Drill down

Published: 2017-09-19

Chart metrics often raise questions about behavior in your environment. For example, if you find a large number of DNS request timeouts on your network, you might wonder which DNS servers are experiencing those timeouts. ExtraHop drill down functionality can help answer that question and other questions that come up when viewing charts.

The ExtraHop system enables you to 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 metric value-key pairs.

Drill down on metrics from device or application protocol pages

When you see an interesting top-level metric about protocol activity on a device, a device group, an activity group, or an application page, you can drill down to investigate which factors are linked to that activity. Drilling down on a metric lets you investigate metric values broken down by key, such as client IP address, server IP address, methods, or resources.

1. Click **Metrics** and then click **Device**, **Device Group**, **Activity Group**, or **Application** in the left pane.
2. Click a device, group, or application name.
3. Click on a metric value or a metric label in the chart legend. A menu appears.

   Tip: You can also click a drill-down shortcut button in the Drill Down section in the upper right corner of the page.
4. In the Drill down by… section, select a key. A drill-down metrics page with a topnset of metric values by key appears. You can view up to 1,000 key values in a topnset.

   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.

Drill down on flow network metrics

When you see an interesting top-level metric about network activity on a flow network or flow interface page, you can drill down to investigate which factors are linked to the activity. Drilling down on a metric lets you investigate metric values broken down by peer IP addresses, protocols and ports, conversations, and sender and receiver IP addresses.

1. Click **Metrics** and then click **Networks** in the left pane.
2. Click a flow network or flow interface name.
3. Click a metric value or a metric label in the chart legend. A menu appears.
4. In the Drill down by… section, select a key. For example, in the Endpoints region, you can drill down on charts by peer IP addresses.
   You will navigate to a page that contains a table of metric values by key from a topnset. You can view up to 1,000 key values in a topnset.

   Note: For drill-down metric values, which are not polled automatically, you will see the snapshot of the global time interval, which includes a blue refresh icon and gray text that indicates when the metric or record query was last polled. To reload the metrics for the specified time interval, click the refresh icon in the Global Time Selector display.

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.

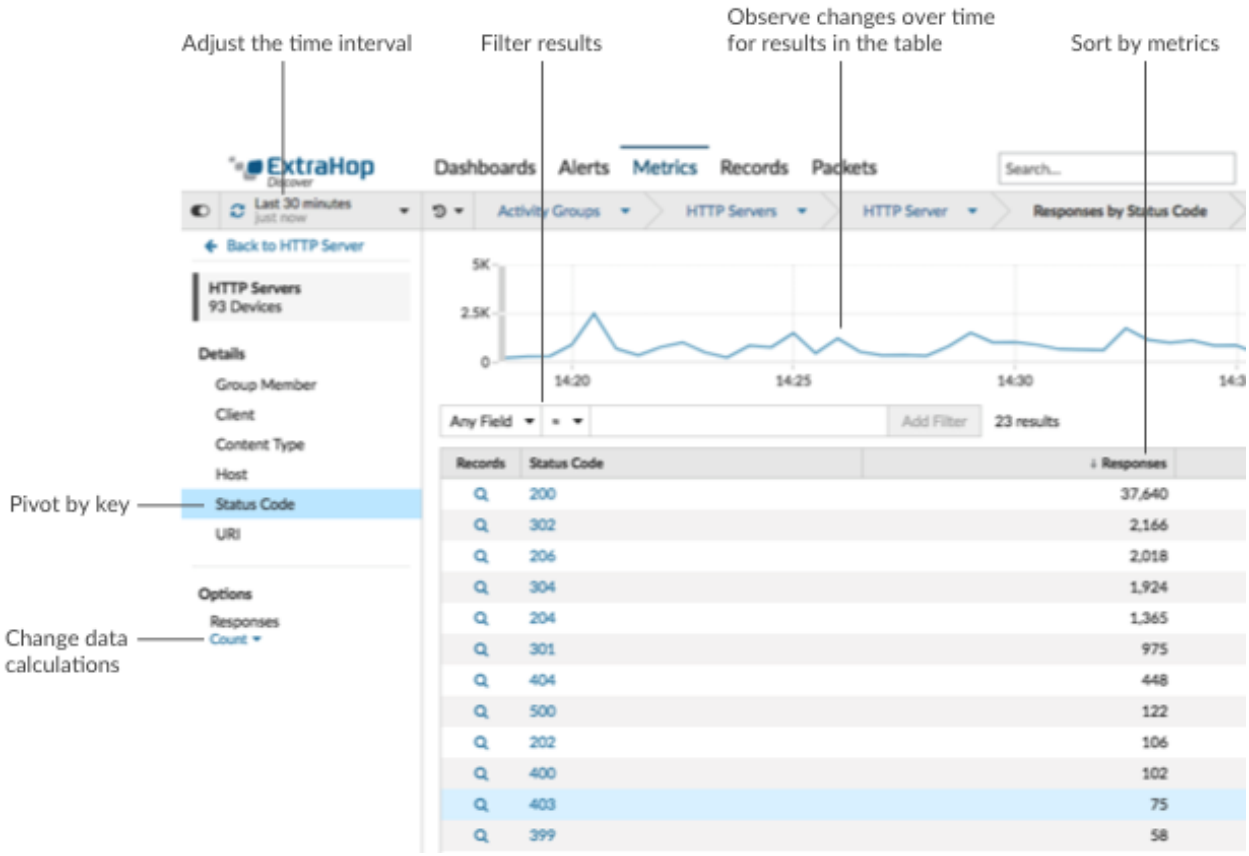
Note: For information about how to drill down on metrics from a flow network or flow network interface page, see the Drill down on flow network metrics section.

1. Click **Metrics**.
2. Click **Networks** in the left pane.
3. Click a network capture or VLAN interface name.
4. 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.
5. Click the chart data, which updates the list to display only the devices that are associated with the data.
6. Click a device name. A Device page appears, which displays traffic and protocol activity associated with the selected device.

Investigate drill-down metrics by key

Drilling down on a metric lets you view metric values by key, such as client IP address, server IP address, methods, or resources. On the drill-down, or detail metric, page, there are several ways to interact with value-key pairs, which help you to learn how a specific device, method, or resource is linked to network activity.

The following figure shows all the available options for exploring detail metrics:



Filter results

You can filter drill-down 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 **>** 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.

Observe changes over time in the chart

You can observe how a metric value changed over the selected time interval in the chart above the table. Select an individual row or multiple rows to change chart data. Hover over data points in the chart to view more information about each data point.

Pivot to more data

You can view metric values for different keys by clicking key names in the Details section in the left pane. If available, click a device name in the table to navigate to a Device page, which displays traffic and protocol activity associated with that device.

Adjust time interval and compare data from two time intervals

You can change the time interval in the Global Time Selector to view metric values from different time intervals. You can also perform a metric delta comparison from two different time intervals in the same table. For more information, see Compare metric deltas.

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 data in columns

You can sort by metrics to learn which keys are associated with the largest or smallest metric values. For example, when you drill down on HTTP responses by client for an HTTP server, you can sort on processing time to see which clients experienced the longest website load times. You can then click the host name to navigate to the Device page to learn more about the client.

Note: When you drill down on a response, request, or network byte metric, related metrics such as processing time are included in the table. For example, when you drill down on CIFS responses by files, related metrics such as goodput bytes and access time appear in the far right columns in the table.

Change data calculation for metrics

You can 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

You can download a PDF, CSV, or Excel file with all the drill-down results by right-clicking on the table.

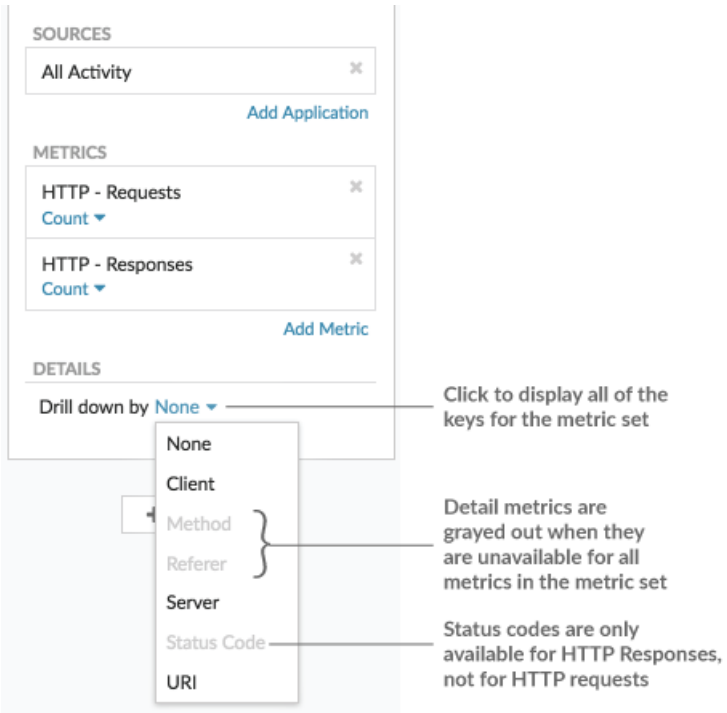
Add drill down metrics to chart

You can add drill-down metrics to charts on protocol pages and dashboards. When you drill down on a metric in the Metric Explorer, you can view up to 20 top key values in a chart for a specific time interval. A key can be a client IP address, hostname, method, URI, referrer, or more. For example, if your chart displays a total count for HTTP Requests, you can drill down by client to view the IP addresses that sent the most requests to your web servers.

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.
   - 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.