# System Health FAQ

Published: 2021-08-31

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 Capture Drop Rate chart for packets dropped at the network card interface, SPAN, or network tap
- Check the 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 sensor (Discover appliance) is not exceeding product thresholds:
  - Throughput
  - Packet Rate

  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 and Datastore Heap Allocation
- Trigger and Remote Heap Allocation
- Datastore Trigger Load

### 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 Forwarded by Peer chart to make sure that the volume of packets sent to the ExtraHop system match the filter rules specified for your RPCAP peer devices.
- Monitor the Received by Appliance chart to make sure ExtraHop systems are efficiently receiving packets from RPCAP peers.

### Are my triggers running properly?

To get the most out of your triggers, make sure that new and modified triggers are producing accurate data without degrading system performance.

- View the Trigger Executes and Drops 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. With this chart, you can also track the number of triggers that have been dropped from the trigger queue. The ExtraHop system might drop a long-running trigger that is dominating resource consumption.
- 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.

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

- Datastore Trigger Executes and Drops
- Datastore Trigger Exceptions by Trigger

### 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.
- Check the Trigger Cycles by Thread chart to view the number of cycles each thread has 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.

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 Executes and Drops

### 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 and the number of errors that occurred during those transmissions. 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.

- Monitor the Messages Dropped by Remote Type chart to view the rate that messages are being dropped before they reach a recordstore or ODS target. A high number of drops can indicate that message throughput is too high to be processed by the ExtraHop system or the target server. .
- Monitor the Exremote Message Queue Length and Capture Message Queue Length charts to display the number of messages waiting in the ExtraHop Remote (exremote) and Capture (excap) queues. A high number of messages in these queues might indicate that message throughput is too high to be processed by the ExtraHop system or the target server.

### 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 Metric Data Lookback Estimates 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 Certificate Details 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 create a new, customized dashboard of system metrics or you can add a single system health chart to an existing dashboard. Locate the chart you want on the System Health dashboard, click the title, and then select **Copy to...**. Select **New Dashboard** or select an existing dashboard.

**Tip:** If you are unfamiliar with creating and editing dashboards, see our Dashboard Walkthrough.

### What other tools can help me evaluate system health?

The Status and Diagnostics section of the Administration settings provides metrics about the overall health of the ExtraHop system 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 system.
- 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 system.
- Learn about support scripts and how to upload and run them on the ExtraHop system.

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

- System Health Walkthrough: Assess trigger performance

- ExtraHealth Bundle