Integrate ExtraHop with Splunk

Published: 2018-10-27

The ExtraHop system monitors network and application performance by gathering data passively on the network. It offers deep and customizable analytics of wire data in real time.

Splunk collects and indexes data generated by applications, servers, and other devices. The Splunk big-data platform offers storage and correlation of a variety of data sources.

Integrating ExtraHop with Splunk enables long-term storage and trending of wire data and correlation of wire data with other sources, such as machine data from logs.

The ExtraHop Splunk bundle and the Splunk app serve as templates for getting started with integrating the two solutions. You can modify these templates to configure what data is sent from ExtraHop to Splunk and how it is displayed in Splunk.

Note: This guide assumes a general understanding of how to write and deploy ExtraHop Application Inspection Triggers, bundles, and other user-defined data-gathering methods in ExtraHop. To learn more about triggers, see the ExtraHop Trigger API Reference guide.

System requirements

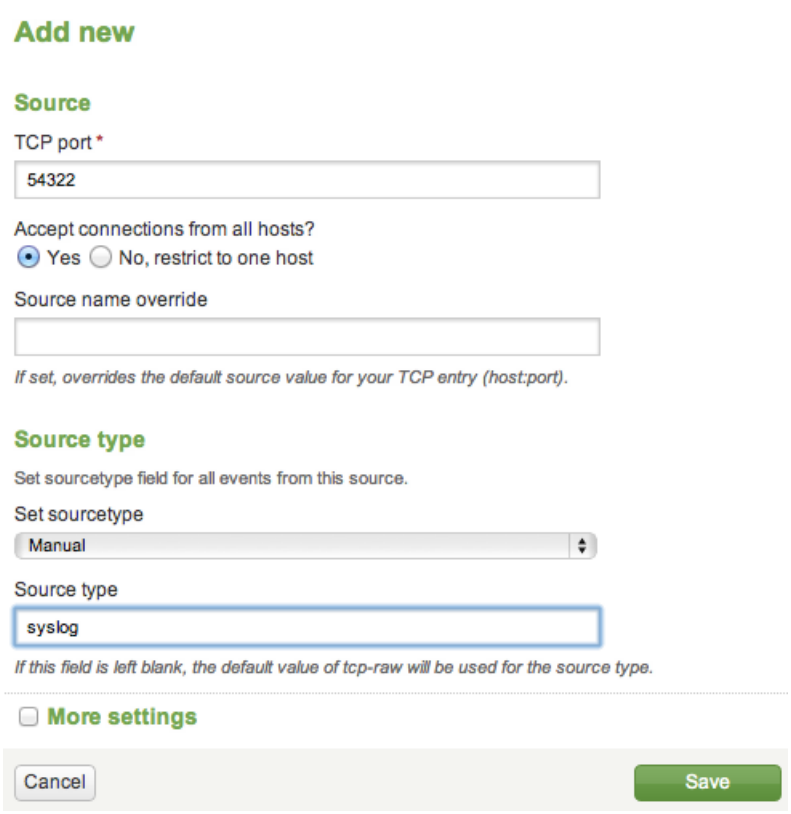
- ExtraHop platform version 4.0 or later
- Splunk version 4.3 or later

Configure ExtraHop to send events to Splunk

1. Open Splunk and enter your username and password.
2. Go to Manager and click **Data Inputs**.
3. In the TCP section, click **Add New**.
4. On the Add New page, complete the following actions to configure a TCP port:

   • **Source type:** In the Source type field, enter `syslog`.

   • **TCP port:** In the TCP port field, note the port number. You will need this port number to send triggers and alerts from ExtraHop to Splunk.



Send triggers to Splunk

1. From the ExtraHop Web UI, click the System Settings icon at the top of the page, and then click **Administration**.
2. From the Admin UI, in the System Configuration section, click **Open Data Streams**.
3. Click **Add Target**.
4. From the Target Type drop-down menu, select **Syslog**.
5. Enter the following information:

   Name

   A name to identify this configuration.

   Note: The configuration you create is automatically titled `default` and cannot be renamed.

   Host

   The hostname or IP address of your syslog server.

   Port

   The port number configured in Splunk.

   Protocol

   From the drop-down, select **TCP**.

   Local Time

   Select this checkbox if you want to send syslog information with timestamps in the local time zone of the ExtraHop appliance. If this option is not selected, timestamps are sent in GMT.
6. Click **Save**.

Note: In an ExtraHop Command appliance deployment, perform these steps on each Discover node and not on the Command appliance.

Send alerts to Splunk

1. From the ExtraHop Web UI, click the System Settings icon at the top of the page and click **Administration**.
2. From the Admin UI, in the Network Settings section, click **Notifications**.
3. Click **Syslog**.
4. On the Syslog Notification Settings page, complete the following actions:
   - **Destination:** In the Destination field, enter the host name.
   - **Protocol:** Click the **Protocol** drop-down list and select **TCP**.
   - **Port:** In the Port field, enter the port number configured in Splunk.
5. Click **Save**.

Note: In an ExtraHop Command appliance deployment, perform these steps on each Discover node and not on the Command appliance.

Install the ExtraHop Splunk bundle

1. On the ExtraHop website, click the Community menu and select the Solutions Bundle Gallery.
2. Log in with your credentials.
3. From the list of bundles, click **ExtraHop Splunk Bundle**.

Note: You can filter the list of bundles by entering a keyword, such as "`Splunk`" into the Filter bundle list field.

4. Click **Download Now** and save the .json file to your computer.
5. From the Web UI of a Discover appliance, click the System Settings icon at the top of page and click **Bundles**.
6. Click **Upload** and do one of the following:
   - Paste the raw bundle data into the window.
   - Upload a saved bundle in .json file format from your workstation.
7. Click **Upload**.
8. Click **OK** to save the bundle.
9. Reopen the bundle and click **Apply** to load the triggers.
10. Assign the triggers to an appropriate device or a device group (for example, assign "HTTP Events to Splunk" to web server devices) by doing one of the following:
    - (Device) In the top menu, click **Metrics**. tIn the left panel, under Sources, click **Devices**. On the **Devices** page, select a device from the list. In the left pane, click the name of the device. On the device overview page, select the **Trigger** tab, and then click the green icon.
    - (Device group) In the top menu, click **Metrics**. In the left panel, under Sources, click **Device Groups**. Select a group from the list. In the left pane, click the name of the device group. On the device group overview page, select the **Trigger** tab, and then click the green icon.

    Note: Only assign triggers to devices that require the collection of custom metrics. Assigning triggers to all devices causes unnecessary triggers to run, which might cause the system to run slowly.
11. From the Assign Triggers window, select the checkbox next to the trigger you want to assign to the device or device group.

12. Click **OK**.
13. From the Web UI of a Discover appliance, click the System Settings icon and click **Triggers**.
14. Select the checkbox next to the trigger you recently assigned.
15. Click **Enable**.

View results in the Splunkbase ExtraHop app

1. Go to `http://splunk-base.splunk.com/apps/53757/extrahop` and log in with your Splunk credentials to download the Splunkbase ExtraHop app.
2. Click **Download App**.
   A list of apps appears.
3. Click **ExtraHop**.
4. At the top of the page, click **App** and then click **Manage apps…**
5. On the Apps page, click **Install app from file**.
6. Click **Choose File**, select the file you downloaded, and then click **Upload**.
7. Click **Restart Splunk**.
8. At the top of the page, click **App** and then click **ExtraHop** to see the data.

   You can customize the fields and set the frequency for sending data to Splunk by modifying the triggers in the ExtraHop Web UI. For example, you can set a condition such that data is only sent to Splunk if errors occur or if response times are exceedingly high. For more information about triggers, see the Trigger section of the ExtraHop Web UI Guide.

   You can customize how the ExtraHop data appears in Splunk by creating your own views. For more information about how to work with Splunk data, refer to the Splunk KnowledgeBase at http://docs.splunk.com/Documentation/Splunk.