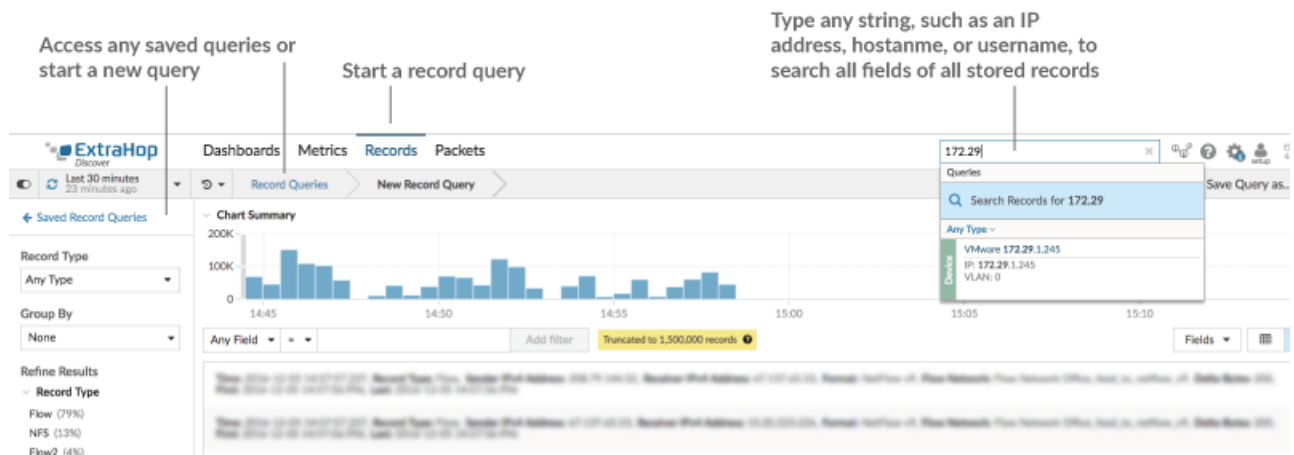


Query for stored records from a Discover or Command appliance

Published: 2017-08-08Z

After records are sent to an 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.




Access any saved queries or start a new query

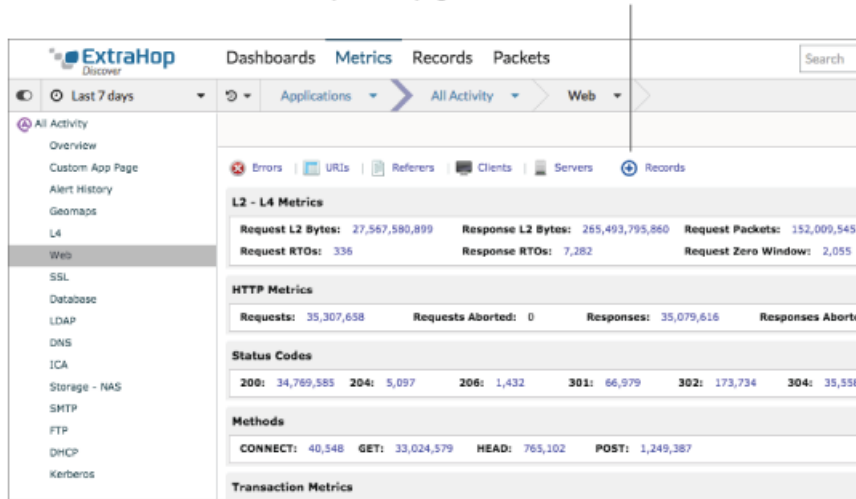
Start a record query

Type any string, such as an IP address, hostname, or username, to search all fields of all stored records


- 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.

- Click the Records icon  from the panel of Action icons on an application or device protocol page that has built-in record formats. This option queries for records that match the selected metric source

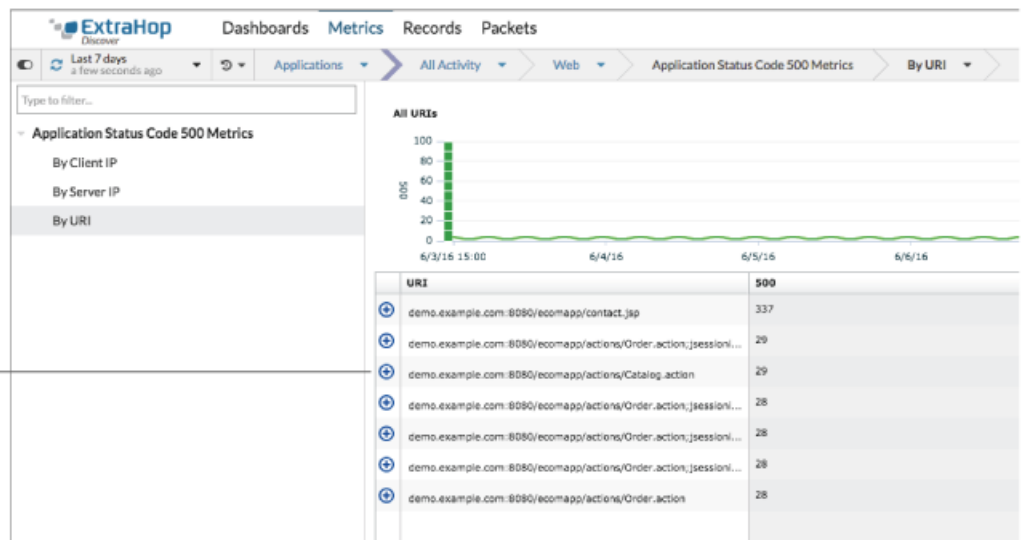
Click the Records icon on an application or device protocol page that has built-in record formats



and protocol.

- Click the Records icon  in the left-hand column from any drill-down metrics page. This option queries for records that match the selected metric source, protocol, and detailed stat value.

Click the Records icon in the left-hand column from any drill-down metrics page



- Click the Records icon  from a chart widget or on a metric drill-down page.

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.

Packets	Time	Record Type
⊙	2017-03-21 15:02:29.793	HTTP
⊙	2017-03-21 15:02:29.793	Flow
⊙	2017-03-21 15:02:29.793	Flow
⊙	2017-03-21 15:02:29.784	HTTP
⊙	2017-03-21 15:02:29.772	HTTP

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.

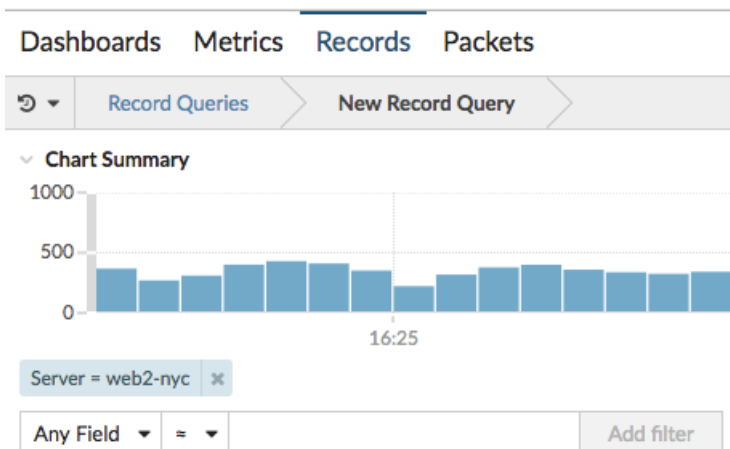
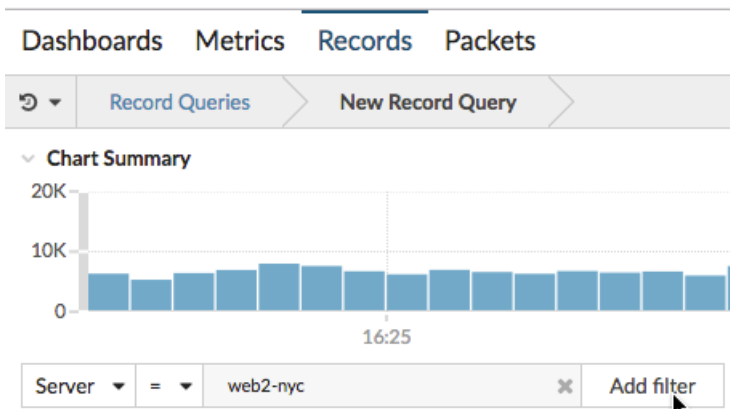
The **Group By** drop-down gives you a list of fields to further filter the record type by.

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`.

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).

Dashboards Metrics **Records** Packets

Record Queries > New Record Query

Chart Summary

Any Field = Add filter 390,723 records

Packets	Time	Record Type	Client	Server	Answers (answerC
⊙	2017-03-21 16:22:53.897	HTTP	VMware 4B139C	web1-nyc	—
⊙	2017-03-21 16:22:53.896	DB	web1-nyc	mysql1-nyc	—
⊙	2017-03-21 16:22:53.895	DB	web1-nyc	mysql1-nyc	—
⊙	2017-03-21 16:22:53.890	HTTP	VMware 4B139C	web1-nyc	—
⊙	2017-03-21 16:22:53.889	DB	web1-nyc	mysql1-nyc	—
⊙	2017-03-21 16:22:53.888	DB	web1-nyc	mysql1-nyc	—
⊙	2017-03-21 16:22:53.871	HTTP	VMware 4B139C	web2-nyc	—
⊙	2017-03-21 16:22:53.870	DB	web2-nyc		
⊙	2017-03-21 16:22:53.870	DB	web2-nyc		
⊙	2017-03-21 16:22:53.867	Flow	—		

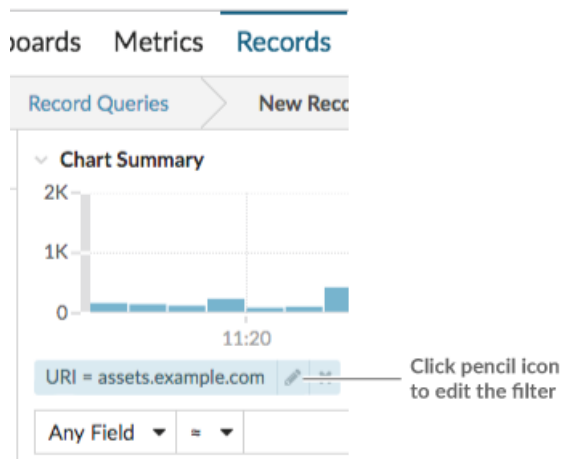
Add filter = ≠
Go to [web2-nyc](#)

Next steps

- [Filter your records with advanced query rules](#)
- [Learn how to monitor activity on suspicious ports in our records walkthrough](#)

Filter your records with advanced query rules

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



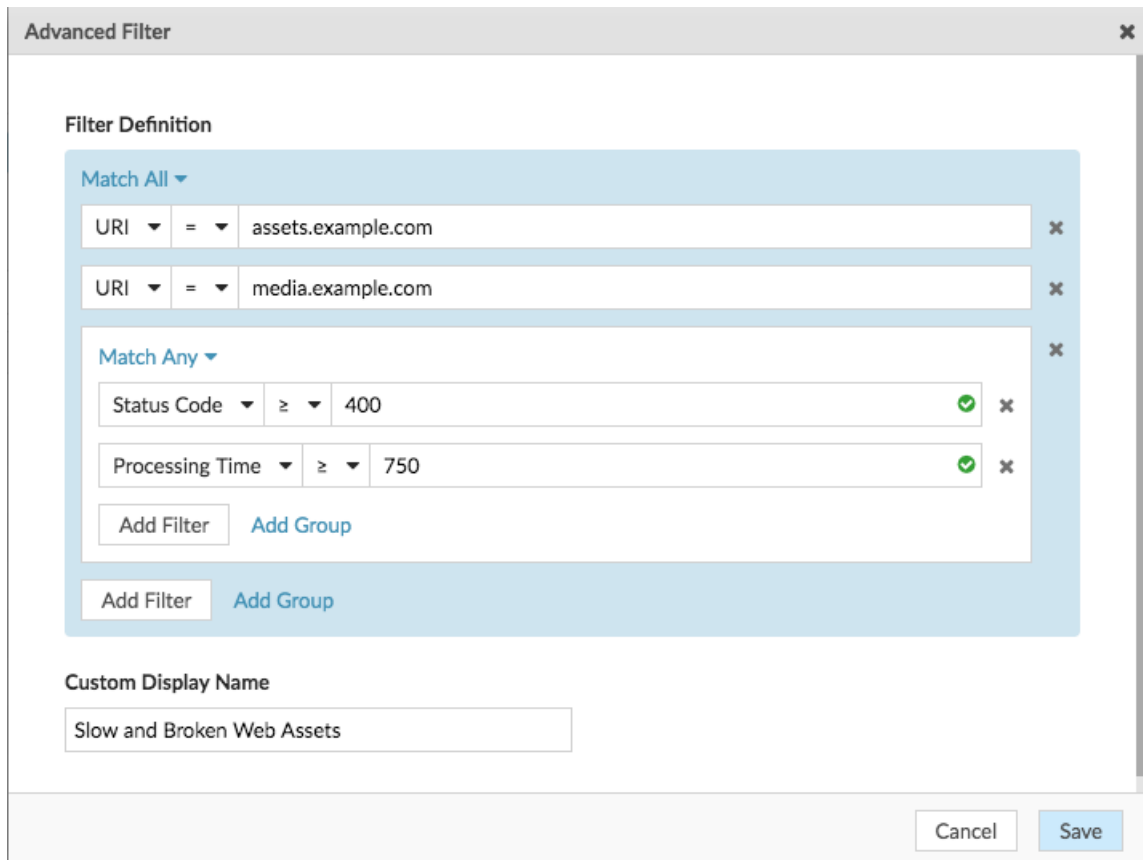
Here are some important things to know about advanced queries:

- 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.

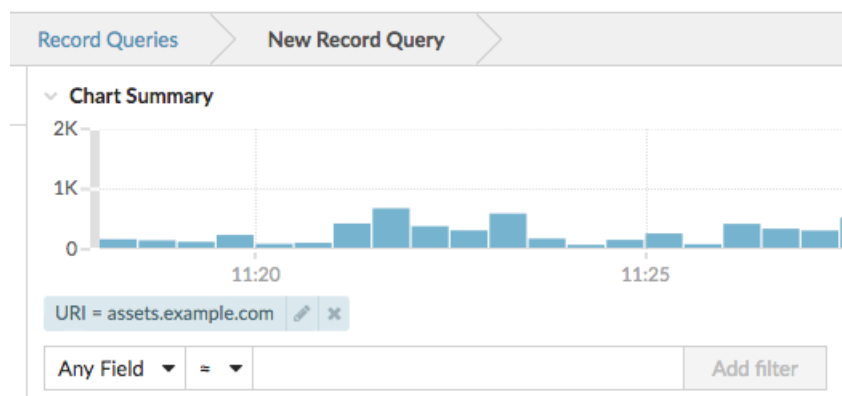
⚠ Important: To try this example on your own Discover appliance, you must have HTTP traffic on your network.



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. From within your record results, click an entry for a web server on your network in the URI column. Then, click the equal sign (=) to add the filter. We will select a URI called `assets.example.com`. The filter is now saved and appears beneath the chart.
4. Click the pencil icon  next to your saved filter to open the Advanced Filter editor. The Advanced Filter window opens with the Filter Definition already showing the URI you added.

boards Metrics **Records** Packets



5. Click **Add Filter** to add a second URI for another web server.
6. Select **URI**, the equal sign (=), and then enter another URI. We will add `media.example.com`.

7. Under Filter Definition, change **Match Any** to **Match All**. Match Any is an AND operator and will let us search for criteria that matches both of these URIs.
In the next steps, we will add a group of criteria that applies specifically to the URIs we added.
8. Click **Add Group**.
 - a) Click the **Any Field** drop-down and select **Status Code**.
 - b) Select the greater than or equal to (**#**) symbol.
 - c) Type 400 in the number field.
9. Click **Add Filter** inside the white box to add another filter to the group.
 - a) Click the **Any Field** drop-down and select **Processing Time**.
 - b) Select the greater than (**>**) symbol.
 - c) Type 750 in the number field.
10. 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:



All of 'URI = assets.example.com', and 3 other rules  

We will type “Slow and Broken Web Assets” in the field.

11. 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.