

Integrate ExtraHop with Splunk

Introduction

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 allows for 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.

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 user-defined elements, go to the navigation bar in the ExtraHop Web UI and click the **Help** button.

System Requirements

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

Configuring ExtraHop to Send Events to Splunk

1. Open Splunk and enter your username and password.
2. Go to **Manager** and click **Data Inputs**.

Data inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to [Forwarding and receiving](#).

[Add data](#)

| Type | Inputs | Actions |
|---|--------|-------------------------|
| Files & directories <i>Upload a file, index a local file, or monitor an entire directory.</i> | 4 | Add new |
| TCP <i>Listen on a TCP port for incoming data, e.g. syslog.</i> | 0 | Add new |
| UDP <i>Listen on a UDP port for incoming data, e.g. syslog.</i> | 0 | Add new |
| Scripts <i>Run custom scripts to collect or generate more data.</i> | 0 | Add new |

3. Go to TCP and click **Add New**.
4. Configure a TCP port with source type `syslog` and note the port.

Add new

Source

TCP port *

Accept connections from all hosts?
 Yes No, restrict to one host

Source name override

If set, overrides the default source value for your TCP entry (host:port).

Source type

Set sourcetype field for all events from this source.

Set sourcetype

Source type

If this field is left blank, the default value of tcp-raw will be used for the source type.

More settings

Sending Triggers to Splunk

1. In the ExtraHop Web UI, click **Settings** and click **Administration**.
2. Go to the Configuration section and click **Open Data Streams**.

| Configuration | |
|----------------------------|------------------------|
| Running Config | Change |
| Geomap Data Source | Change |
| Datastore & Customizations | Change |
| Open Data Streams | Change |
| Capture | Change |
| Trends | Change |

3. Click **Syslog Systems**.
4. On the Open Data Stream for Syslog Settings page:
 - a. In the **Host** field, enter the host name.
 - b. Click the **Protocol** drop-down list and select **TCP**.
 - c. In the **Port** field, enter the port you noted earlier.

Open Data Stream for Syslog Systems

Host:

Protocol: TCP

Port:





Save
Test Settings
Cancel

5. Click **Save**.

In an ECM-powered deployment, perform these steps on each node, not on the ECM.

Sending Alerts to Splunk

1. In the ExtraHop Web UI, click **Settings** and click **Administration**.
2. Go to the Network Settings section and click **Notifications**.

| Network Settings | |
|------------------|---|
| Atlas Services |  Connect |
| Connectivity |  Change |
| Notifications |  Change |
| SSL Certificate |  Change |

3. Click **Syslog**.
4. On the Syslog Notification Settings page:
 - a. In the **Destination** field, enter the host name.
 - b. Click the **Protocol** drop-down list and select **TCP**.
 - c. In the **Port** field, enter the port you noted earlier.

Syslog Notification Settings

Destination:

Protocol:

Port:

5. Click **Save**.

In an ECM-powered deployment, perform these steps on each node, not on the ECM.

Installing the ExtraHop Splunk Bundle

1. Log in to the ExtraHop Support Forum (<https://forum.extrahop.com>) with your Support Portal credentials and click **ExtraHop Splunk Bundle**.
2. Select and copy the ExtraHop Splunk bundle data.
3. In the ExtraHop Web UI toolbar, click **Settings** and then click **Bundles**.



4. Click **Upload**, paste the raw bundle data into the window OR upload a saved bundle in .json file format from your workstation, and then click **Upload**.

Load Bundle

Paste bundle data:



Upload bundle file: No file chosen

- Click **OK** to save the bundle, reopen the bundle, and then click **Apply** to load the triggers.





Bundle Settings



Name:

Contents:

-  Alerts (0)
-  Triggers (5)

| Name | Description |
|-----------------------------------|-------------|
| HTTP events to Splunk | |
| Memcache events to Splunk | |
| Database events to Splunk (helper | |
| Database events to Splunk | |
| CIFS events to Splunk | |
| | |
| | |
| | |

-  Pages (0)
-  Flex Grids (0)
-  Dynamic Groups (0)
-  Geomaps (0)

Actions:  Apply |  Download

No assignments in bundle **Existing objects:** Skip ▼

Description:

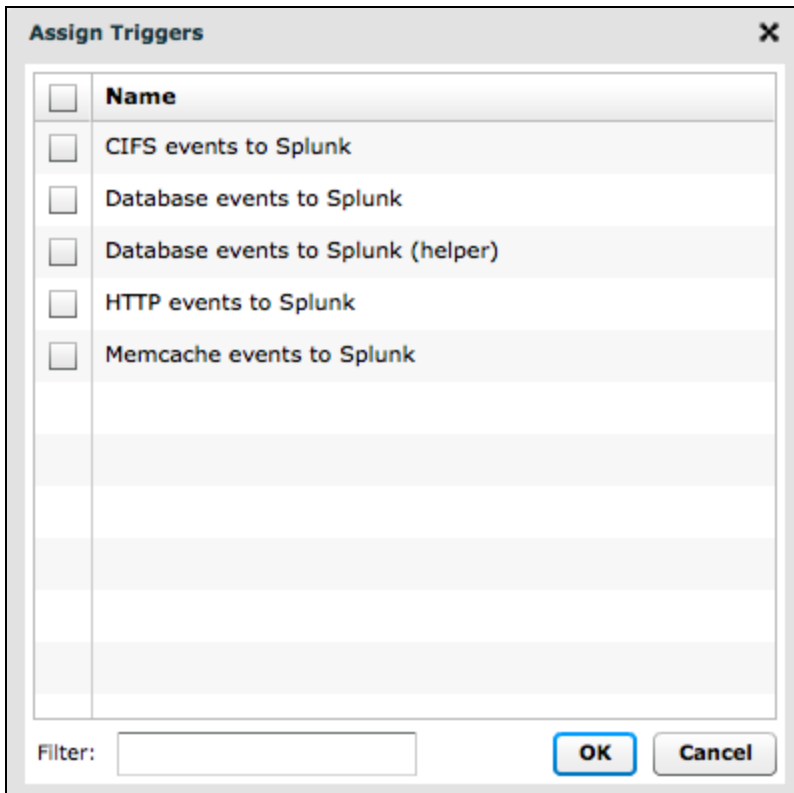
Edit Raw Data ...
OK
Cancel

- Assign the triggers to appropriate devices and device groups (e.g., assign "HTTP Events to Splunk" to web servers).
 - Go to **Devices** and select a device from the list. Click the **Select Action** drop-down list and select **Assign Trigger**.
 - OR
 - Go to **Device Groups**, select the **Activity Groups** tab, and then select a group from the list. Select a

device from the list, and then click the device name in the left panel. Click the **Triggers** tab, and then click the **Add** symbol.

Assign triggers only to devices that require the collection of custom metrics. Assigning triggers to all devices will cause unnecessary trigger executions that may cause the system to run slowly.

7. In the **Assign Triggers** window, select the checkbox next to the triggers and click **OK**.



8. Click **Settings**, click **Triggers**, select the triggers, and then click **Enable**.

Settings » Triggers

+ New |
 📄 Copy |
 ✖ Delete |
 ● Enable |
 ● Disable

| <input type="checkbox"/> | Name | Author | Event | Type | Debug Mode | Description | Status |
|--------------------------|--|--------|-------------|--------|------------|-------------|----------|
| <input type="checkbox"/> | HTTP events to Splunk | | HTTP_RES | Device | Disabled | | Disabled |
| <input type="checkbox"/> | Memcache events to Splunk | | MEMCACH | Device | Disabled | | Disabled |
| <input type="checkbox"/> | Database events to Splunk (helper) | | DB_REQUIRE | Device | Disabled | | Disabled |
| <input type="checkbox"/> | Database events to Splunk | | DB_RESPONSE | Device | Disabled | | Disabled |
| <input type="checkbox"/> | CIFS events to Splunk | | CIFS_RES | Device | Disabled | | Disabled |

Viewing the Results in the SplunkBase ExtraHop App

1. To see the results, go to <http://splunk-base.splunk.com/apps/53757/extrahop> and click **Download App**.
2. Log in or sign up for Splunk.
3. A list of apps appears. 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**.

Apps Find more apps online Install app from file Create app

Showing 1-10 of 10 items Results per page 25 ↓

| Name ↓ | Folder name ↓ | Version ↓ | Update checking ↓ | Visible ↓ | Sharing ↓ | Status ↓ | Actions |
|-----------------|----------------|-----------|-------------------|-----------|-----------------------------------|-----------------------------------|---|
| Getting started | gettingstarted | 1.0 | Yes | Yes | App Permissions | Enabled Disable | Launch app Edit properties View objects |
| Home | launcher | | Yes | Yes | App Permissions | Enabled | Launch app Edit properties View objects |
| learned | learned | | Yes | No | App Permissions | Enabled Disable | Edit properties View objects |
| legacy | legacy | | Yes | No | App Permissions | Disabled Enable | |

6. Click **Choose File**, select the file you downloaded, and then click **Upload**.

Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. [Learn more.](#)

File

extrahop.tar.gz

Upgrade app. Checking this will overwrite the app if it already exists.

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 using triggers, refer to *ExtraHop Guide: Getting Started with Application Inspection Triggers* on the ExtraHop Support Forum (<https://forum.extrahop.com>).

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>.