Send system notifications to a remote syslog server

Published: 2024-07-16

The syslog export option enables you to send alerts from an ExtraHop system to any remote system that receives syslog input for long-term archiving and correlation with other sources.

Only one remote syslog server can be configured for each ExtraHop system.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **Notifications**.
3. In the Destination field, type the IP address of the remote syslog server.
4. From the **Protocol** drop-down list, select **TCP** or **UDP**.

   This option specifies the protocol over which the information will be sent to your remote syslog server.
5. In the Port field, type the port number for your remote syslog server.

   The default value is 514.
6. Click **Test Settings** to verify that your syslog settings are correct.

   If the settings are correct, you should see an entry in the syslog log file on the syslog server similar to the following:

   ```
   Jul 27 21:54:56 extrahop name="ExtraHop Test" event_id=1
   ```
7. Click **Save**.
8. Optional: Modify the format of syslog messages.

   By default, syslog messages are not compliant with RFC 3164 or RFC 5424. However, you can format syslog messages to be compliant by modifying the running configuration file.
   a) Click **Admin**.
   b) Click **Running Config (Unsaved Changes)**.
   c) Click **Edit Config**.
   d) Add an entry under `syslog_notification`, where the key is `rfc_compliant_format` and the value is either `rfc5424` or `rfc3164`.

      The `syslog_notification` section should look similar to the following code:

      ```
      "syslog_notification": {
          "syslog_destination": "192.168.0.0",
          "syslog_ipproto": "udp",
          "syslog_port": 514,
          "rfc_compliant_format": "rfc5424"
      }
      ```
   e) Click **Update**.
   f) Click **Done**.
9. Optional: Modify the timezone referenced in syslog timestamps.

   By default, syslog timestamps reference UTC time. However, you can modify timestamps to reference the ExtraHop system time by modifying the running configuration file.
   a) Click **Admin**.
   b) Click **Running Config (Unsaved Changes)**.
   c) Click **Edit Config**.
   d) Add an entry under `syslog_notification` where the key is `syslog_use_localtime` and the value is `true`.

The `syslog_notification` section should look similar to the following code:

```
    "syslog_notification": {
        "syslog_destination": "192.168.0.0",
        "syslog_ipproto": "udp",
        "syslog_port": 514,
        "syslog_use_localtime": true
    }
```

e) Click **Update**.
f) Click **Done**.

Next steps
After you confirm that your new settings are working as expected, preserve your configuration changes through system restart and shutdown events by saving the running configuration file.