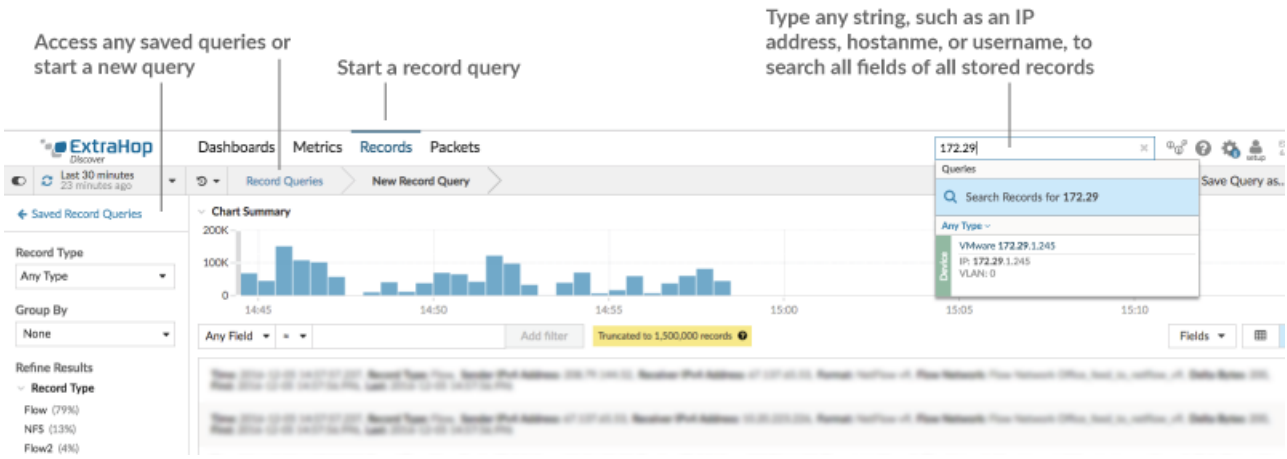
Query for stored records on an Explore appliance from a Discover or Command appliance

Published: 2020-02-23

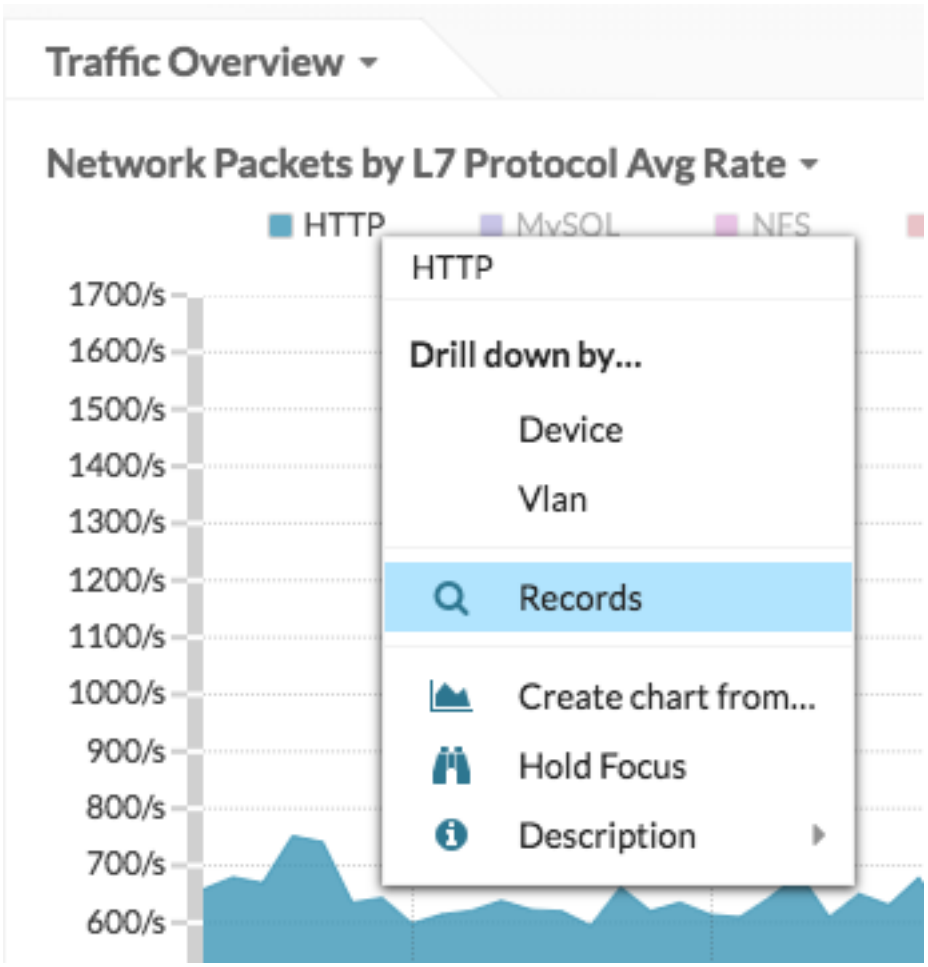
After you connect your Explore appliance to your Discover and Command appliances, and records are sent to the Explore appliance, you can query for those stored records from either the Discover or Command appliance. In addition, you can save record queries to run at a later time.

You can query records that are stored in the Explore appliance from multiple areas in the ExtraHop Web UI. The following figure shows the main records page, that you access by clicking **Records** from the top menu.

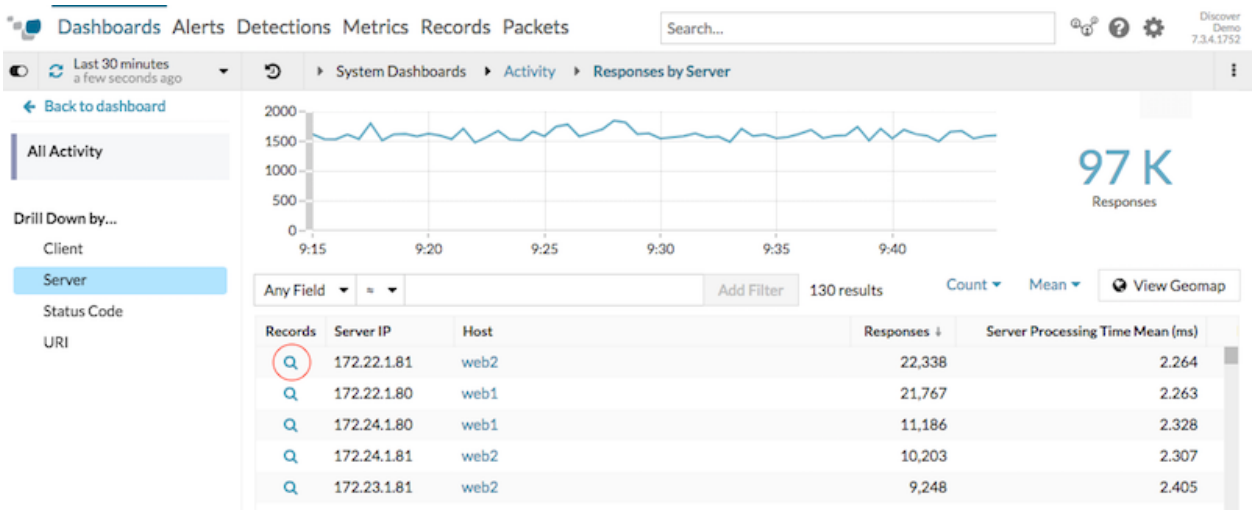
Note: You can also automate this task through the REST API.



- Click **Records** from the top menu to start a new record query for all records stored on the Explore appliance.
- From the records page, click **Record Queries** in the navigation bar or **Saved Record Queries** in the left pane to access any saved queries or start a new query.
- 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.
- 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, as shown in the following figure.



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.

No matter where you start your query from, you might have a large set of records results. You can narrow down your results by applying filters to find the specific record you need.

Next steps

- Filter your record query
- To learn how to query for a specific record, see our walkthrough for Discovering missing web resources.

Filter your records with a simple query

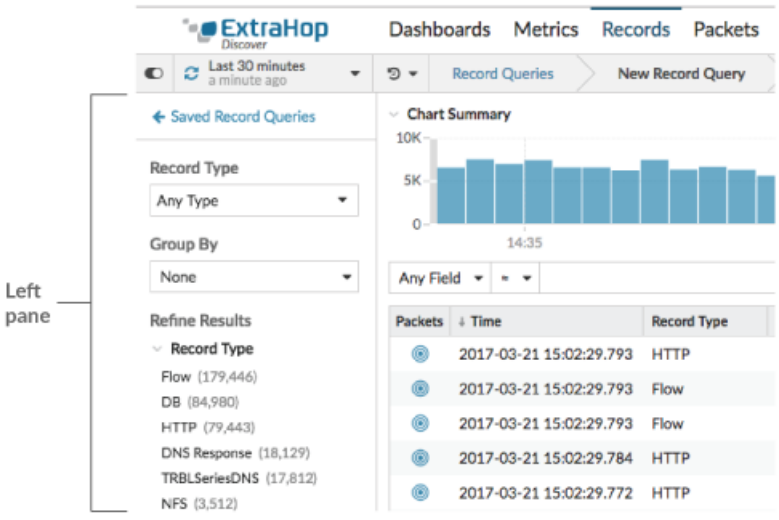
There are a number of ways you can filter your record query results to find the exact transaction you are looking for. The sections below describe each method and show examples you can start with to familiarize yourself.

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

Filter 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.

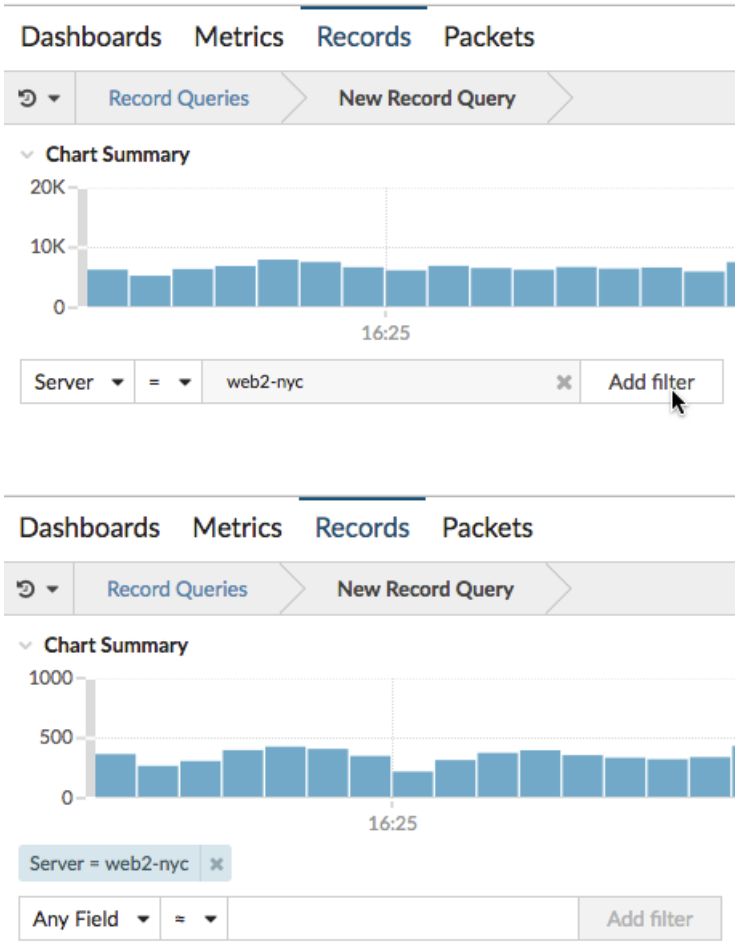
The **Group By** drop-down gives you a list of fields to further filter the record type by.

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

Filter 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 `web2-nyc`.

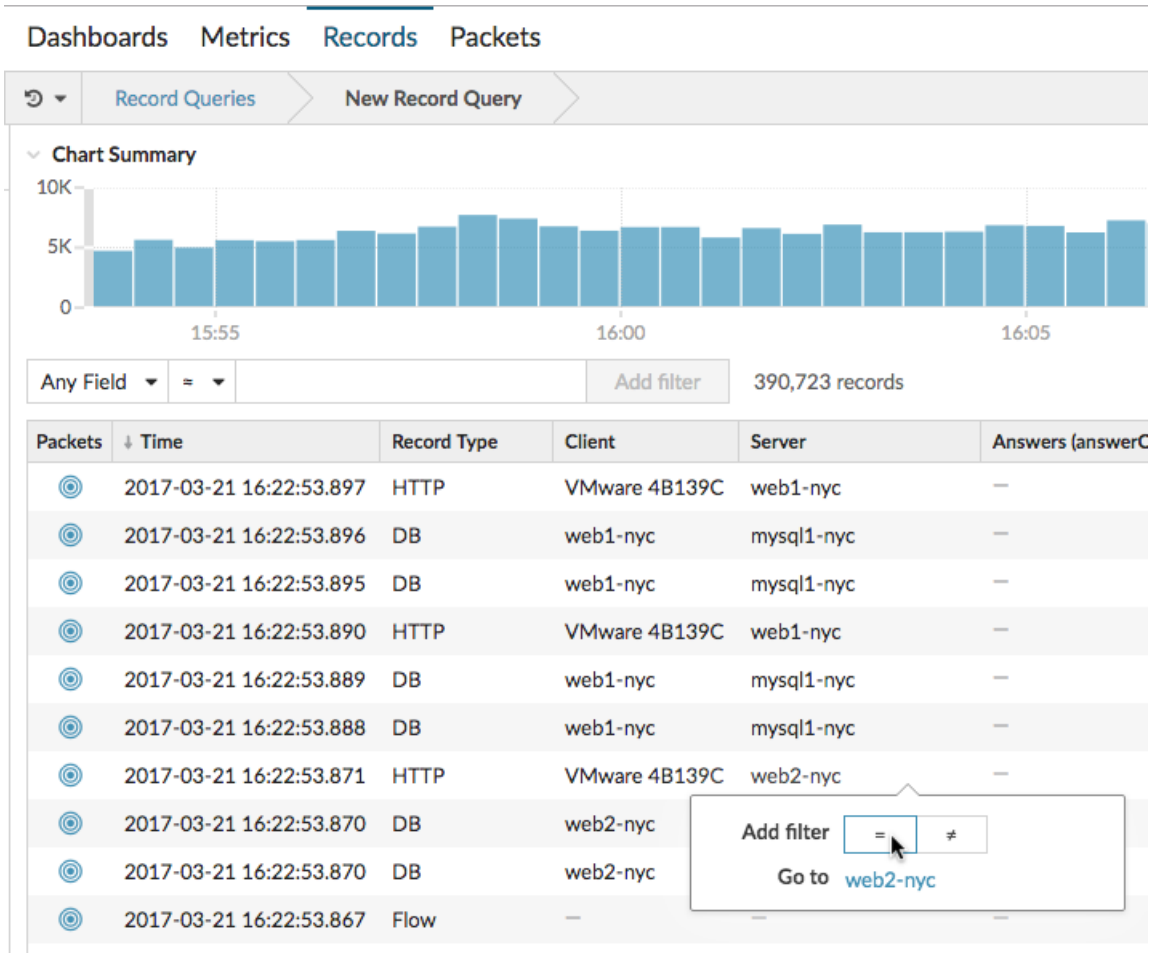
The following operators can be selected, based on the selected field name:

Operator	Description
=	Equals
≠	Does not equal
≈	Includes
≈/	Excludes
<	Less than
≤	Less than or equal to
>	Greater than

Operator	Description
≥	Greater than or equal to
starts with	Starts with
exists	Exists
does not exit	Does not exist

Filter 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).

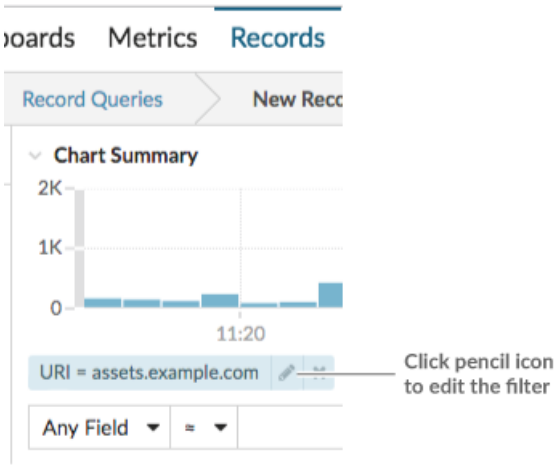


Next steps

- Filter your records with advanced query rules
- Learn how to monitor activity on suspicious ports in our records walkthrough
- Click the Packets icon to create a packet query for your record.

Filter your records with advanced query rules

For advanced queries, you can create and modify complex filters by clicking the Add Advance Filter button or by clicking the pencil icon next to any filter that you have added.



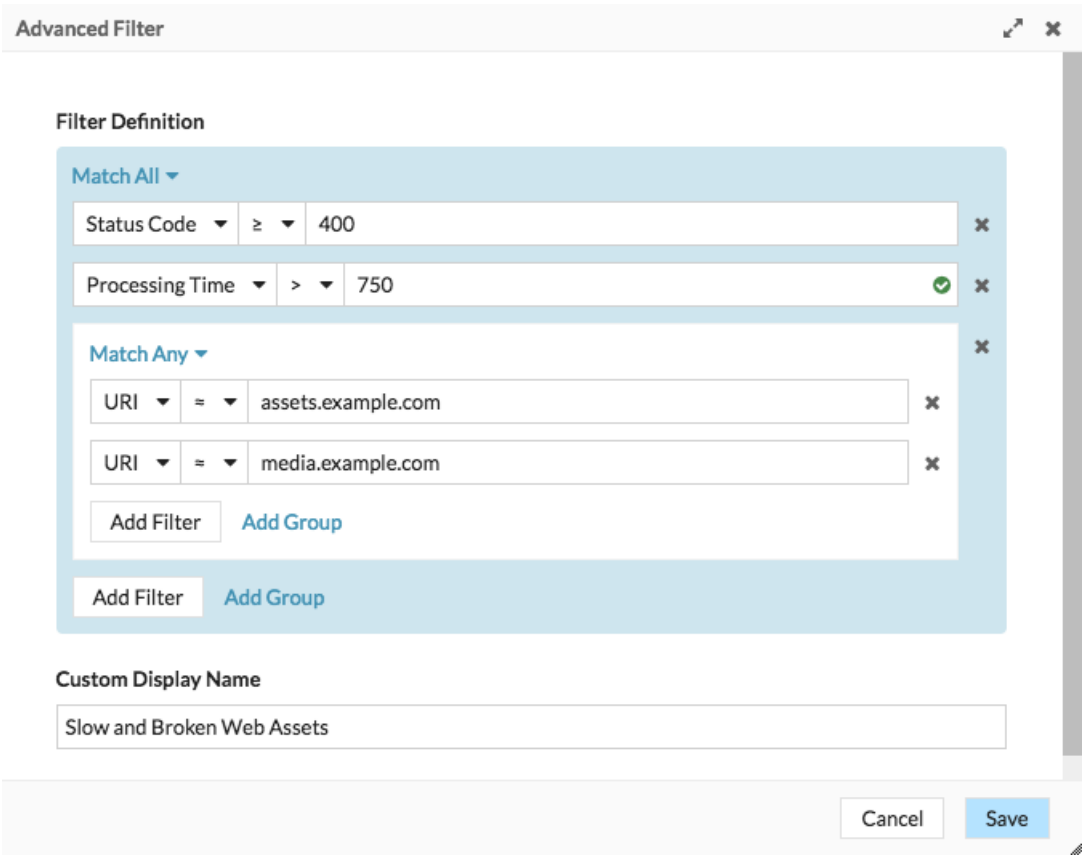
Here are some important things to know about advanced queries:

- You can specify multiple criteria with OR (Match Any), AND (Match All), and NONE operators
- You can group filters and nest them to four levels within each group
- You can edit a filter group after you create it
- You can create a descriptive name to identify the general purpose of the query

Create a complex filter with AND and OR operators

The following example shows how you can create an advanced query to filter your records with complex criteria. We will create a filter to return results for all HTTP records that include two URIs plus a status code greater than or equal to 400 or a processing time greater than 750 milliseconds.

Important: To try this example on your own Discover appliance, you must have HTTP traffic on your network.



1. Click **Records** from the top menu.
2. In the left pane, select **HTTP** from the Refine Results section. Only available records are displayed in the Refine Results section. This step ensures that you have available records for this query.

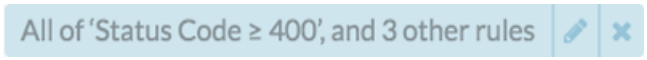
   Note: Record types do not appear as filters; they are displayed in the left pane.

3. Click the Add Advanced Filter button . The button is on the right side of the page, above the records search results.
4. Under Filter Definition, we will keep **Match All**. Match All is an AND operator and will let us search for criteria that matches the status code and the processing time criteria.
5. Select **Status Code**, the greater than or equal to sign (**≥**), and then type `400` in the number field.
6. Click **Add Filter** to add a filter for processing time.
7. Select **Processing Time**, the greater than sign (**>**), and then type `750` in the number field.

   In the next steps, we will add a group of criteria that applies specifically to the fields we added.
8. Click **Add Group**.

   We are keeping **Match Any** for this group. Match Any is an OR operator and will let us search for criteria that matches either of our URIs.
9. Click the **Any Field** drop-down and select **URI**.
10. Select the includes (**≈**) symbol.
11. Type a URI for one of your web servers in the text field. We will add `assets.example.com`.
12. Click **Add Filter** inside the white box to add a second URI filter to the group.
13. Click the **Any Field** drop-down and select **URI**.
14. Select the includes (**≈**) symbol.
15. Type a URI for one of your web servers in the text field. We will add `media.example.com`.

16. In the Custom Display Name field, type a descriptive name to make the filter easy to identify on the results page, otherwise the display name shows the first filter and the number of other applied rules:



    We will type "Slow and Broken Web Assets" in the field.
17. Click **Save**.

After you click **Save**, the query automatically runs, and returns records that match either URI and that have either a status code equal to or greater than 400 or a processing time that is greater than 750 milliseconds.

Next steps
You can click **Save Query as...** from the top right of the page to save your criteria for another time.