by protocol.



4. In the Drill down by… section, select a key. A detail metrics page with a topnset of metric values by key appears. You can view up to 1,000 key-values pairs on this page.

   Tip: If a View More link appears at the bottom of a chart, click **View More** to drill down on the metric displayed in the chart.

Next steps

- Investigate detail metrics

Drill down on network capture and VLAN metrics

When you see an interesting top-level metric about network activity on a Network capture or VLAN page, you can identify which devices are linked to that activity.

Note: For information about how to drill down on metrics from a flow network or flow network interface page, see the Drill down on metrics from a dashboard or protocol page section.

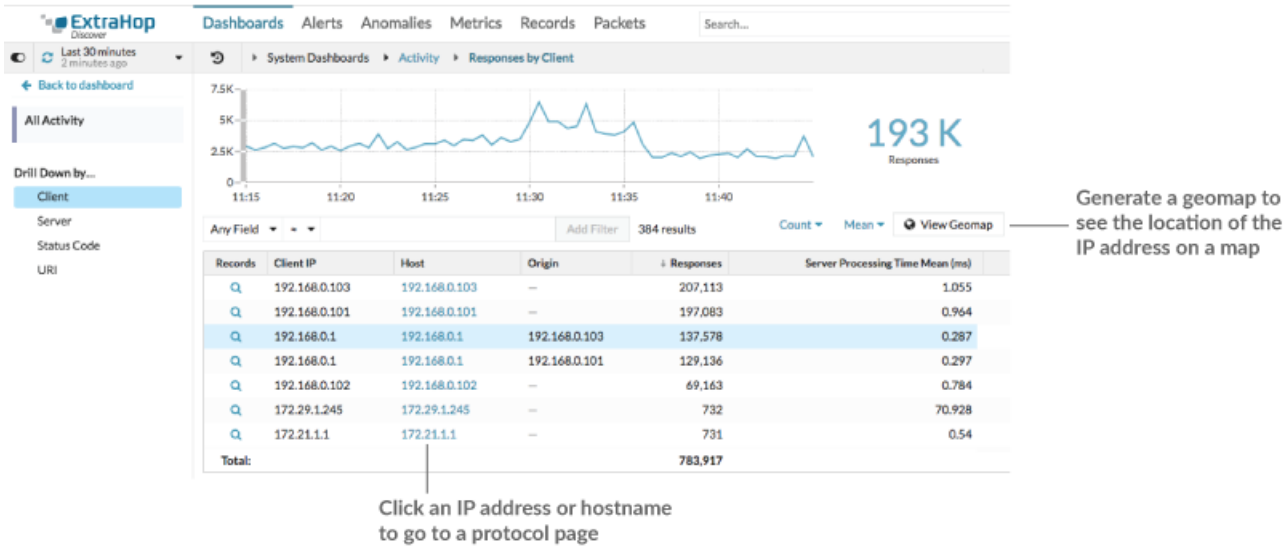
1. Log into the Web UI on the Discover or Command appliance.
2. Click **Metrics**.
3. Click **Networks** in the left pane.
4. Click a network capture or VLAN interface name.
5. Click a network layer in the left pane, such as **L3** or **L7 Protocols**. Charts that display metric values for the selected time interval appear. For most protocols and metrics, a Device table also appears at the bottom of the page.
6. Click the chart data, which updates the list to display only the devices that are associated with the data.
7. Click a device name. A Device page appears, which displays traffic and protocol activity associated with the selected device.

Investigate detail metrics

After you drill down on a metric from a dashboard, overview page, or protocol page, you can filter data or select different keys, such as status codes or URIs, to investigate your data from different perspectives.

The following figure shows you how to filter, pivot, sort, or export data.

If you drilled-down on a metric by IP, Client, or Server, IP addresses and hostnames (if observed from DNS traffic) appear in the table. Additional options are now available to you. For example, you can generate a geomap or directly navigate to a client or server protocol page, as shown in the following figure.



Filter results

A detail page can contain up to 1,000 key-value pairs. There are two ways to find specific results from all this data: filter results with a set of three filters (known as the trifield) or click a key in the table to create another drill-down filter.

The trifield filter is available below the chart to help you filter results in the following ways:

- Type in the filter field to dynamically filter results
- Click the Any Field drop-down list and make a selection
- Choose an operator to define parameters for your filter:
  - Select **=** to perform an exact string match.
  - Select **#** to perform an approximate string match. The # operator supports regular expression.

Note: To exclude a result, enter a regular expression. For more information, see Create regular expression filters in a chart.

- Select **#** to exclude an approximate string match from your results.
- Select **>** or **#** to perform a match for values greater than (or equal to) a specified value.
- Select **<** or **#** to perform a match for values less than (or equal to) a specified value.

- Click **Add filter** to save the filter settings. You can save multiple filters for one query. Saved filters are cleared if you select another key from the Details section in the left pane.

Investigate threat intelligence data (ExtraHop Reveal(x) Premium and Ultra only)

Click the red camera icon to view threat intelligence information about a suspicious host, IP address, or URI found in detail metric data.

Highlight a metric value in the top chart

Select an individual row or multiple rows to change chart data in the top chart on the detail metric page. Hover over data points in the chart to view more information about each data point.

Pivot to more data by key

Click key names in the Details section to see more detail metric values, broken down by other keys. For IP address or host keys, click a device name in the table to navigate to a Device protocol page, which displays traffic and protocol activity associated with that device.

Adjust the time interval and compare data from two time intervals

By changing the time interval, you can view and compare metric data from different times in the same table. For more information, see Compare time intervals to find the metric delta.

Note: The global time interval in the upper left corner of the page includes a blue refresh icon and gray text that indicates when the drill-down metrics were last polled. To reload the metrics for the specified time interval, click the refresh icon in the Global Time Selector display. For more information, see View the latest data for a time interval.

Sort metric data in columns

Click the column header to sort by metrics to view which keys are associated with the largest or smallest metric values. For example, sort on processing time to see which clients experienced the longest website load times.

Change data calculation for metrics

Change the following calculations for metric values displayed in the table:

- If you have a count metric in the table, click **Count** in the Options section in the left pane and then select **Average Rate**. Learn more in the Display a rate or count in a chart topic.
- If you have a dataset metric in the table, click **Mean** in the Options section in the left pane and then select **Summary**. When you select **Summary**, you can view the mean and the standard deviation.

Export data

Right-click a metric value in the table to download a PDF, CSV, or Excel file.

Drill-down a second time by a key filter

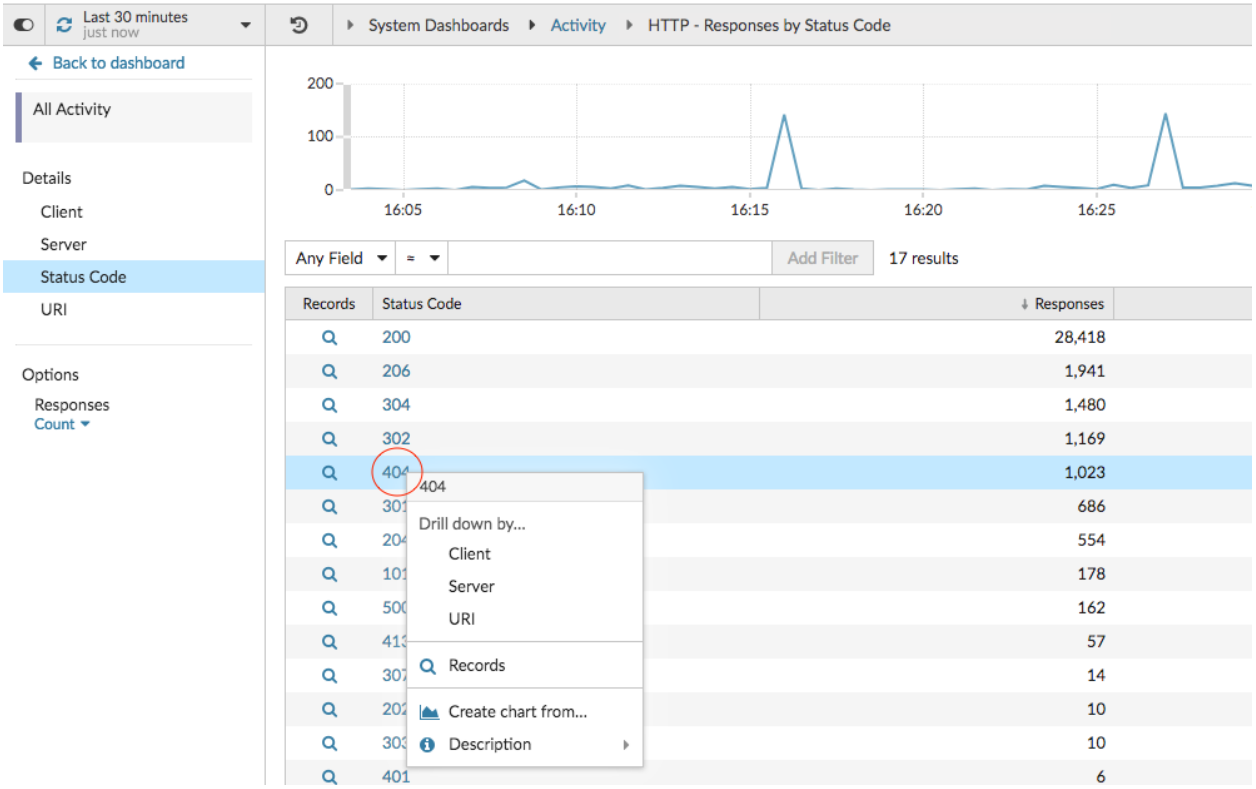
After you first drill down on a top-level metric by key, a detail page appears with a topnset of metric values broken down by that key. You can then create a filter to drill down a second time by another key. For example, you can drill down on HTTP responses by status code, and then drill down again by the 404 status code to find more information about the servers, URIs, or clients associated with that status code.

Note: The option to drill-down a second time is only available for certain topnsets.

The following steps show you how to drill down from a chart and then drill down again from a detail metric page:

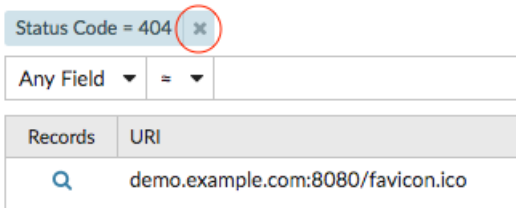
1. Log into the Web UI on the Discover or Command appliance.

2. Navigate to a dashboard or protocol page.
3. Click a metric value or label.
4. In the Drill down by… section, select a key.
   A detail page appears.
5. Click a key in the table, such as a status code or method. (The key must not be an IP address or hostname.)
6. In the Drill down by… section, select a key, as shown in the following figure.

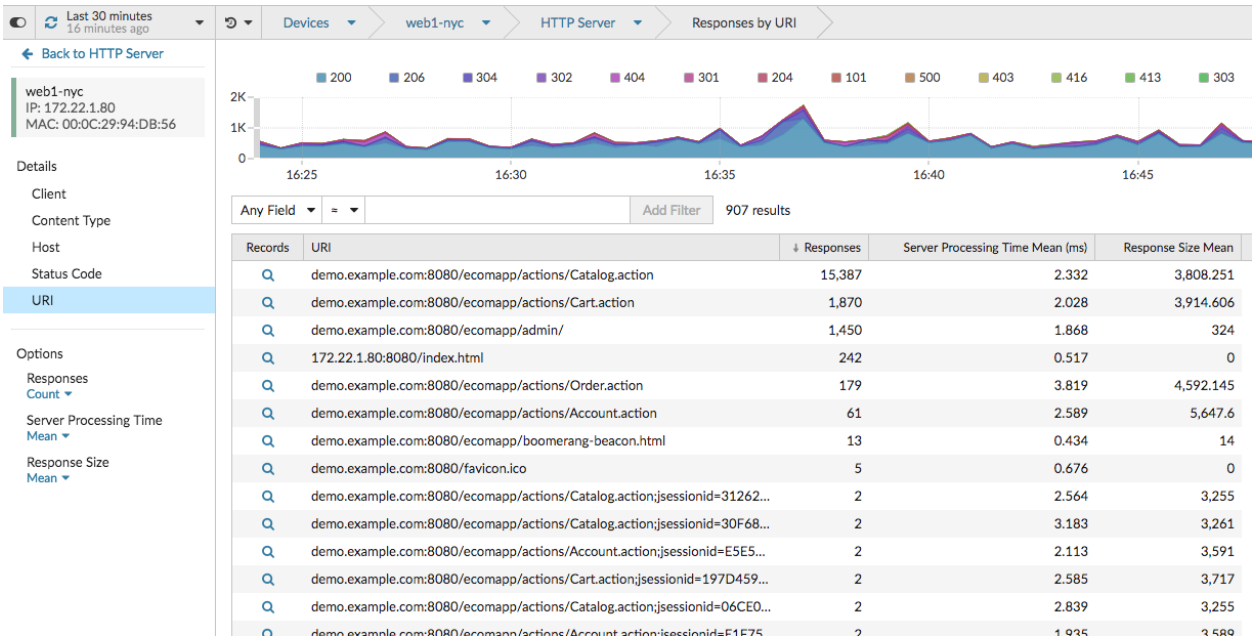


The key filter appears above the table. You can now view all the detail metrics associated with that single key.

7. To remove this filter from the table and then apply the filter to the top chart, click the **x** icon, as shown in the following figure.



The filter in the chart persists as you select other keys in the Details section.



Add detail metrics to chart

If you want to quickly monitor a set of detail metrics in a dashboard, without repeatedly performing the same drill-down steps, you can drill down on a metric when editing a chart in the Metric Explorer. A chart can display up to 20 of the top detail metric values broken down by key. A key can be a client IP address, hostname, method, URI, referrer, or more.

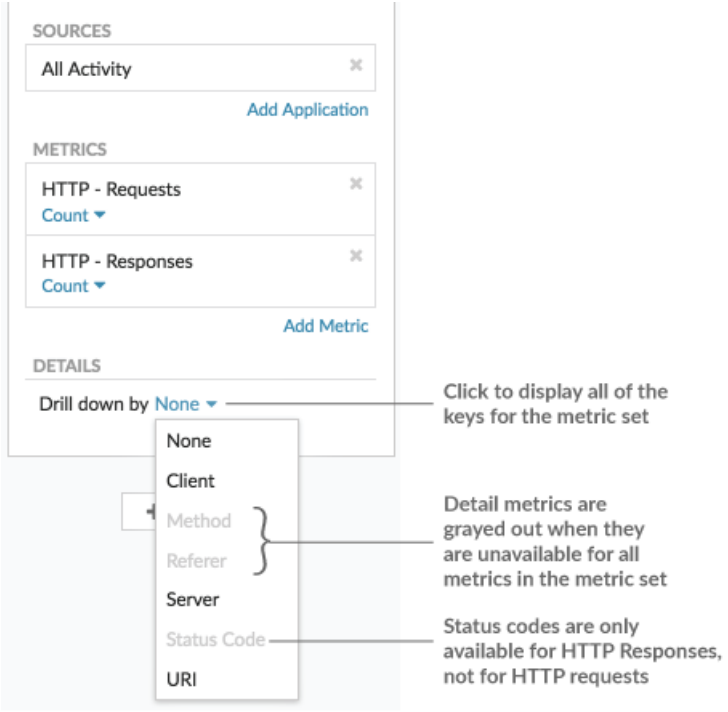
For example, a dashboard for monitoring web traffic might contain a chart displaying the total number of HTTP requests and responses. You can edit this chart to drill down on each metric by IP address to see the top talkers.

The following steps show you how to edit an existing chart and then drill down to display detail metrics:

1. Log into the Web UI on the Discover or Command appliance.
2. Navigate to a dashboard or protocol page.
3. Click the chart title and then select **Edit**.
4. In the Details section, click **Drill down by <*None*>**, where <*None*> is the name of the drill-down metric key currently displayed in your chart.
5. Select a key from the drop-down list.

Note: If you have more than one source selected in your metric set, such as two devices, the sources are automatically combined into an ad hoc source group as you drill down. You cannot deselect the **Combine Sources** checkbox. To view drill-down metrics for each source, you must remove a source from the metric set and then click **Add Source** to create a new metric set.

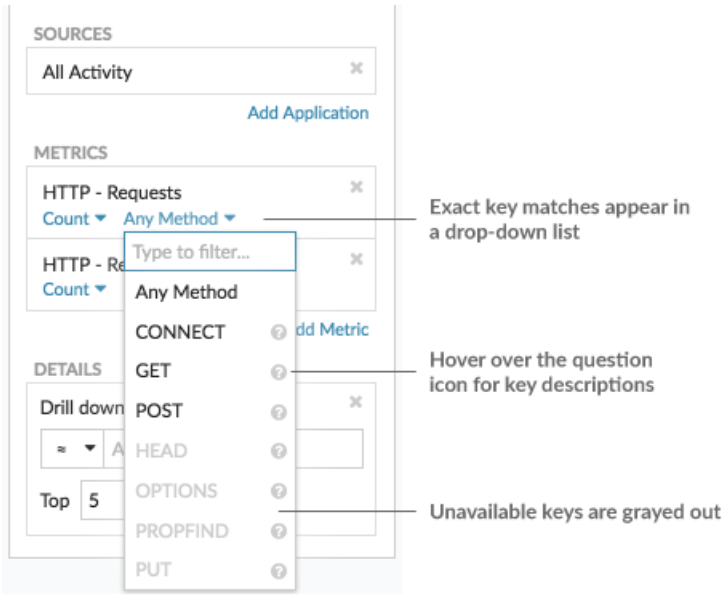
If drill-down metric data for a common key is available for all of the metrics in a metric set, the drill-down metrics automatically appear in the drop-down list, as shown in the following figure. If a drill-down metric in the list is grayed out, data is unavailable for all of the metrics in that metric set. For example, client, server, and URI data are available for both HTTP Requests and HTTP Responses metrics in the metric set.



6. You can filter drill-down metric keys with an approximate match, regular expression (regex), or exact match through one of the following steps:
   - In the Filter field, select the **#** icon to display keys by an approximate match or with regex. You must omit forward slashes with regex in the approximate match filter.

     Note: The **#** filter option to exclude results is only available on detail pages. If you want to exclude results in a dashboard chart, create a regex string.
   - In the Filter field, select the **=** icon to display keys by an exact match. In the Filter field, select the **=** icon to display keys by an exact match.
7. Optional: In the top results field, enter the number of keys that you want to display. These keys will have the highest values.
8. To remove a drill-down selection, click the **x** icon.

   Note: You can display an exact key match per metric, as shown in the following figure. Click the drill-down metric name (such as **All Methods**) to select a specific drill-down metric key (such as `GET`) from the drop-down list. If a key appears gray (such as `PROPFIND`), drill-down metric data is unavailable for that specific key. You can also type a key that is not in the drop-down list.


SOURCES
All Activity
Add Application
METRICS
HTTP - Requests
Count
Any Method
Type to filter...
Any Method
CONNECT
GET
POST
HEAD
OPTIONS
PROPFIND
PUT
Exact key matches appear in a drop-down list
Hover over the question icon for key descriptions
Unavailable keys are grayed out