Configure a syslog target for an open data stream

Published: 2019-10-18

You can export data on an ExtraHop Discover appliance to any system that receives syslog input (such as Splunk, ArcSight, or Q1 Labs) for long-term archiving and comparison with other sources.

1. Log into the Admin UI on the ExtraHop Discover appliance.
2. In the System Configuration section, click **Open Data Streams**.
3. Click **Add Target**.
4. From the Target Type drop-down menu, select **Syslog**.
5. In the Name field, type a name to identify the target.
6. In the Host field, type the hostname or IP address of the remote syslog server.
7. In the Port field, type the port number of the remote syslog server.
8. From the Protocol drop-down menu, select one of the following protocols over which to transmit data:
   - **TCP**
   - **UDP**
9. Select **Local Time** to send syslog information with timestamps in the local time zone of the Discover appliance. If this option is not selected, timestamps are sent in GMT.
10. Optional: Click **Test** to establish a connection between the Discover appliance and the remote syslog server and send a test message to the server.
    The dialog box displays a message that indicates whether the connection succeeded or failed. If the test fails, edit the target configuration and test the connection again.
11. Click **Save**.

Next steps

Create a trigger that specifies what syslog message data to send and initiates the transmission of data to the target. For more information, see the Remote.Syslog class in the ExtraHop Trigger API Reference.