Records

Published: 2020-08-19

Records are structured information about transaction, message, and network flows that are generated and sent from the ExtraHop system to a data warehouse. After your records are collected and stored, you can query for them throughout the ExtraHop system.

Records are collected at two protocol levels: L3 and L7. L3 (or flow) records show network-layer transactions between two devices over the IP protocol. L7 records show transactions that are message-based (such as ActiveMQ, DNS, and DHCP), transactional (such as HTTP, CIFS, and NFS), and session-based (such as SSL and ICA).

For example, if you had fifty HTTP 503 errors, the related HTTP transactions would contain details about the URL, the web server, the client that sent the request, and so on. These details can help you identify the underlying problem.

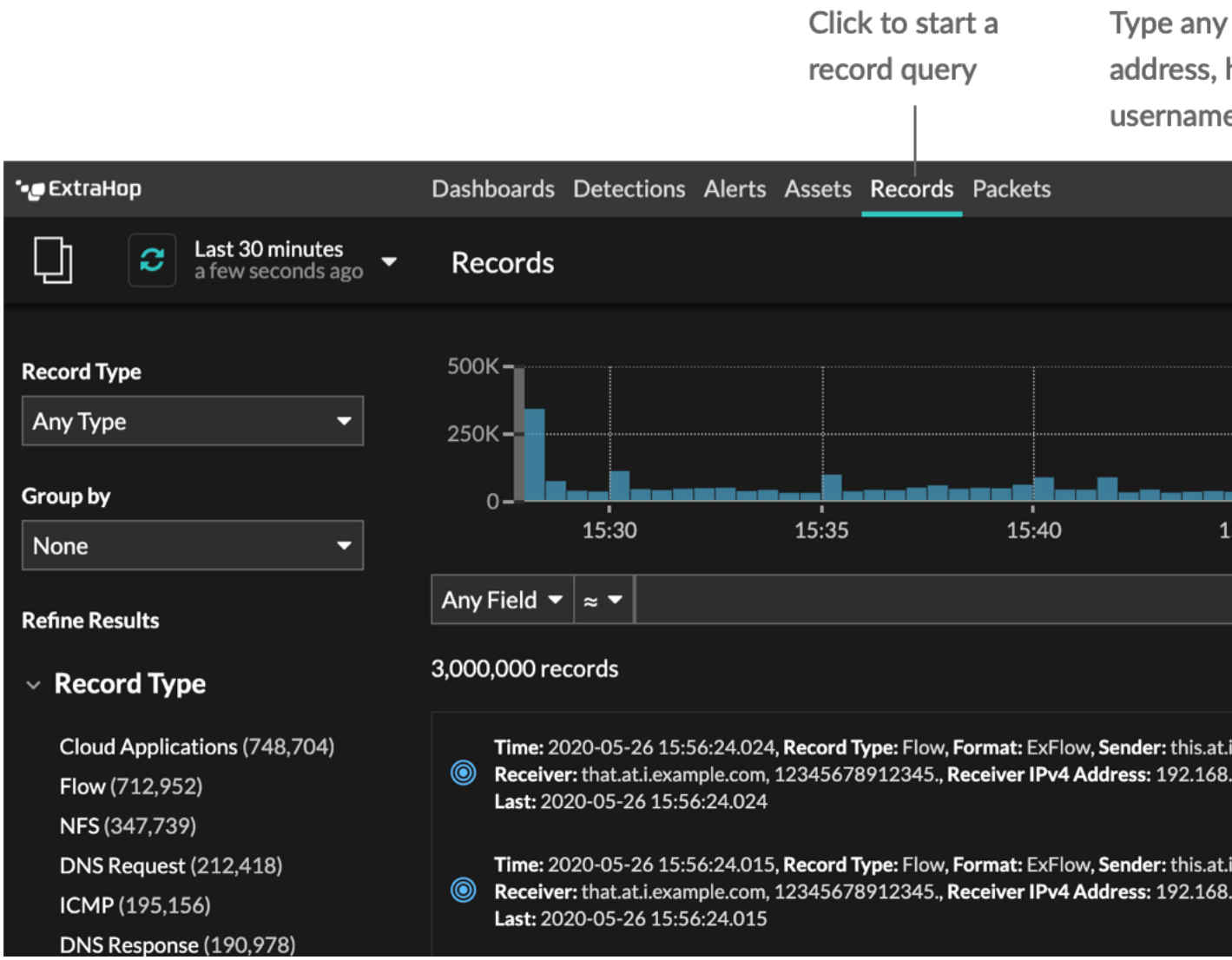
Before you begin

- You must have a configured recordstore, such as an Explore appliance or with Splunk or BigQuery.
- You can only configure one recordstore for the ExtraHop system.
- Your ExtraHop system must be configured to collect and store flow records or L7 records.

Navigating records

Click **Records** from the top menu to run a query for all stored records. The results are displayed on the main Records page. You can then apply simple or advanced filters to find potential issues, such as overly-long processing times or unusual response sizes.

Record query results that contain suspicious IP addresses, hostnames, and URIs appear with a red camera icon next to the record. For more information about these indicators of compromise, see Threat intelligence.



Records

An object that contains fields, where each field is a name and a value pair. The value can be a string, number, boolean, array, or nested object.

Record Types

An ID that determines what data is collected and stored in the recordstore. Because you must write a trigger to collect records, you need a way to identify the type of data you will collect. There are built-in record types, which collect all of the available known fields for a protocol. You can start with a built-in record type (such as HTTP) and write a trigger to collect only the fields for that protocol that matter to you (such as URI and status code). Or, advanced users can create a custom record type if they need to collect proprietary information that is not available through a built-in record type.

Note: To create a record query for a custom metric, you must first define the record relationship by linking the custom metric to a record type.

Filter your records with a simple query

There are a number of ways you can filter your record query results to find the exact transaction you are looking for. The sections below describe each method and show examples you can start with to familiarize yourself.

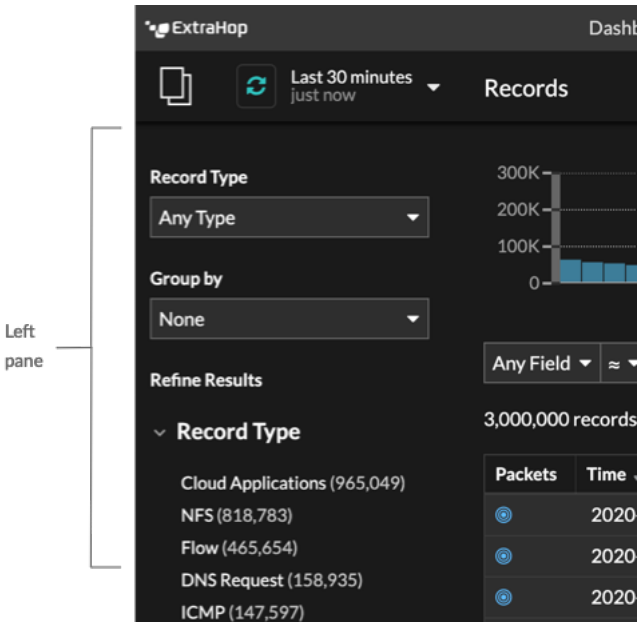
If you are trying to filter records by simple criteria (say, if you want all HTTP transactions from a single server that generated 404s), you can create a simple query. For simple queries, start by clicking **Records** from the top menu to get to the main Records page, and then add a filter in one of the following ways:

- Add a filter or refine results from the left pane
- Add a filter from the trifield
- Add a filter directly from record results

For complex filtering, see Query records with an advanced filter.

Filtering record results from the left pane

When you click **Records** from the top menu, all of the available records for your selected time interval appear. You can then filter from the left pane to refine your results.



The **Record Type** drop-down menu displays a list of all of the record types that your Discover or Command appliance is configured to collect and store.

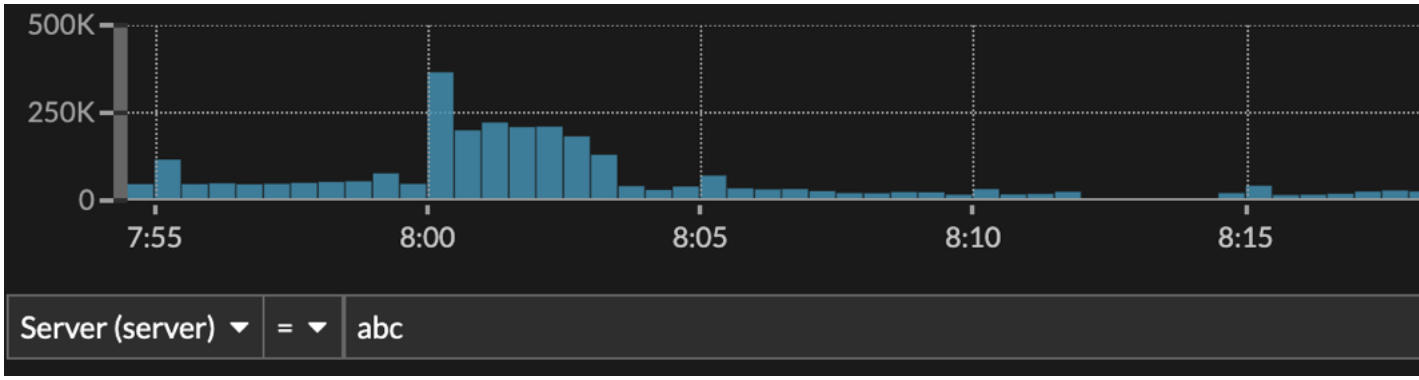
The **Group By** drop-down gives you a list of fields to further filter the record type by.

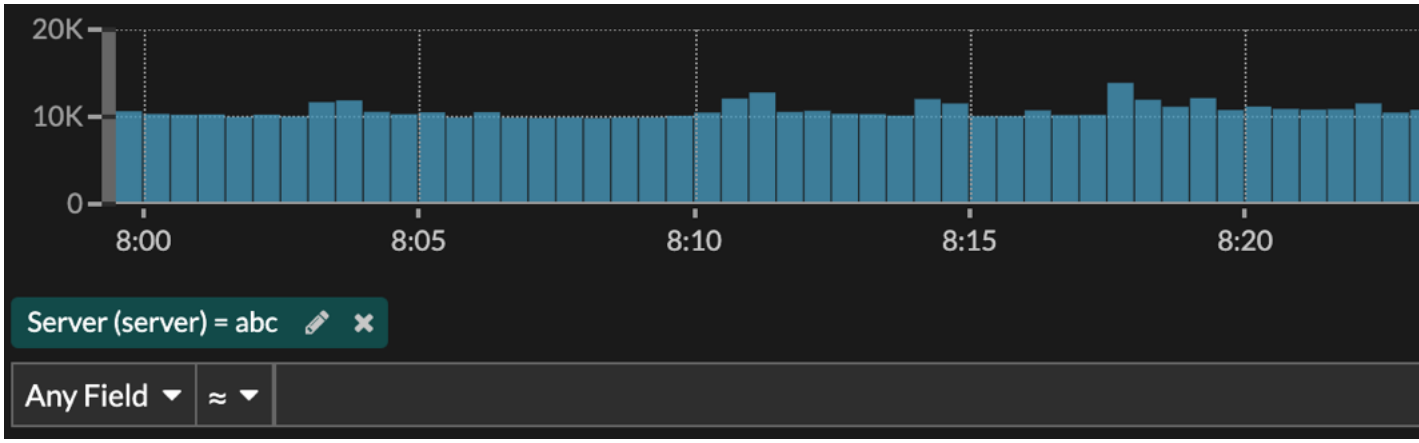
The **Refine Results** section shows you a list of record types that are currently on the Explore appliance or other supported recordstore with the current number of records in parenthesis.

Filtering record results through the trifield

When you click **Records** from the top-level navigation, all of the available records for your selected time interval appear. A set of three filters (or the trifield) is available below the chart.

Select a field from the **Any Field** drop-down (such as Server), select an operator (such as the equal sign (=)), and then type a hostname. Click **Add filter**, and the filter is added above the filter bar.





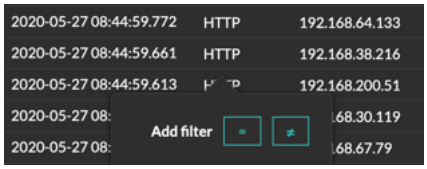
Your results only show records that match the filter; in our example this means we only see results for transactions that are for the server named abc.

The following operators can be selected, based on the selected field name:

Operator	Description
=	Equals
≠	Does not equal
≈	Includes
≈/	Excludes
<	Less than
≤	Less than or equal to
>	Greater than
≥	Greater than or equal to
starts with	Starts with
exists	Exists
does not exit	Does not exist

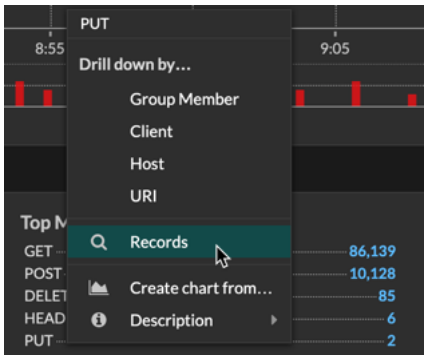
Filtering directly from record results

You can select any field entry displayed in either table view or verbose view in your record results and then click the pop-up operator to add the filter. Filters are displayed below the chart summary (except for the record type field, which is changed in the left pane).



Finding records in the ExtraHop system

- Type a search term in the global search field at the top of the screen and click Search Records to start a query across all stored records.
- From a device Overview page, click **View Records** to start a query filtered by that device.
- From a detection card, click View records to start a query filtered with the transactions associated with the detection.
- Click the Records icon from a chart widget, as shown in the following figure.



- Click the Records icon next to a detail metric after drilling down on a top-level metric. For example, after drilling down on HTTP Responses by Server, click the Records icon to create a query for records that contain a specific server IP address.