Records

Published: 2020-02-23

Records are structured information about transaction, message, and network flows that are generated and sent from a Discover appliance to an Explore appliance for storage and retrieval. After your records are stored, you can query for them from the Discover or Command appliances.

Before you begin
You must have a configured ExtraHop Explore appliance and connect it to your Discover appliance before you can store and query for packets. See our deployment guides to get started.

With the Discover appliance, you start with a high-level view of your Discover appliance data, and then drill down to view your device data. With records stored on an Explore appliance, you can drill down to individual transactions from those devices, or you can query for outlying transactions, such as overly-long processing times or unusual response sizes.

For example, if you had fifty HTTP 503 errors, you could view details about those errors by querying the records stored on the Explore appliance. The records would contain specific information about each individual HTTP transaction, which might reveal the underlying problem.

There are two basic types of records: flow and L7. Flow records show network-layer communication between two devices over an (L3) IP protocol. L7 records show details from individual messages or transactions over L7 protocols. There are three types of supported L7 protocols: transactional (such as HTTP, CIFS, and NFS), message-based (such as ActiveMQ, DNS, and DHCP), and session-based (such as SSL and ICA).

Important: Most user privileges let you query for records, but collecting and storing records requires full write privileges and familiarity with writing triggers.

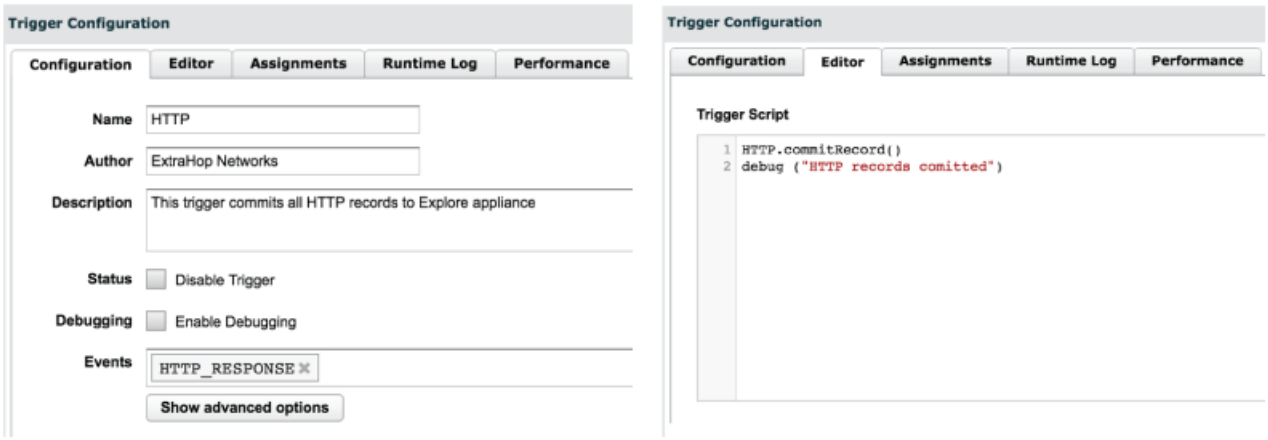
Here are a few definitions you should know about records in the ExtraHop Web UI:

- **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 on your Explore appliance. 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.
- **Record formats:** A schema that lets you display stored records in a formatted table (or table view) when you run a record query. The Discover appliance has record formats for each built-in record type. However, if you create a custom record type, but do not create a corresponding record format, you will only be able to view your fields in a text verbose view—custom fields will not appear in any selectable lists, such as the Group By list.
- **Indicators of compromise (ExtraHop Reveal(x) Premium and Ultra only):** 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 indicators of compromise, see Threat intelligence - Reveal(x) only.

Collecting and storing built-in records

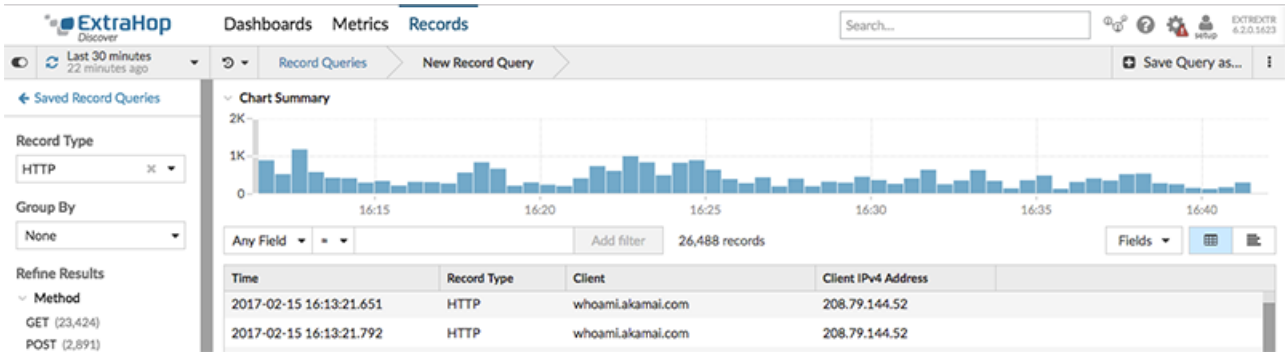
Any system protocol can be committed (collected and stored) as a record through a global trigger function. The basic trigger syntax is `<protocol>.commitRecord()`.

`HTTP.commitRecord()` commits all detected HTTP traffic for the devices to which the trigger is assigned. The following figure shows the completed Trigger Configuration window.



For each built-in record type (such as HTTP), there is a corresponding built-in record format. Record formats control how records of a certain type are displayed in the ExtraHop Web UI, such as the display name of each field, the preferred order of fields, and which fields are visible by default. A record format is needed to show fields in the table view. Without a record format, all the fields in a record can still be viewed in verbose view, which displays all fields in plain text. (Modifying record formats for custom record types is an advanced feature.)

The following figure shows record results for all HTTP transactions.



Related topics

Check out the following guides and resources that are designed to familiarize new users with our top features.

- Collect flow records
- Collect L7 records
- Query for stored records on an Explore appliance from a Discover or Command appliance