System Health FAQ

Published: 2020-02-21

Here are some answers to frequently asked questions about System Health.

How do I check for possible data loss?

The best indicators of data loss are dropped packets, TCP desyncs, and excessively high packet or throughput rates.

- Check the Drops chart for packets dropped at the network card interface, SPAN, or network tap
- Check the TCP desyncs chart for system-wide desyncs, which indicate that synchronization was lost when processing a TCP connection.
- Monitor the following charts to ensure that the ExtraHop Discover appliance is not exceeding product thresholds:
  - Incoming packets breakdown
  - Incoming throughput breakdown

  A high packet rate or throughput rate might result in packets dropped at the span source or at a span aggregator. Acceptable rates and limits are available on the Datasheets for Discover appliances.

How do I monitor resource consumption?

The Discover appliance allocates memory resources for capturing packets, running triggers, transmitting data to remote servers, and recording to the datastore.

Check the following charts for the amount of memory that the Discover appliance dedicates to each resource area over a given time range:

- Capture heap allocation
- Trigger heap allocation
- Remote heap allocation
- Datastore heap allocation
- Datastore trigger heap allocation

How do I check the performance of my RPCAP deployments?

After the initial setup of a remote packet capture (RPCAP) deployment, it is a good idea to make sure your deployment is working as expected.

- Check the RPCAP packets chart to ensure that packets are being captured and that the volume matches your network traffic.

- Monitor the RPCAP throughput chart to check whether RPCAP resources are being consumed efficiently. If RPCAP resources are heavily consumed, you could have expansion problems as throughput increases or as you add RPCAP deployments.

Are my triggers running properly?

To get the most out of your triggers, it makes sense to make sure that new and modified triggers are running and to monitor for problems that can affect system performance or result in incorrect data.

- View the Trigger executes chart to ensure that the amount of trigger activity is consistent with your expectations. Look for bursts of trigger activity that might indicate inefficient behavior from one or more triggers.
- View the Trigger executes by trigger chart after you have created a new trigger or modified an existing one to ensure that the trigger is running. Any trigger consuming higher resources than average might have a poorly-optimized script that is affecting performance.
- Check the Trigger exceptions by trigger chart to display any unhandled trigger exceptions. Exceptions are a large contributor to system performance issues and should be corrected immediately
- Check the Trigger drops chart to view the number of triggers that have been dropped from the trigger queue. A common cause of dropped triggers is a long-running trigger that is dominating resource consumption.

You can monitor whether your datastore triggers, also referred to as bridge triggers, are running properly with the following charts:

- Datastore trigger executes
- Datastore trigger exceptions by trigger
- Datastore trigger drops

How do triggers affect my Discover appliance?

In addition to monitoring how well your triggers are running, the System Health page provides charts that enable you to monitor and assess the impact of running triggers to your Discover appliance.

- View the Trigger load chart to display several measurements of resource consumption by all running triggers. Look for spikes in consumption that can indicate that a new trigger has been introduced or that an existing trigger is having issues.
- Check the Trigger load by trigger chart to view the number of cycles consumed by each running trigger. A trigger that runs seldom but consumes more cycles than average can cause other triggers to be dropped from the queue. To investigate further, click this chart to open a details page containing additional per-trigger consumption metrics, such as the number of cycles and the number of exceptions.
- Check the Trigger load by thread chart to view the percentage of trigger cycle consumption of each thread allocated to trigger operations. Look for an even amount of consumption among multiple threads. Trigger drops might occur if the consumption of one thread is considerably higher than the others, even if the thread consumption is at a low percentage.

You can monitor the impact of datastore triggers, also referred to as bridge triggers, that are running on your Discover appliance with the following charts:

- Datastore trigger load
- Datastore trigger load by trigger

How are my open data streams performing?

You can monitor charts that pertain to the health and performance of open data stream (ODS) transmissions to a third-party syslog, database, or server.

- Click the Messages sent chart to view the total number of messages transmitted by all active data streams. Monitor this chart to ensure that messages are being transmitted as expected. If no bytes are sent, there might be an issue with the configuration of an open data stream or an ODS trigger.

- Click the Message throughput chart to view the total number of bytes transmitted by all active data streams. Monitor this chart to ensure that bytes are being transmitted as expected. If no bytes are sent, there might be an issue with the configuration of an open data stream or an ODS trigger.
- Check the Connections chart for an at-a-glance view of attempts to connect to ODS targets and errors that occurred during the attempts.
- Check the Message errors chart to view which ODS connections resulted in errors. Mouse over the graph to display additional error details that help you determine the cause of an error.
- Monitor the Messages dropped chart to view the number of messages dropped from an open data stream because the message queue was full. Dropped messages indicate that the message queue is too long.
- Monitor the Message queue length chart to display the number of messages waiting in the queue. A long message queue might indicate that the Discover appliance is sending data faster than the remote system can process.

What is the estimated lookback capacity?

Lookback refers to how far back you are currently able to look up historical data. For example, you might be able to look up 1-hour intervals of data as far back as 9 days.

- Monitor the Store lookback chart to determine the current estimated lookback capacity of your Discover appliance. The chart displays lookback metrics for 1 hour, 5 minute, and 30 second time intervals based on the write throughput rate.

How many devices is the appliance monitoring?

The System Health page provides charts that help you determine how many L2, gateway, pseudo, custom, and L3 devices are monitored by the Discover appliance.

- Check the Active devices chart to ensure that the total number of active devices being monitored is as expected.
- Check the Total devices chart to ensure that the total number of all devices recognized by the Discover appliance, whether active or inactive, is as expected.

Are my SSL certificates decrypting as expected?

You can access a list of all certificates that perform decryption on the Discover appliance by clicking **Certificates** at the top of the System Health page.

- Check the SSL certificates table to ensure that the correct SSL certificates are installed on the Discover appliance and to view encryption metrics for each certificate. Encryption metrics help you determine if your certificates are performing decryption as expected. For example, you can check the number of successfully encrypted sessions or the number of sessions that were not decrypted due to hardware errors.

How do I add system health metrics to a dashboard?

You can customize your view of system performance information by adding system health metrics to a dashboard. You can add multiple metrics to a chart to compare data, such as the total throughput of the network capture compared with the total packets. You can choose a chart type that best fits how you would like to view data. For example, you can view how often each trigger is running in a line chart or a pie chart. You can also add chart notes and tips in text boxes.

1. Log into the Web UI on the ExtraHop Discover or Command appliance.
2. Click **Dashboards** from the top menu.
3. Click the command menu ⋮ in the upper right corner and select **Create Dashboard** to open an empty dashboard.
4. Type a name for your dashboard, and then click **Create**.

5. Click the empty chart widget in your newly created dashboard to launch the Metric Explorer where you will configure your dashboard.
6. Click **Add Source**, and then add the wire network monitored by the ExtraHop appliance to the Sources field. This entry is typically at the top of the list and is identified by the word Capture followed by a MAC address.
7. In the Metrics field, click the **Any Protocol** text, and then select ExtraHop from the list.
8. From the drop-down list, select the health metric you would like to add, such as L2 Duplicate Packets or Trigger Executes.
9. Click **Save** to return to your dashboard.
10. Click **Exit Layout Mode** from the upper-right corner.

Assess available system health metrics to identify metrics that are most important to you. For example, you can create a dashboard that focuses on the performance of remote packet capture or one that tracks SSL certificates.

If you are unfamiliar with creating dashboards, see our Dashboard Walkthrough.

What other tools can help me evaluate system health?

The Status and Diagnostics section of the Admin UI provides metrics about the overall health of the ExtraHop appliance and diagnostic tools that enable ExtraHop Support to troubleshoot system errors.

- Check health statistics to view metrics that indicate the operating efficiency of the ExtraHop appliance.
- Check the audit log to view event logging data and to change syslog settings.
- Learn about exception files and how to enable or disable them on the ExtraHop appliance.
- Learn about support scripts and how to upload and run them on the ExtraHop appliance.

You can also view the following resources to learn more about system health:

- System Health Walkthrough: Assess trigger performance
- ExtraHealth Bundle