Send records from ExtraHop to Splunk

Published: 2020-02-23

You can configure your Discover appliance to send transaction-level records to a Splunk server for long-term storage, and then query those records from the ExtraHop Web UI and the ExtraHop REST API.

Before you begin

- You must have version 7.3.0 or later of Splunk Enterprise and a user account that has administrator privileges.
- You must configure the Splunk HTTP Event Collector before your Splunk server can receive ExtraHop records. See the Splunk HTTP Event Collector documentation for instructions.

Note: Any triggers configured to send records through `commitRecord` to an Explore appliance are automatically redirected to the Splunk server. No further configuration is required.

Send records from ExtraHop to Splunk

1. Log into the Admin UI on the ExtraHop appliance.

   Complete this procedure on all connected Command and Discover appliances.
2. In the Records section, click **Third-party Recordstore**.
3. Select **Enable Splunk as the recordstore**.

   If you are migrating to Splunk from a connected Explore appliance, you will no longer be able to access records stored on the Explore appliance.
4. In the Record Ingest Target section, complete the following fields:

   a) Splunk Host: The hostname or IP address of your Splunk server.

   b) HTTP Event Collector Port: The port for the HTTP Event Collector to send records over.

   c) HTTP Event Collector Token: The authorization token you created in Splunk for the HTTP Event Collector.
5. In the Record Query Target section, complete the following fields:

   a) Splunk Host: The hostname or IP address of your Splunk server.

   b) REST API Port: The port to send record queries over.

   c) Authorization Token: The authorization token for the Splunk REST API.
6. Clear the **Require certificate verification** checkbox if your connection does not require a valid SSL/TLS certificate.

   Note: Secure connections to the Splunk server can be verified through trusted certificates that you upload to the ExtraHop system.
7. In the Index Name field, type the name of the Splunk index where you want to store records.

   The default index on Splunk is called `main`, however, we recommend that you create a separate index for your ExtraHop records, and type the name of that index.
8. Click **Test Connection** to verify that your Discover appliance can reach your Splunk server.
9. Click **Save**.

After your configuration is complete, you can query for stored records in the ExtraHop Web UI by clicking **Records**.

Note: The **Chart Summary** and **Group by** selector are not available on the Records page.